UNIVERZA V LJUBLJANI
FAKULTETA ZA DRUŽBENE VEDE

Anja Kolak

Mentor: doc. dr. Iztok Prezelj

POMEN IN VLOGA KRIPTOGRAFIJE IN KRIPTOANALIZE NA PODROČJU ZAGOTAVLJANJA NACIONALNE VARNOSTI

Diplomsko delo

Ljubljana, 2006

KAZALO

SEZNAM KRATIC

AES	Advanced Encryption Standard Simetrični algoritem za šifriranje
CA	Certificate Authority Overitelj digitalnih potrdil
DES	Data Encryption Standard Standardni kriptografski algoritem
EU	European Union Evropska unija
INFOSEC	Information Security Informacijska varnost
KDC	Key Distribution Center Strežnik ključev
NATO	North Atlantic Treaty Organization Organizacija severnoatlantskega sporazuma
NIST	National Institute of Standards and Technology Nacionalni inštitut za standarde in tehnologijo
NSA	National Security Authority Nacionalno varnostni organ
PGP	Pretty Good Privacy Program za šifriranje sporočil na osebnih računalnikih
PKI	Public Key Infrastructure Infrastruktura javnih ključev
SIGEN-CA	Slovenian General Certification Authority Izdajatelj digitalnih potrdil za fizične osebe in poslovne subjekte
SIGOV-CA	Slovenian Governmental Certification Authority Izdajatelj digitalnih potrdil za državne organe
SSL	Secure Sockets Layer Protokol za zagotavljanje varne komunikacije
TEMPEST	Transient Electromagnetic Pulse Emanation Surveillance Technology Tehnika prestrezanja oddanih začasnih elektromagnetnih signalov
ZDA	Združene države Amerike

1 UVOD

Dejstvo je, da je informacijska tehnologija dosegla vse pore posameznikovega in javnega življenja. Informacijska in računalniška varnost sta tako postali najpomembnejši zahtevi informacijske družbe. S prodorom računalniške tehnologije na vsa področja državnih institucij, služb in agencij se je povečal pretok informacij in podatkov. Ti subjekti so se povezali v različne komunikacijske sisteme in zastavlja se vprašanje, kako varovati pomembne informacije in tajne podatke, ki morajo ostati nerazkriti, da lahko sistem, kot je država, nemoteno in učinkovito deluje. Danes ni države, ki pri varovanju informacij in podatkov ne uporablja kriptografske zaščite (programske ali strojne), ter si s tem zagotavlja mesto enakovrednega partnerja v meddržavnih in mednarodnih zvezah ter povezavah.

Da je možnost vdora v sisteme zmanjšana na minimum, nam omogočajo dobri varnostni mehanizmi in varnostna politika. Varnostni mehanizmi so orodja, s pomočjo katerih skušamo preprečiti neželene napade na kriptografske sisteme in 'razbijanje' (kriptoanaliza) šifrirnih algoritmov. Osnoven varnostni mehanizem je šifriranje, ki ga dosežemo s pomočjo kriptografije. Enako pomembno vlogo imajo še mehanizmi, kot so: digitalno potrdilo, digitalno podpisovanje, kontrola dostopa itn.

V zgodovinski literaturi sta kriptografija in kriptoanaliza fascinantni, pri učenju teorije zapleteni, v praksi nepogrešljivi. Koncept varnosti in zaščite sporočil pri prenosu od pošiljatelja do prejemnika ima dolgo zgodovino. Z razvojem komuniciranja med ljudmi (govor in pisava) se je pojavila želja in potreba po skrivanju vsebine sporočil. Začelo se je s preprosto substitucijo črk in znakov na ravni posameznika in se nadaljevalo vse do zapletenih, visoko strukturiranih matematičnih kriptografskih sistemov na nacionalni ravni.

Na razvoj kriptologije so korenito vplivali trije dejavniki, ki jih lahko označimo tudi kot mejnike moderne kriptologije. V poznih sedemdesetih letih prejšnjega stoletja se je rodila zamisel o sistemu šifriranja z javnimi ključi; zasnovan je bil algoritem RSA in v začetku devetdesetih je bil napisan program PGP. Posledica tega je bila, da se je začela kriptografija množično uporabljati na zasebnem področju in tako ni bila več skrita očem javnosti.

Danes med nami ni posameznika, ki se pri svojih vsakodnevnih opravilih in obveznostih ne bi srečal s kakšnim kriptografskim zapisom. Vsaka bančna kartica ali pametna kartica v GSM aparatu ima namreč varnostni mehanizem (šifrirni zapis) in med drugim ima vsak moderen medmrežni brskalnik vgrajene različne kriptografske algoritme, s pomočjo katerih so pomembni podatki zaščiteni in nedostopni vsiljivcem ali nepooblaščenim osebam.

Uporaba in zmogljivost današnjih kriptosistemov rešujeta številne probleme, ki so povezani z nacionalnim in informacijskim razvojem ter medmrežno komunikacijo, še posebno v elektronskem poslovanju. Danes kriptografija predstavlja bistveni del informacijskega sistema. Zagotavlja nam varnost, točnost, zaupnost, zanesljivost in odgovornost. Lahko potrdi našo identiteto ali zaščiti anonimnost, prepreči in onemogoči nedovoljene uporabe dokumentov, pomembnih informacij in tajnih podatkov. Kriptologija je 'orodje', ki postaja vedno bolj pomembno tudi pri preprečevanju terorizma in organiziranega kriminala, in sicer z metodami, kot so prestrezanje in dešifriranje sporočil ter prisluškovanje.

Posledice uporabe kriptografije in kriptoanalize imajo v praksi tudi negativen vpliv, saj se je v boju proti organiziranemu kriminalu, terorizmu, napadom na gospodarska, ekonomska, politična in vojaška področja stopnja nadzora v družbi močno povečala. Organi pregona in druge službe tako tudi s pomočjo različnih kriptografskih in kriptoanalitičnih metod pogosto posegajo v človekovo zasebnost in kršijo človekove pravice.

V diplomski nalogi predstavljam kompleksno področje kriptografije in kriptoanalize ter poizkušam prikazati povezavo teh mehanizmov z nacionalno varnostjo. Najprej postavljam metodološki okvir naloge, opredeljujem temeljne pojme s tega področja, predstavljam cilje ter hipoteze. V nadaljevanju opisujem kratek zgodovinski pregled uporabe kriptologije v praksi, metode in tehnike kriptografskih sistemov ter naštevam področja uporabe. V osmem poglavju poizkušam ugotoviti, kako varni in zanesljivi so kriptosistemi ter katere varnostne modele uporabljamo. Podrobneje analiziram uporabo kriptologije v Sloveniji, katerim standardom se je morala Slovenija prilagoditi in katere zakone sprejeti z vstopom v zvezo NATO in EU. Na koncu poizkušam ugotoviti, ali z uporabo kriptologije lahko zagotavljamo nacionalno varnost (kako?) oziroma, ali jo lahko ogrožamo (kako?).

2 METODOLOŠKO HIPOTETIČNI OKVIR

2.1 OPREDELITEV PREDMETA IN CILJEV PROUČEVANJA

Osrednji predmet proučevanja v diplomski nalogi sta pomen in vloga kriptografije ter kriptoanalize na področju zagotavljanja nacionalne varnosti. Nedvomno je kriptologija področje, ki predstavlja pomemben del varnostne arhitekture. Kje in kako se uporablja ter kako pomembna je za nacionalno varnost, poizkušam ugotoviti v nadaljevanju. Za lažje raziskovanje in analiziranje v diplomski nalogi sem si zastavila naslednje cilje:

- pojasniti temeljne pojme s področja kriptografije in kriptoanalize;
- opisati zgodovinski razvoj in uporabo kriptografije in kriptoanalize;
- analizirati vzroke uporabe kriptografije in kriptoanalize;
- opisati metode in tehnike uporabe kriptografije in kriptoanalize;
- prikazati področja uporabe kriptografije in kriptoanalize;
- analizirati uporabo kriptografije in kriptoanalize v Republiki Sloveniji;
- ugotoviti, kakšen pomen in vlogo imata kriptografija in kriptoanaliza pri zagotavljanju nacionalne varnosti.

2.2 HIPOTEZE

V nalogi preverjam naslednje hipoteze:

1. Metode (tehnike) kriptografije in kriptoanalize se razvijajo vzporedno z razvojem informacijske in računalniške tehnologije, le te pa prinašajo nove oblike varnostnih tveganj.
2. Čeprav se je morala Republika Slovenja z vstopom v zvezo NATO in EU prilagoditi določenim standardom uporabe kriptografske zaščite ter spremeniti zakonodajo, še vedno nima enotnega sistema kriptozaščite.
3. Kriptografski sistemi so pomembni varnostni mehanizmi, ki se uporabljajo za izpolnitev varnostnih zahtev na področju nacionalne varnosti in so najvarnejši takrat, ko jih država patentira sama.
4. Kriptografija in kriptoanaliza imata pomembno vlogo na področju nacionalne varnosti, lahko jo zagotavljata ali ogrožata.

2.3 METODOLOŠKI PRISTOP

Pri pisanju diplomske naloge uporabljam naslednje raziskovalne metode:

- s pomočjo ***analize in interpretacije primarnih virov*** sem razčlenila in proučila dokumente, pogodbe, zakone ter dela navedenih avtorjev v literaturi. Pisna dela, kot so knjige, članki, enciklopedije ter raziskovalna dela, proučujem s pomočjo ***analize in interpretacije sekundarnih virov****;*
- za analizo razvoja in uporabe kriptografije in kriptoanalize od antike do danes uporabljam ***zgodovinsko razvojno analizo***;
- ***deskriptivno (opisno) metodo,*** s pomočjo katere bom pojasnila temeljne pojme, ki so v diplomski nalogi ključnega pomena;
- ***intervju,*** s pomočjo katerega bom pridobila podatke o Ministrstvu za obrambo Republike Slovenije in javni upravi.

3 TEMELJNI POJMI

Temelji pojmi so nujna osnova in instrument pri proučevanju ter analiziranju podatkov, zgodovinskih dejanj, mnenj in stališč. Za lažje razumevanje diplomske naloge sem v nadaljevanju opredelila naslednje temeljne pojme: kriptologija, kriptografija, kriptoanaliza in nacionalna varnost. Pri prebiranju literature sem naletela še na nekatere pojme, ki so tesno povezani s tem področjem (informacija, tajni podatki, varnost itn.), ki sem jih v poglavju, kjer se pojavijo, tudi razložila.

Naj povem, da pojmi kriptologija, kriptografija in kriptoanaliza v SSKJ niso opredeljeni. SSKJ definira samo pojem ***kriptogram***, ki knjižno pomeni besedilo oziroma so to znaki s prikritim besedilom.

3.1 KRIPTOLOGIJA

Kriptologija je veda o tajnem pisanju oziroma komuniciranju. Beseda je grškega izvora in je sestavljena iz dveh besed kryptós (skrito) in lógos (beseda) (Oliver Pell, http://www.ridex.co.uk/cryptology, 10. 10. 2005). Predmet proučevanja kriptologije sta kriptografija in kriptoanaliza in sta prav tako njena sestavna dela (A. Menezes, P. van Oorschot, and S. Vanstone, 1996:15). Še natančneje,

kriptologija je veda o tajnosti, šifriranju[1], zakrivanju sporočil (kriptografija) in o razkrivanju šifriranih podatkov (kriptoanaliza) (http://www.sigov.si/tecaj/kripto/kr-osn.htm, 10. 10. 2005).

Proučuje vse oblike tajnega sporazumevanja in je znanost o prevajanju nezaščitenih podatkov v zaščitene in obratno. Uporabljamo jo na vseh področjih komuniciranja in shranjevanja pomembnih in tajnih podatkov. (Encyclopaedia Britannica 2005 Deluxe Edition: Elektronska izdaja: United Kingdom).

3.2 KRIPTOGRAFIJA

Beseda kriptografija je grškega izvora kryptós (skrito) in gráphein (pisava). Kriptografija je veda, ki se ukvarja s skrivnim pisanjem oziroma natančneje s transformiranjem informacij v tako obliko, ki omogoča vpogled le pooblaščenim osebam oziroma osebam, ki imajo za tako informacijo ustrezen ključ[2] (Encyclopaedia Britannica 2005 Deluxe Edition: Elektronska izdaja: United Kingdom). V klasičnem smislu je kriptografija teorija o zakrivanju vsebine sporočil, danes pa je obsežno področje, ki obsega probleme, kot so pristnost, avtorizacija in digitalni podpis (Jurišić in Tonejc, 2001: 58).

Kadar govorimo o kriptografiji, govorimo tudi o matematičnih tehnikah, ki zadevajo varnost informacij z vidika zaupnosti – tajnosti, integritete podatkov, avtentičnosti udeležencev, izvora podatkov in preprečevanja tajenja. Kriptografija se ne uporablja samo za šifriranje oziroma dešifriranje podatkov temveč tudi za določitev katero matematično ali drugo tehniko bomo uporabili pri različnih metodah (Menezes, J. Alfred, van Oorschot, C. Paul, Vanstone, A. Scott (1996: 4).

---

[1] V kriptologiji se uporabljata še pojma enkripcija (šifriranje) in dekripcija (dešifriranje). Osnovno sporočilo ponavadi imenujemo **čistopis** (cleartext, plaintext), šifrirano pa **šifropis** ali **tajnopis** (kriptogram, ciphertext) (http://www.sigov.si/tecaj/kripto/kr-osn.htm, 21. 12. 2005).

[2] Sporočilo, ki ga želimo kriptografirati po nekem **postopku** (algoritmu, metodi, zaporedju) spremenimo v šifrirano sporočilo, pri tem uporabimo določene vrednosti za parametre v algoritmu, ki jim rečemo **ključ**. Sogovornika se morata dogovoriti, kakšen algoritem in ključ bosta uporabila, da si lahko pošiljata šifrirana sporočila. (http://www.sigov.si/tecaj/kripto/kr-osn.htm, 21. 12. 2005).

Da dobimo šifrirano sporočilo, uporabimo metodo šifriranja (enkripcije), pri branju zakodiranega besedila pa uporabimo metodo dešifriranja (dekripcije). Postopek šifriranja in dešifriranja imenujemo tudi **kriptosisitem**. Nasprotje tega pojma je **kriptoanaliza**.

Šifra (ang. cipher), izhaja iz hebrejske besede Saphar, ki pomeni šteti oz. označiti (Jurišić, Perko, Presek, letnik 33., št. 1, str. 22–24).

Glavni namen kriptografije je zagotoviti:

- ***zaupnost*** *(ang. confidentiality) in* ***tajnost*** *(ang. secrecy):* z ustreznimi postopki šifriranja zagotoviti zaupnost povezave med uporabnikom in prejemnikom, prav tako pa mora biti zagotovljena zaščita podatkov in informacij, ki se ob tem izmenjajo;
- ***celovitost podatkov*** *(ang. integrity): zagotoviti, da* podatki niso bili kakorkoli spremenjeni od svojega nastanka in da o tem ciljni uporabnik ne bi bil obveščen;
- ***avtentikacijo oz. overjanje*** *(ang. authentication):* zagotoviti verifikacijo resničnosti identitete in verifikacijo resničnosti izvora podatkov in informaci;
- ***preprečevanje tajenja*** *(ang. non-repudiation*): zagotoviti nezmožnost zanikanja izvora podatkov in preprečiti možnost ponarejanja opravljenih storitev;
- ***kontrolo dostopa*** *(ang. access control): zagotoviti zaščito pred nedovoljeno uporabo virov, ki so dosegljivi preko omrežja. Potrebno je upoštevati pravila dostopa in identiteto uporabnika.*

(Menezes, J. Alfred, van Oorschot, C. Paul, Vanstone, A. Scott (1996: 4).

V uradnem listu EU je kriptografija opredeljena kot: *»/d/isciplina načel, sredstev in metod preoblikovanja podatkov za zakrivanje vsebine informacije, zaščito pred njenim nezaznavnim spreminjanjem ali pred njeno nepooblaščeno rabo. Kriptografija se omejuje na preoblikovanje informacij z uporabo enega ali več tajnih parametrov*[3] *(tj. kriptospremenljivk) ali vgrajenega ključa.«* (Uradni list EU, Uredba Sveta (ES) št. 394/2006: 74/10).

Jerman Blažič opredeli šifriranje kot temeljni postopek vseh varnostnih sistemov. Pri šifriranju gre za manipulacijo znakov na način, da rezultat pokaže naključen niz znakov, torej za proces transformacije podatkov (čistopis) v obliko, ki onemogoča razumevanje teh znakov oziroma podatkov (tajnopis) (Jerman Blažič, 2004: 60).

[3] Tajni parameter je konstanta ali ključ, ki ni znan drugim oziroma je znan le znotraj skupine (Uradni list EU, Uredba Sveta (ES) št. 394/2006: 74/10).

Preprosto lahko rečem, da je poglaviten cilj kriptografije omogočiti prenos sporočila od osebe *A* do osebe *B,* na način, da nepooblaščenim osebam sporočilo ne bo razumljivo oz. berljivo.

Poleg šifriranja lahko sporočila tudi skrijemo, tako da niso vidna našim očem (npr. skrivanje v slike, v zvočne ali tekstovne datoteke). S tem se ukvarja steganografija (ang. steganography). Metoda se v večji meri uporablja pri digitalnem vodnem tisku ali za označevanje datotek z digitalnimi serijskimi številkami (Kovačič, 2003: 68).
Zelo učinkovito zaščito podatkov dobimo s kombinacijo kriptografije in steganografije, in sicer tako, da sporočilo najprej šifriramo, potem pa ga še skrijemo.

3.3 KRIPTOANALIZA

Beseda kriptoanaliza je grškega izvora kryptós (skrito) in analýein (ang. loosen – razrešiti, 'razbiti') in je del kriptologije. Kriptoanaliza je veda o pridobivanju podatkov, ki so bili zavarovani s kriptografsko metodo. Ko govorimo o kriptoanalizi, govorimo lahko o kriptografovem neuspehu in kriptoanalitikovem uspehu (Encyclopaedia Britannica 2005 Deluxe Edition: Elektronska izdaja: United Kingdom). Pri kriptoanalizi gre za matematične tehnike, s katerimi poizkušamo 'razbiti' kriptografski sistem in tako dešifrirati podatke oziroma besedilo brez ustreznega ključa (http://en.wikipedia.org/wiki/Cryptanalysis, 21. 12. 2005). Natančneje, kriptoanaliza je razbijanje kriptosistemov in napadi nanje, kot je iskanje vsebine sporočil brez vednosti ključa ter iskanje zasebnih ključev iz javnih (Jurišić in Tonejc, 2001: 58).
Cilj kriptoanalize je:

- analiza 'čvrstosti' kriptografskega sistema;
- vdiranje oziroma 'razbijanje' kriptografskega sistema (ang. code-breaking).

(Kovačič 2001: 7)
Buchmann opredeljuje Kriptoanalizo kot tehniko, s katero 'napadamo' (ang. attack) oz. 'razbijamo' kriptosisteme in je področje na katerem 'napade' razvrščamo v različne skupine (Buchmann, 2000: 71).

V uradnem listu EU je kriptoanaliza opredeljena kot*: »/a/naliza kriptografskega sistema ali njegovih vhodov in izhodov zaradi zakrivanja zaupnih spremenljivk ali občutljivih podatkov, vključno z odprtim besedilom.«* (Uradni list EU, Uredba Sveta (ES) št. 394/2006: 74/10).

3.4 NACIONALNA VARNOST

Za lažje razumevanje bom najprej opredelila pojem varnosti v ožjem in širšem smislu ter podobnosti in razlike med državno in nacionalno varnostjo.

Pojem varnosti predstavlja celo vrsto različnih vidikov človekovega obstoja in delovanja v družbi in naravi. Posega na vsa področja človekovega delovanja in v vse njegove aktivnosti. Je stanje, v katerem je zagotovljen uravnotežen fizični, duhovni in duševni ter gmotni obstoj posameznika in družbene skupnosti v razmerju do drugih posameznikov, družbenih skupnosti in narave (Grizold, 1999: 23). Anžič opredeli varnost kot družbeno in politično vrednoto, ki označuje okvir socialne in politične skupnosti. Omogoča obstoj družbene reprodukcije, notranji red in mir in razvoj notranje ureditve (Anžič: 2001: 33).

Nacionalno varnost opredelimo kot varnost naroda oziroma nacije v neki državi in kot sposobnost zaščite države in njenega ozemlja, ohranjanje gospodarskih odnosov z drugimi državami, varnost življenja ljudi in njihove lastnine, ohranitev nacionalne suverenosti ter uresničevanje temeljnih funkcij družbe (Grizold, 1999: 25). Gre za prizadevanje države, da vsem članom družbe zagotovi varnost pred zunanjim ogrožanjem (posegi, napadi, okupacijo, blokado, množičnimi migracijami) in znotraj družbe (ogrožanjem reda in miru, kriminalom, asocialnim in patološkim ravnanjem) (Grizold, 1992: 65 v Svete, 2005: 66).

Harold Brown (v Grizold, 1999: 25) opredeli nacionalno varnost kot sposobnost zaščite fizične integritete države in njenega ozemlja, ohranjanja gospodarskih odnosov z drugimi državami pod razumnimi pogoji, zaščite narave države, institucij in vodstva pred zunanjim ogrožanjem ter sposobnost nadzora državnih meja. *»/N/obilo opredeljuje nacionalno varnost kot zapleteno interakcijo političnih, ekonomskih, vojaških, ideoloških, pravnih, socialnih in drugih notranjih in zunanjih družbenih dejavnikov«* (Nobilo, 1988: 72,73 v Čas 2005: 5).

V praksi se pojma državna varnost in nacionalna varnost prepletata in pogosto izenačujeta. Pojem varnosti v državni varnosti ima dva pomena: državna varnost je stanje varnosti na celotnem ozemlju države oziroma v nacionalni varnosti in drugič je dejavnost, s katero država sistemsko zagotavlja varnost na ravni celotne družbe (Grizold, 1999: 26).

4 ZGODOVINA KRIPTOGRAFIJE IN KRIPTOANALIZE

V tem poglavju na kratko predstavljam zgodovino kriptologije (kriptografija + kriptoanaliza), ki jo za boljši pregled razdelim v tri razvojne faze in vsako podrobneje opišem in analiziram. Zgodovinski pregled poizkušam oblikovati tako, da je razvidno, kdaj se je kriptologija uporabljala v državne in kdaj v civilne namene.

Skrivanje besednih zvez v različne znake se je razvilo že s samim razvojem pisave. Prvi dokazi so bile čisto naključne uganke, ki so si jih ljudje preprosto izmišljevali. Kriptologija se je skozi svojo bogato in zanimivo zgodovino razvila iz preproste kriptologije (svinčnik, papir, človeški spomin) z le nekaj simboli, vse do zapletene in visoko strukturirane kriptologije – zmogljivi računalniški sistemi. Metode kriptografije in kriptoanalize so se skozi zgodovino razvijale vzporedno.

Tri razvojne faze kriptologije[4] (kriptografija + kriptoanaliza):

- **kriptologija pred in med prvo svetovno vojno**: za to obdobje je značilna t.i. 'ročna' kriptologija, katere prve zapise najdemo v antiki in se je uporabljala vse do prve svetovne vojne. Katera tehnika kriptologije se je uporabljala, je bilo popolnoma odvisno od pisarja in njegove domišljije ter iznajdljivosti. Posledica tega je bila, da so bili tajnopisi sestavljeni le iz nekaj sto črk, številk ali znakov;
- **kriptologija po prvi svetovni vojni**: v tem obdobju se je začela kriptologija 'mehanizirati' oziroma za šifriranje in dešifriranje še danes uporabljajo temu primerne stroje in računalnike. Kriptologija se je razvijala vzporedno s tehnologijo (telefon, telegraf, računala). Z razvojem rotorja pa je postalo

[4] V tem poglavju pogosto zamenjujem besedi kriptografija in kriptoanaliza z besedo kriptologija. Pri razvoju in uporabi kriptografije in kriptoanalize je pogosto težko ločiti mejo med eno in drugo.

šifriranje in dešifriranje hitrejše, lažje in bolj natančno. Tajnopisi so obsegali na tisoče znakov, danes že na bilijone;

- **kriptologija v zadnjih 20-ih letih:** bistvena sprememba v tem obdobju je velika uporaba kriptologije v informacijski tehnologiji (digitalni podpis, dokaz pristnosti). V tem obdobju se razvila tudi kriptografija z uporabo javnih ključev (ang. public-key cryptography). (Encyclopaedia Britannica 2005 Deluxe Edition: Elektronska izdaja: United Kingdom).

4.1 KLASIČNA KRIPTOGRAFIJA IN KRIPTOANALIZA

Prvi zapisi kriptografije so stari že več kot 4500 let in izvirajo iz **Egipta**. Začetki kriptografije so popolnoma nenačrtovani in preprosti, saj so pisarji besedne igre sestavljali zato, da so med seboj tekmovali in se igrali. 2000 let kasneje so v **Mezopotanij** na glinene tablice že pisali kriptografske zapise, in sicer kako izdelati lončarske posode. **Hebrejci** so uporabljali sistematično metodo šifriranja *temurah* (zamenjava). Abecedo so razdelili na dva dela ter ju v obrnjenem vrstnem delu zapisali enega pod drugim (500–600 let pred našim štetjem). Samo nekaj let kasneje v **Grčiji** vojaški pisec napiše priročnik, v katerem je poglavje o skrivnih pisavah, **Špartanci** pa so prvi, ki izumijo mehanski pripomoček za pošiljanje sporočil, in sicer leseni valj, imenovan *'skytale'* – skital. Uporabljal se je tako, da so na valj navili pergament, nanj pa napisali sporočilo, ga odvili in poslali. Prejemnik je pergament zopet navil na valj in tako prebral sporočilo (400 let pred našim štetjem). Metoda se imenuje transpozicija, kar pomeni, da so črke ostale iste, le njihov vrstni red je drugačen. Kriptologija se je prvič uporabila v **vojaške namene**.

Slika 4.1: Skital

Vir: http://global.mitsubishielectric.com/misty/tour/stage1/, 5. 1. 2006

Julij Cezar je bil prvi, ki je šifrirna sporočila uporabil **v državne namene** oziroma za **meddržavno komuniciranje**. Vsako črko je zamenjal s črko, ki v abecedi leži tri[5] mesta pred njo. To metodo imenujemo substitucija ali zamenjava.
Dobro je poznana tudi indijska kriptografija, ki je opisna v knjigi Kama Sutra, in sicer kako naj se ljubimci pogovarjajo v šifrah, da jih drugi ne bi odkrili (0–400 našega štetja).

Slika 4.2: Transformacijska tabela

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Vir: http://cse.unl.edu/~bholley/Cypher%20Tutorial.html, 5. 1. 2006

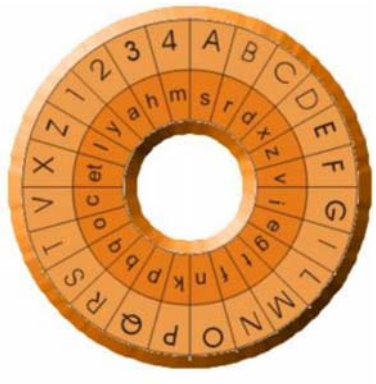
Po tej metodi bi se stavek »***VRNITE SE V RIM***«, glasil »***YUQLWH VH Y ULP***«.

4.2 KRIPTOGRAFIJA IN KRIPTOANALIZA V SREDNJEM VEKU

Srednji vek je prinesel veliko novosti. Odkrili so metodo za dešifriranje monoalfabetske substitucije, ki se je imenovala metoda frekvenčne analize[6]. Kriptografija dobi v tem obdobju velik pomen zaradi političnih nasprotij in verskih revolucij. Prvi, ki so razumeli načela in pravila kriptografije in kasneje interpretirali kriptoanalizo, so bili **Arabci**. Leta 1412 napiše al Qalqashandi (Al Kalkašanadi) enciklopedijo z naslovom »Subh al-a sha« (Sub al Saša). V enciklopediji opiše več vrst šifriranja, za katere je najbolj primeren nepoznan jezik in opiše tudi že tehnike dešifriranja. V tem času **Evropa** hitro napreduje, zasluge za razvoj kriptografije pa gre pripisati različnim italijanskim mestnim državam, papeški državi in tudi Rimskokatoliški cerkvi. Leta 1470 je **Leon Battista Alberti** napisal esej, v katerem je podrobno opisal sisteme šifriranja. Izumil je novo napravo za šifriranje, t. i. dvojno ploščo z vrtljivim srednjim delom, ki je temeljila na polialfabetskemu sistemu. Metoda se je uporabljala celih pet stoletij, med drugim jo je uporabljala ameriška vojska med prvo svetovno vojno.

[5] Število, ki nam pove, za koliko znakov smo zamaknili abecedo, označimo s črko K in predstavlja ključ za šifriranje in dešifriranje sporočila. Če si izberemo K=3, namesto črke A v sporočilu pišemo tako črko C, namesto črke B črko D in tako vse do črke Ž, ki nam predstavlja črko Č (Jurišić, Perko, Presek, letnik 33., št. 1, str. 22–24).
[6] Frekvenčna analiza temelji na lastnosti jezika, pri kateri se v tekstih nekatere črke pojavljajo bolj pogosto kot druge. Črke in glasovi ne nastopajo enako pogosto in se pojavljajo samo v določenih kombinacijah. To pomeni, da lahko neko besedo tudi uganemo, čeprav ne poznamo vseh črk, ki jo sestavljajo (http://www.sigov.si/tecaj/kripto/kr-entropija.htm, 5. 1. 2006).

Slika 4.3: Dvojna plošča z vrtljivim srednjim delom



Vir: http://www.riksoft.com/indexok.asp?Goto=crileon.htm, 5. 1. 2006

Blaise de Vigenère je leta 1586 v delu Traicté des Chiffres opisal najbolj znano polialfabetsko metodo, ki z razliko od prejšnje uporabil še ključ. Pomembno vlogo v kriptografiji ima tudi **Thomas Jefferson**, ki je leta 1970 iznašel novo šifrirno metodo, t. i. šifrirno kolo. Metodo je kasneje uporabljala ameriška mornarica v drugi svetovni vojni.

4.3 KRIPTOGRAFIJA IN KRIPTOANALIZA MED 1800 IN DRUGO SVETOVNO VOJNO

Čeprav ima kriptografija dolgo zgodovino so se potrebe in zahteve po njej vse do 19. stoletja razvijale in reševale samo začasno in kratkoročno. S hitrim razvojem kriptoanalize so bile tehnike in metode kriptografije hitro odkrite in s tem tudi ranljive. Leta 1861 je **Friderich W. Kasiski** objavil knjigo, v kateri je opisal kriptoanalizo polialfabetskega šifriranja in tako je bila odkrita metoda za šifriranje, ki se je uporabljala več stoletij. Približno 50 let kasneje je ameriška vojska izdelala šifrirni algoritem, imenovan **One Time Pad** ali **OTP**, ki je veljal za nezlomljivega in je še danes eden od varnejših šifrirnih algoritmov. Algoritem je izboljšana verzija Vigenèreve tabele, ki je statična, OTP-jeva pa se spreminja, vendar je le za enkratno uporabo http://en.wikipedia.org/wiki/One-time_pad, 5. 1. 2006). Med prvo svetovno vojno so prevladovale matematične tehnike šifriranja in dešifriranja, vidnejšega napredka ni bilo.

4.4 KRIPTOGRAFIJA IN KRIPTOANALIZA MED DRUGO SVETOVNO VOJNO

Z razvojem mehanike in elektromehanike se je razvijala tudi kriptologija, ki ni bila več samo domena vojaške strategije, temveč je vedno bolj postajala orodje politike in tajnih organizacij. Najvidnejši napredek na področju kriptografije je bil izum kolesnega sistema šifriranja. S tem napredkom je bila kriptoanaliza za nekaj časa ohromljena.

V času druge svetovne vojne je bil najbolj poznan nemški šifrirni stroj **ENIGMA**, ki je bil patentiran leta 1918. Enigma je električna naprava za šifriranje sporočil in je podobna pisalnemu stroju. Stroj je sestavljen iz baterije, tipk za črke kot pri pisalnem stroju, luči za vsako črko in šifrirnega mehanizma iz štirih okroglih ploščic, ki so jih imenovali rotorji (http://www.sigov.si/tecaj/kripto/enigma.htm, 6. 1. 2006).

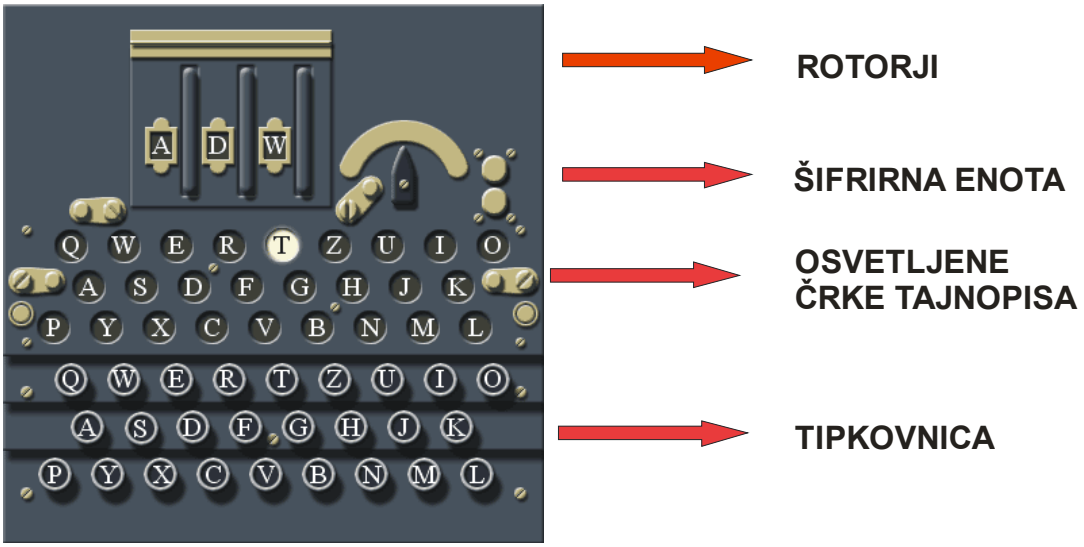
Slika 4.4: Pomorska Enigma s štirimi valji, razstavljena v Bletchley Parku

Vir: http://sl.wikipedia.org/wiki/Enigma_%28naprava%29, 6. 1. 2006

Vsaka posamezna črka čistopisa se je vnašala prek tipkovnice, ta pa se je preko zaporednih rotorjev zakodirala. Povraten električni signal je osvetlil zakodirano črko tajnopisa (Živec, 2005: 13). Vojak je sporočilo šifriral tako, da je vtipkal posamezno črko in zapisal črko, ki se mu je osvetlila. Prejemnik šifriranega sporočila je moral imeti stroj, ki je imel enake rotorje kot pošiljateljev

(vsak rod vojske je imel svoje kombinacije). Vsak dan so tako spreminjali vrstni red kot tudi začetne položaje rotorjev. Nemci so menili, da tako šifriranih podatkov ni mogoče dešifrirati (http://www.sigov.si/tecaj/kripto/enigma.htm, 6. 1. 2006).

Slika 4.5: Osnovna zgradba Enigme



Vir: http://maettig.com/?page=Studium/Enigma, 6. 1. 2006

Projekt '*Ultra*', ki je potekal v angleškem Bletchley Parku, je bil strateško zelo pomemben in je imel velik vpliv na razplet druge svetovne vojne. Angležem je uspelo pod vodstvom Alana Turinga[7] odkriti šifrirni algoritem in tako razbiti kodo Enigme. V veliko pomoč so jim bile informacije, ki so jih dobili od poljskega matematika Mariana Rejewskega, ki je na podlagi skic dobljenih od francoskih obveščevalcev, uspel odkriti dnevne ključe (Živec, 2005: 14).

Na splošno velja, da je razbitje šifre Enigme pomembna strateška prednost zaveznikov in da je to skrajšalo vojno za nekaj mesecev. Iz tega lahko sklepamo, da sta bili kriptografija in kriptoanaliza pomembna dejavnika med drugo svetovno vojno in pomembno je, da so zavezniki vso vojno in do 70. let ohranili popolno tajnost o 'zlomu' Enigmine šifre (http://sl.wikipedia.org/wiki/Enigma_%28naprava%29, 6. 1. 2006).

[7] **Alan Mathison Turing**, angleški matematik in kriptograf (1912–1954).

Med drugo svetovno vojno so se uporabljali tudi drugi sistemi šifriranja. Japonska vojska je uporabljala šifrirni sistem JN-25, Velika Britanija je uporabljala stroje imenovane TypeX in Amerika stroje SIGABA. Tudi v drugih državah je kriptologija dobila v času druge svetovne vojne velik pomen in tako so države v ta namen zaposlovale strokovnjake običajno matematike, da so odkrivali nove metode šifriranja in dešifriranja. Zelo pomembna je postala kriptoanaliza, kajti države so si vedno bolj prizadevale ugotoviti skrivne namene drugih držav. Velika Britanija in ZDA sta po koncu vojne v ta namen prodali del šifrirnih naprav na Bližnji Vzhod in v Afriko, da sta lahko brali radijski promet drugih držav (http://sl.wikipedia.org/wiki/Enigma_%28naprava%29, 6. 1. 2006).
Do obdobja moderne kriptologije oziroma do približno 1970. leta se je kriptologija uporabljala predvsem v državne namene.

4.5 MODERNA KRIPTOGRAFIJA IN KRIPTOANALIZA

Moderna kriptografija in kriptoanaliza temeljita skoraj izključno na računalniških programih, kar pomeni obdelavo na nivoju strojnega jezika. Z uporabo računalnikov so se razvile nove zapletene in visoko strukturirane metode šifriranja in dešifriranja. Danes so nam na voljo kriptosistemi z eliptičnimi krivuljami (ang. Elliptic Curve Cryptosystem – ECC), katerih glavna prednost so krajši ključi (npr. 160 bitov za isto varnost kakor 1024-bitni RSA).
Claude Shannon je 'oče' matematične kriptografije in lahko rečemo, da se je z njegovim delom leta **1949 Communication Theory of Secrecy Systems** začelo obdobje moderne kriptologije. Njegova druga dela v zvezi z informacijskimi in komunikacijskimi teorijami pa so temelj današnji kriptografiji in kriptoanalizi.
Kriptologija se je uporabljala samo za skrite akcije vladnih organizacij, kot je na primer NSA in se v javnosti ni pojavila vse do leta 1976, ko se je vse spremenilo. Na nadaljnji razvoj kriptografije in kriptoanalize sta vplivala predvsem dva dejavnika: objava standardnega kriptografskega algoritma in sistem distribuiranja javnih ključev.

4.5.1 Standardni kriptografski algoritem

17. marca 1975 je bil objavljen DES (Data Encryption Standard)[8], ki ga je razvil in patentiral IBM in je izpeljanka enkripcijskega algoritma Lucifer, ki ga je uporabljala ameriška[9] vojska. Namen tega je bil povečati varnost komunikacij. Leta 1976 je bil sprejet kot standardni kriptografski algoritem v ZDA. DES je kasneje nadomestil AES (Advanced Encryption Standard) in leta 2000 izbran algoritem Rijndael.

Leta 2004 je NIST (National Institute of Standards and Technology) objavil, da se DES s 56-bitnim[10] ključem ne bi več uporabljal, ker naj bi bil ranljiv. Leta 2005 je NIST umaknil vse standarde v zvezi DES, ki so bili v uporabi tri desetletja (http://www.sigov.si/tecaj/kripto/DES.htm, 7. 1. 2006).

4.5.2 Javni ključ

Leta 1976 so se spremenili temelji delovanja kriptosistema, in sicer se je uveljavila popolnoma nova metoda »distributing cryptographic keys«, izmenjava kriptografskih ključev.
Sprva se je uporabljala samo simetrična kriptografija, pri kateri se uporablja isti ključ tako za šifriranje kot dešifriranje. Pri tem nastane težava, kako varno izmenjati ključ med pošiljateljem in prejemnikom. Problem je rešila Diffie-Hellmanova[11] izmenjava ključev, temelječa na asimetričnem algoritmu, ki uporablja dva ključa – javnega in zasebnega. Javni ključ (ang. public key) je eden od dveh šifrirnih ključev v asimetričnem kriptosistemu. Ključ je javno objavljen in ga lahko uporabljajo vsi.

---

[8] Najbolj razširjeni algoritem po drugi svetovni vojni je bil DES in je uporabljal 56-bitne ključe, kar pomeni 2^{56} možnosti za izbiro ključa. Računalniki so postajali vse hitrejši, tako so ga leta 2000 nadomestili z AES, ki uporablja ključe dolžin 128, 196 in 256 bitov (Jurišić, Perko, Presek, letnik 33., št. 1, str. 22–24).

[9] Velika verjetnost je, da je vojska poznala bližnjico za razbitje civilne enačice DES (Vidmar 1997: 179 v Kovačič 2003: 73).

[10] »**Bít** je osnovna in hkrati najmanjša, nedeljiva enota informacije, ki se uporablja v računalništvu. En bit (ime *bit* izhaja iz angleškega izraza »*binary digit*«) predstavlja neko informacijo o opazovanem objektu, ki je lahko 1 ali 0 ali katerikoli dve drugi, medsebojno izključujoči se, stanji« (http://sl.wikipedia.org/wiki/Bit, 7. 1. 2006).

[11] Leta 1976 je izšel članek z naslovom »New Directions In Cryptography«, ki sta ga napisala matematika Whitfield Diffie in Martin E. Hellman. »V članku sta opisala protokol za varno izmenjavo ključev prek nezaščitenega medija in tako je nastala zamisel o sistemu šifriranja z javnimi ključi« (Kovačič, 2003: 9).

Leta 1977 so Ronald. L. Rivest, Adi Shamir in Leonard M. Adleman objavili članek z naslovom *»A Method for Obtaining Digital Signature and Public-kay Cryptosystems«*, kjer je bil opisan nov šifrirni algoritem, ki naj bi temeljil na sistemu javnih ključev in omogočal tudi digitalno podpisovanje. Algoritem so poimenovali po začetnicah avtorjev RSA. Kasneje se je izkazalo, da je algoritem RSA izjemno zmogljiv, kar pomeni, da sporočil, ki so bila šifrirana s tem algoritmom, ni bilo lahko razbiti (Kovačič 2003: 9–10)

Kriptografija se je začela v javnosti uporabljati po letu 1991, ko je Phil Zimmermann objavil PGP[12] (Pretty Good Privacy). PGP je standard šifriranja, ki temelji na javnih in privatnih ključih in se uporablja za šifriranje elektronskih sporočil in računalniških aplikacij. V programu PGP je implementiran RSA algoritem (Kovačič 2003: 10).

5 METODE IN TEHNIKE UPORABE KRIPTOGRAFIJE IN KRIPTOANALIZE

4.1 OSNOVNE LASTNOSTI KRIPTOSISTEMOV

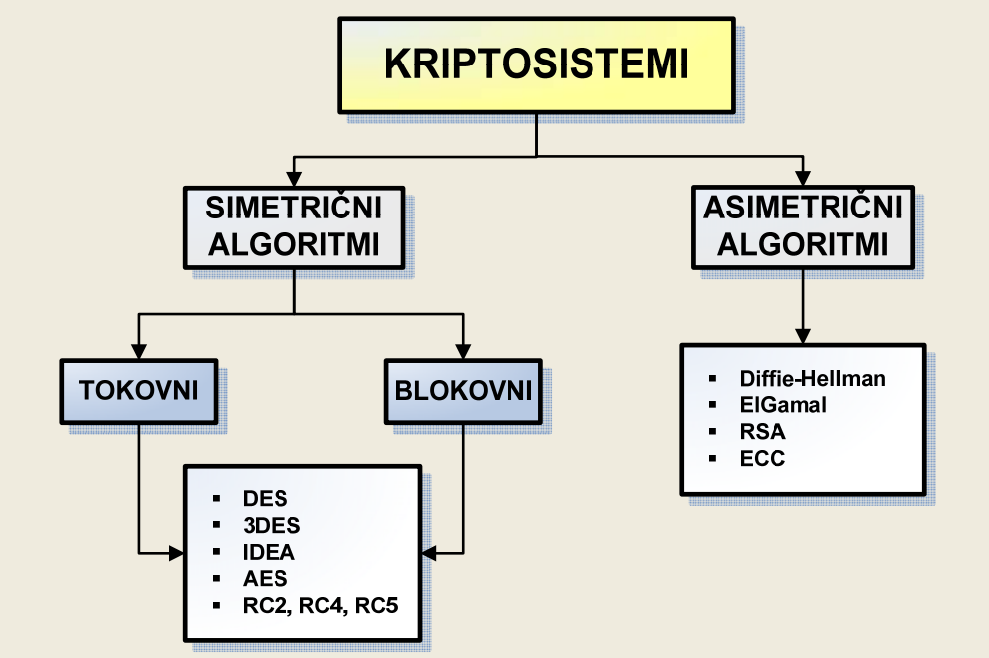
Kriptosistem je algoritem[13] oziroma poljubna šifra, ki poda pravila za preoblikovanje podatkov in se uporablja za šifriranje ali dešifriranje. Vsak kriptosistem ima dve osnovni funkcijski enoti – šifrirni algoritem[14] in ključ. Običajno so kriptosistemi odvisni od vsaj enega skrivnega parametra – npr. ključa. Kriptosistemi se delijo na simetrične (zasebni ključ) in asimetrične (javni ključi) algoritme (Jurišić in Tonejc, 2001: 59). Algoritem določa, kako se podatki preoblikujejo, ključ pa nam zagotavlja različen potek šifriranja za različne uporabnike (http://www.it-akademija.net/kodiranje.pdf, 10.1. 2005). Kriptosistem lahko v praksi realiziramo na dva načina: kot samostojno programsko opremo ali kot samostojno strojno opremo.

[12] Ameriški senat je obravnaval zakon, ki bi močno omejil uporabo kriptografije v javni in zasebni sferi. Phil Zimmerman je v ta namen program PGP javno objavil na medmrežju in dovolil njegovo brezplačno kopiranje (če bi bil zakon sprejet, bi s tem izničil njegove učinke). Program se je v zelo kratkem času razširil po celem svetu (Kovačič, 2003: 10).

[13] Algoritem je navodilo, ki določa vrsto in zaporedje operacij v računskem postopku (SSKJ 2002, elektronska izdaja v 1.0).

[14] Šifrirni algoritmi se uporabljajo za matematično transformacijo berljivih ali preprosto prepoznavnih podatkov (čistopis) v šifrirane podatke (tajnopis) in obratno (Zidar 2003: 1).

Slika 5.6: Kriptosistemi



Vir: Prirejeno po http://www.sigov.si/tecaj/kripto/kr-sim.htm, 10. 1. 2006

5.1.1 Simetrični algoritmi

Simetrični algoritem[15] ali algoritem z zasebnim ključem uporablja samo en ključ, s katerim šifriramo in dešifriramo sporočilo. To pomeni, da se morata uporabnika najprej dogovoriti, kateri ključ bosta za zaščiti uporabljala. Običajno so ti algoritmi hitri, težko pa je ključ varno izmenjati. Ker podatke izmenjujemo z več dopisovalci in strežniki, problem predstavlja tudi upravljanje s ključi. Problem rešuje asimetrična kriptologija, ki temelji na uporabi različnih ključev (glej poglavje 5.1.2) (Jerman Blažič, 2004: 61).

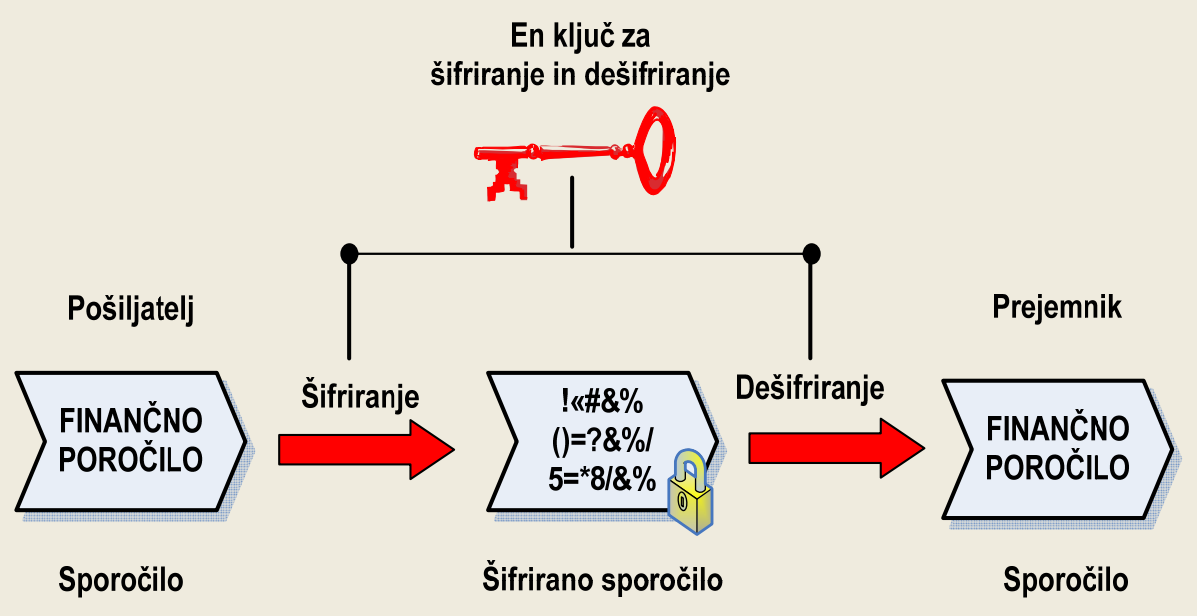
Danes se simetričen algoritem uporablja predvsem pri uporabniških programih, ki nam nudijo zaščito dokumentov, namenjenih osebni rabi, kjer ključ poznamo samo mi (Word, Excel).

Simetrične algoritme delimo na :

- **blokovne** – tekoče šifriranje – sporočilo šifriramo bit za bitom (stream ciphers);
- **tokovne** - sporočilo razbijemo na bloke in vsak blok posebej šifriramo (block ciphers) (http://www.sigov.si/tecaj/kripto/kr-sim.htm, 10. 1. 2006).

[15] Tudi simetrična šifra.

Slika 5.7: Simetrični algoritem



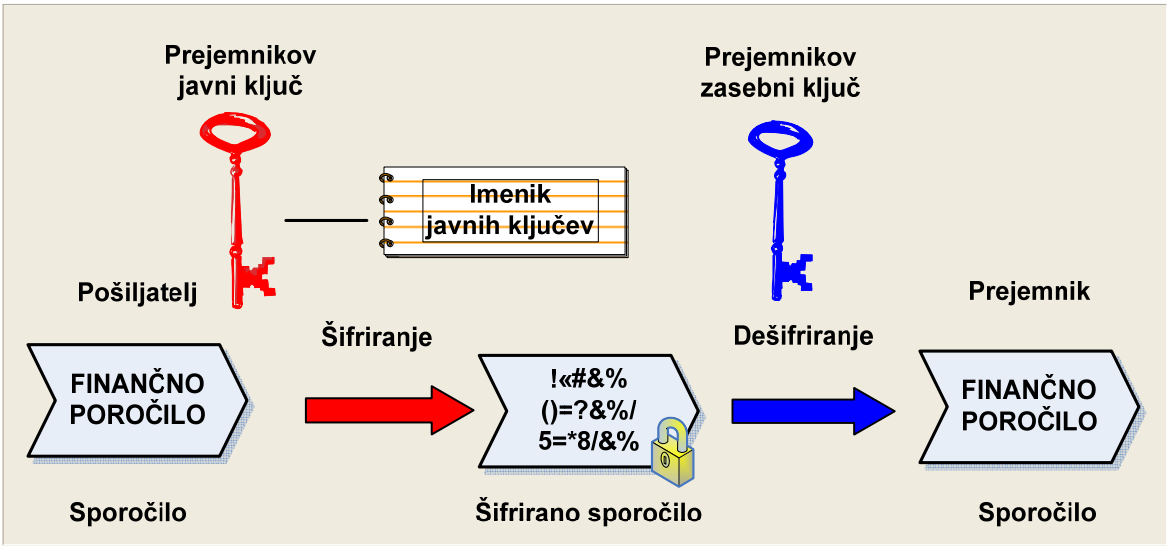
Vir: Prirejeno po Schneier, 1996: 15

5.1.2 Asimetrični algoritmi

Asimetrični algoritem je kriptografski algoritem, ki uporablja različne matematične ključe za šifriranje (enkripcijo) in dešifriranje (dekripcijo) Uradni list EU, Uredba Sveta (ES) št. 394/2006: 74/10).

Asimetrični algoritem ali algoritem z javnim ključem z razliko od simetričnega sistema uporablja dva različna ključa, zasebnega in javnega. Tu ima za razliko od simetričnega sistema vsak uporabnik po dva ključa, en ključ podatke šifrira (zaklepa), drugi pa jih dešifrira (odklepa). Pomembna lastnost tega sistema je, da ključ, ki podatke zaklene, teh ne more odkleniti in obratno. Tak sistem lastniku omogoča, da en ključ objavi, drugega pa hrani v tajnosti. Asimetrični algoritmi poleg šifriranja in dešifriranja omogočajo tudi digitalno podpisovanje, kar pomeni, da prejemnik točno ve, kdo mu je sporočilo poslal.

Slika 5.8: Asimetrični algoritem



Vir: Prirejeno po Schneier, 1996: 15

5.1.3 Primerjava simetričnega in asimetričnega algoritma

Simetrični algoritmi:

- zasebni ključ;
- en ključ;
- hitrost;
- primerni za zaščito shranjenih osebnih podatkov;
- problem z varno izmenjavo ključa med pošiljateljem in prejemnikom;
- problem pri kopičenju ključev, kadar imamo več sogovornikov in za vsakega potrebujemo nov ključ;
- primeri algoritmov: DES (Data Encryption Srandard)
    - dolžina ključa 56 bitov
    - AES (Advanced Encryption Standard)
    - dolžina ključa 128, 192, 256 bitov
    - IDEA (International Data Encryption Algorithem)
    - dolžina ključa 128 bitov

(http://www.it-akademija.net/kodiranje.pdf, 12. 1. 2005).

Asimetrični algoritmi:

- javni ključ in je ponavadi objavljen v javnem imeniku;
- dva ključa (javni in zasebni) in sta enoumno povezana;
- počasnost;
- enostavna izmenjava ključev;
- število ključev narašča po linearnem zaporedju,
- kompleksnost algoritmov;
- primeri algoritmov: RSA
    - dolžina ključa 512, 768, 1024, 2048, 3072, 4096
    - Diffie-Hellman
    - dolžina ključa 512, 768, 1024, 2048

(http://www.it-akademija.net/kodiranje.pdf, 12. 1. 2005).

Težko govorimo kateri algoritem je boljši in varnejši, pomembno je, da pri izboru kriptosistemov poznamo prednosti in slabosti obeh pristopov. V modernih kriptosistemih se oba algoritma dopolnjujeta, saj ima tako en kot drugi dobre lastnosti in tako vsak zagotovi določeno varnostno funkcijo (Zidar, 2003: 3).

5.2 UPORABA KRIPTOSISTEMOV

Splošno lahko rečemo, da kriptosisteme uporabljamo v odprtih in zaprtih sistemih. Kadar govorimo o **odprtih sistemih,** se uporabljajo standardizirani in javno objavljeni šifrirni algoritmi. Prvi standardizirani šifrirni algoritem je bil DES, ki je bil implementiran v veliko različnih aplikacij, v začetku predvsem na bančnem področju. Čeprav ima DES kar nekaj pomanjkljivosti, je njegova uporaba še danes zelo razširjena. Kasneje je bi razvit AES, ki ima višji nivo varnosti, danes pa imamo poleg standardiziranih algoritmov še precej drugih, ki jih je mogoče uporabiti pod licenčnimi pogoji.

Kadar govorimo o **zaprtih sistemih,** imamo možnost izbire kriptosistemov, ker komunikacija poteka v zaprtih krogih, ki so nadzorovani in kjer ni možnosti za aktivno vključitev v komunikacijski krog. Ko govorimo o zaprtih sistemih, mislimo predvsem na vladne organizacije, kot so informacijski sistemi, tajne službe in tiste organizacije, ki so pomembne za **nacionalno varnost**. Prioriteta v teh sistemih je tajnost komunikacij. V zaprtih sistemih se moramo sami odločiti,

katero vrsto šifrirnega algoritma bomo uporabili; na razpolago imamo dva možna pristopa: lasten razvoj ali nakup. Če poznamo kriptografsko področje dovolj dobro, lahko uporabimo šifrirni algoritem, ki je že objavljen, ali pa sami razvijemo novega. Pri nakupu imamo možnost kupiti javno objavljeni šifrirni ali tajni algoritem, ki je proizvod ponudnika in interne strukture, njegove matematične podlage pa niso nikjer objavljene (Zidar, 2003: 3).

Pri uporabi šifriranja je zelo pomembno, katero kriptografsko metodo bomo uporabili. Uporaba šibkih in nepreverjenih kriptografskih metod nam lahko daje občutek varnosti, vendar to še ne pomeni, da nam jo tudi zagotavljajo. Veliko šifrirnih algoritmov je bilo razvitih v ameriških državnih organih (npr. National Security Agency, NSA), za katere velja, da niso tako varni, kot je videti na prvi pogled. Veliko metod razvijajo majhna in nepoznana podjetja, ki to delajo v tajnosti in tako v njihovo zanesljivost ni mogoče zaupati. Problem je v tem, da metode niso bile javno preizkušene. V kriptografiji namreč velja pravilo, da morajo biti vse kriptografske metode javno objavljene in jih morajo preizkusiti tudi vodilni kriptoanalitiki (Kovačič 2003: 66). Tako moramo pri izbiri kriptografske metode paziti, kdo jo je razvil in ali je bila preizkušena ter javno objavljena. Enako velja za kriptografske sisteme.

6 VZROKI UPORABE KRIPTOGRAFIJE IN KRIPTOANALIZE

Odgovor na vprašanje, zakaj se je kriptografija sploh začela uporabljati za zaščito informacij in podatkov, je enostaven in preprost: zaradi človeške radovednosti. Radovednost in želja sta lastnosti vsakega posameznika in če se pojavita v preveliki meri, lahko ogrožata pomembne informacije in podatke.
Odkar so ljudje začeli komunicirati (govor, pisava, televizija, telefon, računalnik), so želeli skriti vsebino sporočil. Ljubimci, vohuni, vojska in ostali že od nekdaj pošiljajo šifrirana sporočila. Ker pa so se razvile tudi tehnike in metode za razbijanje šifrirnih sporočil, so le ta tudi pogosto nepravilna in zavajajoča.
Kriptologija je skozi zgodovino postajala vedno bolj popularna na vojaškem in nacionalnem področju. Z razvojem moderne kriptologije, ki je postala matematična in računalniška disciplina, pa je prodrla na področja, kot so:

politika, gospodarstvo, socialna družba in druga. Pretok informacij med področji se je povečal, tako je postalo varovanje informacij in podatkov osnovna zahteva uporabnikov. Varnost podatkov ni pomembna samo za vojske in tajne organizacije, temveč tudi za industrijske obrate, banke, trgovske mreže, patentne pisarne, šole, telekomunikacijska podjetja in še bi lahko naštevali.
S prehodom v informacijsko družbo je postala informacija osnovna dobrina, znanje o informacijski tehnologiji dostopno, komunikacijska tehnologija pa dovolj razvita za odprt pretok in dostop do informacij in komunikacij.
Danes se kriptografija uporablja skoraj na vseh področjih našega življenja, vedno bolj pa je prisotna tudi v zasebnem življenju (GSM telefoni, bančne in zdravstvene kartice, računalniki). Obseg in uporaba kriptografije, kriptoanalize in seveda tudi drugih sorodnih tehnik in metod stalno narašča. Vzrokov za uporabo kriptologije je več: informacijska varnost, zaščita tajnih podatkov, računalniška varnost, celovitost, identifikacija oseb, avtentičnost, nezmožnost zavrnitve (internet in uporaba elektronske pošte), zaupnost, anonimnost itn.
V nadaljevanju opisujem in analiziram dva najpomembnejša vzroka uporabe kriptologije: informacijsko varnost in zaščito ter varovanje tajnih podatkov.

6.1 INFORMACIJSKA VARNOST

»/l/nformacijska varnost pomeni vsa sredstva in funkcije, ki zagotavljajo dostopnost, zaupnost ali celovitost informacij ali komunikacij, razen sredstev in funkcij varovanja pred napačnim delovanjem.« Uradni list EU, Uredba Sveta (ES) št. 394/2006: 74/10). V Uradnem listu EU je opredeljeno še, da v to področje sodijo kriptografija, kriptoanaliza, zaščita pred odtekanjem podatkov in računalniška varnost.
Kaj je informacija? To so podatki, pomembni za odločanje (Shannon, Weaver v Žumer: http://www.ff.uni-lj.si/oddelki/biblio/ uvinfznan . htm, 20. 1. 2006).
Današnja družba je neločljivo povezana s pojmom informacijska družba in to je družba, v kateri je informacija najpomembnejša tržna dobrina (http://www. ltfe. org/pdf/Varnost%20v%20telekomunikacijah.pdf, 20. 1. 2006).
S hitim razvojem informacijske tehnologije na različnih področjih, predvsem tistih, ki so upravne ali poslovne narave, se vedno znova postavljajo nova varnostna vprašanja in problemi. Informacije se danes v večji meri shranjujejo v

elektronski obliki, kar prinaša veliko prednosti, vendar s tem tudi slabosti (Jerman Blažič, 2004: 60). S slabostmi mislim predvsem na to, da če jih ustrezno ne zavarujemo, postanejo ranljive. Tukaj pride na vrsto šifriranje informacij in podatkov, kjer lahko uporabljamo simetrične in asimetrične algoritme.

Varnostna aplikacija mora zagotoviti: zaupnost, celovitost, overjanje, preprečevanje tajenja in kontrolo dostopa (Menezes, J. Alfred, van Oorschot, C. Paul, Vanstone, A. Scott (1997: 4). Rešitev za to nam ponuja kriptografija. To lahko zagotovimo s podpisovanjem sporočil[16] (digital signtures) in z overjenim javnim ključem. Sporočilu lahko dodamo še digitalno potrdilo (digital certificate), v katerem so zapisani čas nastanka sporočila, podatki o lastniku, rok veljavnosti itn.

6.1.1 Digitalni podpis

Digitalni podpis (ang. digital signature) se uporablja za ugotavljanje pristnosti elektronskega sporočila, dokumenta ali entitete. »Digitalni podpis je dodan čitljivemu besedilu na tak način, da prestane preizkus le, če vsebina sporočila ostane nespremenjena; pravna veljava digitalnega podpisa je ponavadi določena z zakonom« (Jurišić, 2001: 58).

Digitalni podpis se uporablja za podpisovanje dokumentov v elektronski obliki in ima enako veljavnost in dokazno vrednost kot lastnoročni podpis. Je postopek, ki združuje asimetrične algoritme in funkcije zgoščevanja[17] (ang. cryptographic hash functions, one-way hash functions).

[16] Poleg običajnega digitalnega podpisa, poznamo še izpeljanko le tega, tako imenovanega časovni žig (ang. Time Stamp, TS). Posebnost takega podpisa je, da poleg vseh drugih informacij vsebuje še informacijo o natančnem času ustvarjanja podpisa. Pogoj je natančen in verodostojen časovni vir (atomska ura). Časovni žig je pomemben za dokazovanje določenih dogodkov, ki so vezani na čas in je ta čas tudi zelo pomemben (npr. natančen čas oddaje napovedi za dohodnino) (Jerman Blažič, 2004: 64).

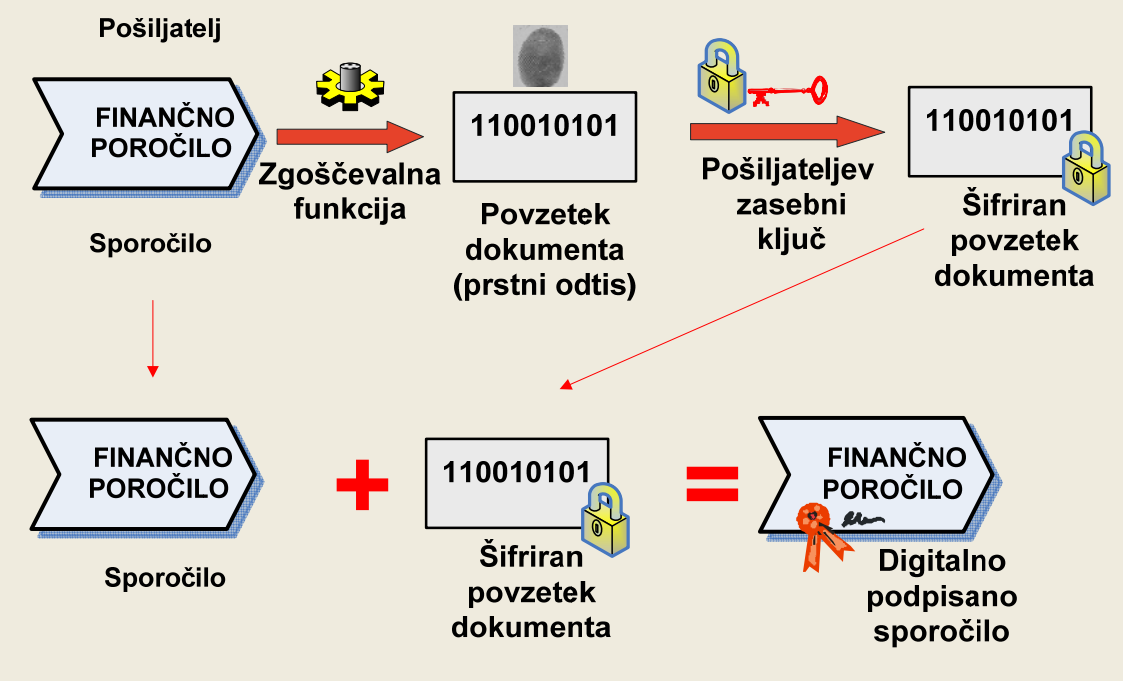
[17] Zgoščevalna funkcija preslika poljubno dolgo sporočilo v blok, ki ima vedno točno določeno dolžino in mu pravimo tudi prstni odtis oziroma povzetek vhodnega sporočila. Dolžina izstopnega podatka je neodvisna od vstopnega podatka. (http://www.sigov.si/tecaj/kripto/kr-zgo.htm, 20. 1. 2006). Najbolj znani zgoščevalni postopki so: MD5 (Message Digest, SHA-1, SHA-2 (Secure Hash Algorithm).

S pomočjo kriptografije dobi digitalni podpis[18] enako veljavnost kot lastnoročni podpis in nam s tem zagotovi:

- avtentičnost,
- podpisa ne moremo ponarediti,
- podpisa ne moremo kopirati,
- podpisanega dokumenta ne moremo spremeniti,
- podpisa ne moremo zanikati.

Pri digitalnem podpisovanju gre pravzaprav za izdelavo prstnega odtisa podatkov, ki je vedno unikaten, kar pomeni, da vsakemu dokumentu pripada natanko en prstni odtis. Ko dokument digitalno podpišemo, se vhodni podatki pretvorijo s pomočjo zgoščevalne funkcije, katere rezultat je prstni odtis dokumenta. Prstni odtis dokumenta moramo še šifrirati z zasebnim ključem in tako dobimo digitalni podpis dokumenta (http://www.halcom-ca.si/slo/infrastruktura_podpis.html, 20. 1. 2006).

Slika 6.9: Postopek digitalnega podpisovanja



Vir: Prirejeno po (http://www.it-akademija.net/kodiranje.pdf, 20. 1. 2005 in Jerman Blažič, 2004: 62.

[18] Pomembno se mi zdi opozoriti na razliko med elektronskim in digitalnim podpisom. Elektronski podpis je kakršnakoli oznaka, narejena z elektronskim medijem, ki jo naredimo, kadar želimo označiti nek dokument ali datoteko. Digitalni podpis je elektronski podpis, kjer uporabljamo kriptografijo (http://www.sigov.si/tecaj/kripto/kr-podp.htm 20. 1. 2006).

Prstni odtis sporočila ima podobne lastnosti, kot človeški prstni odtis:

- vsako sporočilo ima svoj prstni odtis (nikoli se ne more zgoditi, da bi imeli dve različni sporočili enaka prstna odtisa);
- isto sporočilo se vedno preslika v isti blok – prstni odtis;
- iz zgoščevalnega bloka je nemogoče ponovno pridobiti vhodno sporočilo;
- če spreminjamo sporočilo, se z njim spreminja tudi zgoščevalni blok.

Da bo prejemnik lahko prebral sporočilo, bo moral iz prejetega čistopisa (dokumenta) najprej ustvariti prstni odtis s pomočjo enake zgoščevalne funkcije, kot jo je uporabil pošiljatelj. Dobljeni prstni odtis bo nato primerjal s prejetim in s pošiljateljevim javnim ključem dešifriranim prstnim odtisom. Če se oba prstna odtisa ujemata, je podpis veljaven.

6.1.2 Digitalno potrdilo

Bistven podatek pri uporabi kriptografskih sistemov je lastništvo zasebnega in javnega ključa. Digitalno potrdilo[19] (ang. digital certificate) je digitalni dokument, ki predstavlja povezavo med imetnikom in javnim ključem. Digitalno potrdilo zagotavlja verodostojnost javnega ključa.

Lastnosti digitalnega potrdila:

- vsebuje javni ključ ter njegove podatke (parametre);
- zajema vse podatke in informacije o imetniku javnega ključa (ime, priimek, naslov, uporabljene algoritme, namen uporabe ključev, …);
- vsebuje podatke o izdajatelju potrdila;
- je javno objavljen v imenikih ali na spletnih straneh;
- omogoča šifriranje podatkov ter digitalno podpisovanje dokumentov.

(http://www.sigov.si/tecaj/kripto/kr-cert.htm, 1. 2. 2006).

Da so vsi podatki zapisani na potrdilu točni in resnični, jamči overitelj, ki potrdilo digitalno podpiše s svojim zasebnim ključem. Overitelj je agencija (ang. Certification Authority, CA ali Registration Authotity, RA), ki skrbi za izdajo

[19] Lahko tudi: digitalno potrdilo javnega ključa (ang. public key certificate) (http://www.sigov.si /tecaj/kripto/kr-cert.htm, 1. 2. 2006).

potrdil ter za infrastrukturo javno dostopnih podatkov. Varnostna infrastruktura celotnega poteka (generiranje ključev, izdajanje, preklicevanje, podaljševanje itn.) imenujemo infrastruktura javnih ključev (ang. Public Key Infrastrucure, PKI)[20] (Jerman Blažič, 2004: 65).
Digitalno potrdilo lahko razumemo kot osebno izkaznico ali potni list, ki nam omogoča identifikacijo na svetovnem spletu.

Z delovnim področjem informacijske varnosti v Republiki Sloveniji se ukvarja Urad za varovanje tajnih podatkov (več v nadaljevanju diplomske naloge).
Danes v tako imenovani informacijski družbi, družbi tehnike in računalnikov se vedno znova odpirajo številna varnostna vprašanja. Ker sta svinčnik in papir zamenjala internet in elektronsko poslovanje, se varnostna postavka samo še povečala. Z uporabo različnih mehanizmov in postopkov lahko danes onemogočimo prestrezanje informacij, krajo podatkov, različne manipulacije, poneverbe, lažne identitete itn. Digitalni podpis in digitalno potrdilo sta dva varnostna postopka, ki nam omogočata varnejše in zanesljivejše poslovanje.

Na tem mestu se mi zdi pomembno omeniti še SSL[21] protokol, ki nam zagotavlja varno 'deskanje' in uporabo medmrežja. SSL je protokol, ki omogoča šifrirano povezavo med strežnikom in odjemalcem. Je poseben program za šifriranje sporočil, ki potekajo dvosmerno, in je vgrajen tudi v večino brskalnikov. SSL protokol tako zagotavlja varno pot za prenos podatkov s pomočjo šifriranja, uporablja pa tudi poseben digitalni oziroma elektronski podpis. Šifrirana podatkovna linija nam tako v celoti zagotavlja zasebnost komunikacije, ki jo imamo s spletnim portalom, in onemogoča prisluškovanje na vmesnih komunikacijskih točkah (https://dbsnet.dbs.si /eban/ docs/ Varnost _poslovanja.pdf, 1. 2. 2006). SSL protokol se običajno uporablja pri spletnih

[20] V Sloveniji pravila igre v javnih sistemih določa zakonodaja (Zakon o elektronskem poslovanju in elektronskem podpisu, ZEPEP) (Jerman Blažič, 2004: 65).
[21] Ko se odločimo za nakup preko medmrežja ali za plačilo preko e-banke, običajno najprej vzpostavimo nešifrirano povezavo (**http**://www.kriptografija.com). Ikona v desnem spodnjem kotu na ekranu kaže odprto ključavnico  . Ko začnemo pošiljati svoje podatke, se povezava spremeni v šifrirano: v naslovu se protokol spremeni v **https**, spremeni se številka vrat, ikona kaže zaklenjeno ključavnico  (http://www.sigov.si/tecaj/kripto/kr-ssl.htm, 1. 2. 2006).

trgovinah, elektronskih bančnih transakcijah oziroma na vseh spletnih straneh, kjer je potrebna določena stopnja varnosti.

6.2 VAROVANJE TAJNIH PODATKOV

Kaj je tajen podatek? Tajno je vse tisto, kar ni javno oziroma, kar je javno ni tajno. Je nekaj, kar ni poznano širšemu krogu ljudi, ki se s tem tudi ne morejo seznaniti. Je lahko katerakoli informacija ali podatek za katerega ne želimo, da ga izve naš nasprotnik, sovražnik ali konkurent. Danes tajnih podatkov ne enačimo več samo s tajnimi službami in agenti, temveč tudi z različnimi poslovnimi, gospodarskimi in državnimi institucijami.
Tajni podatki niso pomembni samo na državni ravni, temveč tudi v poslovnem svetu in na zasebnem področju. V poslovnem svetu se uporablja tudi termin 'poslovna skrivnost' in 'varnost poslovne skrivnosti'. Vendar ko govorimo o tajnih podatkih, običajno mislimo na podatke, ki so pomembni za varno in nemoteno delovanje različnih državnih organov in služb.

V Zakonu[22] o tajnih podatkih je tajni podatek opredeljen kot *»/d/ejstvo ali sredstvo z delovnega področja organa, ki se nanaša na javno varnost, obrambo, zunanje zadeve ali obveščevalno in varnostno dejavnost države, ki ga je treba zaradi razlogov določenih v tem zakonu zavarovati pred nepoklicanimi osebami, in ki je v skladu s tem zakonom določeno in označeno za tajno.«*

Enako kot pri informacijski varnosti tudi pri zaščiti tajnih podatkov, poleg drugih postopkov in mehanizmov, uporabljamo kriptografijo. Pri varovanju tajnih podatkov poleg tehničnih metod uporabljamo tudi fizične pristope. Problem pri varovanju tajnih podatkov je poleg tega, kako jih zaščititi, tudi katere osebe smejo do njih dostopati. Potrebno je izvajati varnostno preverjanje oseb in določiti stopnjo varovanja podatkov. Sam proces varovanja tajnih podatkov je z nacionalnovarnostnega stališča zelo pomemben, saj *»/d/ržava, ki ustrezno varuje svoje tajne podatke, je v mednarodni skupnosti sprejeta kot zaupanja vreden partner.«* (Čaleta 2004: 55).

[22] Uradni list št. 135, 31. 12. 2003

Kriptosisteme, ki jih uporabljajmo za varovanje državnih tajnih podatkov, se običajno ne kupuje, saj bi s tem razkrili kateri sistem uporabljamo.
Zelo pomembno je tudi, da so vse elektronske naprave, ki jih uporabljamo za obdelavo in shranjevanje tajnih podatkov, ustrezno preverjene in odobrene s strani ustreznih služb (Čaleta 2004: 54).
Pri procesu varovanja in zaščite tajnih podatkov gre za celovit pristop, ki v družbenem in pravnem pogledu zahteva ustrezno zakonsko ureditev.

7 PODROČJA UPORABE KRIPTOGRAFIJE IN KRIPTOANALIZE

Uporaba kriptologije v svetu narašča. Rast uporabe računalniške tehnologije, medmrežja, e-poslovanja, uporaba mobilnih in brezžičnih omrežij so dejavniki, ki so prinesli nove težave in izzive pri varovanju informacij in podatkov. Hitre spremembe na področju računalniške tehnologije so spremenile naravo dela. Pretok informacij se je povečal in večina podatkov se shranjuje v elektronsko obliko. Za informacijsko družbo je značilno, da temelji na informacijski infrastrukturi, ki je sestavljena iz tehnološke opreme, telekomunikacijskih omrežji in različnih storitev. Družbo tvorimo in ustvarjamo ljudje, oblikujemo in uporabljamo informacije ter razvijamo nove aplikacije in storitve. Informacijsko družbo opisujemo kot družbo, ki:

- ne pozna časovne razlike in geografske razdalje,
- temelji na izdelavi, izmenjavi in uporabi informacij,
- osnovna oblika prenosa informacij je postala multimedijska,
- temelji na uporabi znanja,
- se vključuje v družbene procese s pomočjo dostopa do informacij in razvito komunikacijsko infrastrukturo.

(Podešva, 2001: 81)

Primarno področje uporabe kriptografije je področje računalniške tehnologije. In sicer se kriptografija uporablja za:

- zaščito elektronskega poslovanja (elektronska pošta, transakcije),
- zaščito računalniških datotek in programov,
- zaščito internetnega omrežja,

- zaščito telekomunikacij,
- pametne kartice,
- digitalni podpis.

Da bi informacije in podatke v večjih organizacijah in službah uspešno zaščitili, potrebujemo:

- strokovno usposobljeno osebje,
- predpisane procese in postopke,
- ustrezno tehnologijo,
- zakone in predpise vlade.

Kriptografija ne igra pomembne vloge samo v javnem sektorju, temveč tudi v zasebnem. Tukaj govorimo o drugačni zaščiti informacij in podatkov, in sicer takšni, ki nam omogoča zasebnost, anonimnost in potrditev identitete. Kadar se povežemo z zunanjim svetom (družbo) in nismo zaščiteni, lahko postanemo ranljivi. Za primer vzemimo uporabo medmrežja (elektronska pošta, e-poslovanje, e-bančništvo), uporabo mobilne telefonije in bančnih kartic.
Podatke in informacije, ki so pomembni za osebno uporabo (domači PC), lahko zaščitimo s preprostimi kriptografskimi programi, kot je na primer program PGP. V takem primeru ne potrebujemo usposobljenega osebja, predpisanih postopkov in zakonov.

Področja uporabe kriptografije in kriptoanalize, ki so pomembna v sistemu nacionalne varnosti[23]:

- **gospodarska politika** - ekonomija: informacijska varnost, banke, bančne transakcije, pristnost in podpis; elektronske komunikacije: komunikacije po telefonu, faksu, elektronski pošti, svetovnem spletu, pretok komunikacij po telekomunikacijskih omrežjih;
- **zunanja politika** – diplomacija: zbiranje informacij, navodila, vohunjenje;
- **obrambna politika** – vojska: vodenje in poveljevanje, zaščita tajnih podatkov znotraj samega sistema;

[23] Področja nacionalno varnostnega sistema sem povzela po Grizold, 1999: 36.

- **zdravstvena politika**: dokazovanje zdravstvenega zavarovanja bolnika, nadzor stroškov;
- **policija**: zbiranje podatkov in informacij;
- **obveščevalne agencije in službe**: prisluškovanje, prestrezanje podatkov in informacij, vohunjenje;
- **socialna politika**: zaščita osebnih podatkov;
- **kulturna politika**: zaščita DVD in CD medijev.

Kriptografski sistemi se uporabljajo tako v strojni kot v programski obliki skoraj na vseh področjih nacionalno varnostne politike. Seveda ne moremo mimo dejstva, da se kriptografija uporablja prav tako pri kriminalnih dejanjih in drugih delovanjih proti državi. Tukaj nastane problem, do katere meje naj država dovoli uporabo, izvoz in uvoz kriptografskih strojev in programov. V nekaterih državah imajo zakone, ki opredeljujejo katere kriptografske sisteme se sme uporabljati in uvažati. Podobne zahteve narekujeta tudi zveza NATO in EU, kar posledično vpliva tudi na Republiko Slovenijo (več v poglavju 9).

7.1 PAMETNE KARTICE

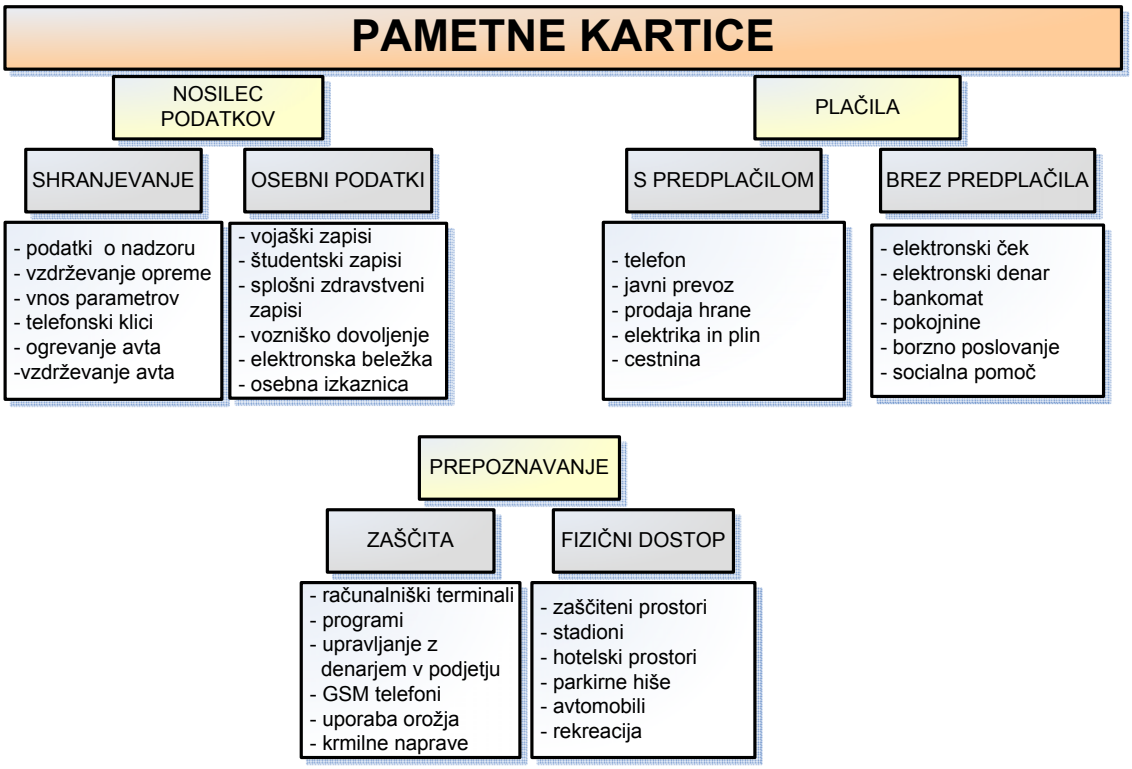
Za podrobno analizo uporabe kriptografije v praksi sem izbrala uporabo pametnih kartic, in sicer zato, ker se uporabljajo na mnogih področjih tako javnega kot zasebnega življenja.
Današnjega življenja si brez uporabe identifikacijskih in pametnih kartic ne moremo zamisliti. Omogočajo nam opravljanje vsakodnevnih dejavnosti, kot so nakupovanje, izposoja knjig, telefoniranje, transport, zdravstvene storitve itn. (Kovačič, 2003: 13).

Pametna[24] kartica je pravi mali računalnik. Je plastična kartica, velikosti[25] kreditne kartice ali SIM kartice, ki je sestavljena iz mikroprocesorja, pomnilnika in vhodne/izhodne enote. Varnost in zaščito pametnih kartic zagotavljajo štiri komponente: kartica, čip, operacijski sistem in namenski program.

[24] Ime pametna kartica se pogosto uporablja za vse kartice s čipom.
[25] Dva standarda: ISO 7810 ali ID-000

Pomembna razloga za uporabo pametnih kartic sta dva: varnost shranjenih podatkov na krtici in zaščita podatkov drugih računalniških sistemov. Za zaščito podatkov se uporabljajo različni kriptografski algoritmi. Približno 30 let po prvem patentu za pametne kartice, smo priča visoki stopnji uporabe na mnogih področjih (Jurišić, Tonejc 2001: 58).

Slika 7.10: Področja uporabe pametnih kartic



Vir: Prirejeno po Jurišić 2001: 69.

Največje število pametnih kartic se še vedno uporablja v telekomunikacijah, zadnja leta pa tudi v zdravstvu (nadzor stroškov), financah (e-bančništvo, shranjevanje certifikatov), elektronskem poslovanju (digitalni certifikati), šolstvu (podatki o študenti), transportu (javni prevozi, cestninjenje), veterinarstvu itn.

Kot sem že opisala pri kriptografskih sistemih, potrebujemo ključ, ki nam omogoča preoblikovanje in šifriranje podatkov. Problem predstavljata varnost in zaščita ključa, ki ga običajno shranimo na disk, kjer pa ni varen. Kriptografske ključe je smiselno shranjevati na ločenih napravah, kot so pametne kartice.

Pametne kartice nam omogočajo shranjevanje certifikatov in zasebnih ključev, namenjene pa so tudi operacijam za kriptografijo javnih ključev, kot so preverjanje pristnosti, digitalno podpisovanje in izmenjava ključev.

Poleg že naštetih razlogov za uporabo pametnih kartic, so razlogi še naslednji:

- shranjevanje različnih oblik osebne identifikacije brez nevarnosti nepooblaščenega spreminjanja;
- ločevanje kritičnih varnostnih izračunavanj, povezanih s preverjanjem pristnosti, digitalnimi podpisi in izmenjavo ključev, od tistih delov sistema, ki takih podatkov ne potrebujejo;
- varen prenos informacij iz enega računalnika v drugega.

(http://www.microsoft.com/slovenija/windowsxp/pro/funkcije/pametne_kartice.mspx, 1. 3. 2006).

Praktičen primer uporabe pametne kartice je bankomat kartica. Banka spravi zasebni ključ stranke na njeno pametno kartico, s katero se stranka nato digitalno podpiše in ji je transakcija tako zagotovljena. Pametno kartico naj bi uporabljal in z njo tudi digitalno podpisoval samo njen lastnik (Jurišić, Tonejc 2001: 64).

Pri uvajanju in uporabi identifikacijskih kartic (npr. osebna izkaznica – v Sloveniji je samo plastična kartica in ne pametna) na nacionalni ravni se pojavi več problemov in eden od njih je tudi nadzor ljudi. Namreč, če državna organizacija dostopa do vseh podatkov na karticah, to lahko močno ogrozi zasebnost in svobodo posameznika. Za vsako identifikacijo predložimo osebno izkaznico in čip na kartici bi si vsako identifikacijo zapomnil ter centralnim sistemom posredoval zbrane podatke. Na podlagi tega lahko policija, tajne službe ali vojska izdelajo natančen profil vsakega državljana, ki je lastnik osebne izkaznice in se z njo identificira (Jurišić, Tonejc 2001: 75). Uporaba pametnih kartic omogoča zlivanje in zbiranje, javnih, državnih in komercialnih baz podatkov (Lyton 1994: 150 v Kovačič 2003: 14).

Če prištejemo še uporabo biometričnih metod (letališča), videonadzora (trgovine, banke), nadzora komunikacijskih sredstev (prisluškovanje), lahko trdim, da anonimnost in zasebnost povsem izgineta iz našega življenja in nadzor je popoln.

V letu 2006 bodo proizvajalci kartic proizvedli 2,2 milijardi kartic, kar je 20 % več kot leta 2005. Proizvodnja in prodaja se bo povečala pri vseh vrstah pametnih kartic. Prevladovale bodo SIM kartice, ki bodo zasedle 73 % trga (http://www.ris.org/main/rubrika3/readrub3.php?sid=224, 1. 3. 2006).

Tako kot osebni računalniki so tudi pametne kartice postale del vsakdana. Razvoj in uporaba kriptografije ter pametnih kartic sta tesno povezana. Za varnost podatkov in shranjevanje certifikatov, ki so zapisani na pametnih karticah, uporabljamo različne kriptografske sisteme (asimetrični algoritmi, simetrični algoritmi in eliptične[26] krivulje). Pametne kartice so pomembne tako za nacionalne agencije (zdravstvo, policija, vojska) kot tudi za posameznika (bančne kartice).

V Republiki Sloveniji overitelj SIGEN-CA priporoča uporabo pametnih kartic za shranjevanje zasebnih ključev in pripadajočih digitalnih potrdil. Pametne kartice namreč predstavljajo ustrezno tehnološko rešitev, ki omogoča varen način hranjenja zasebnih ključev in pripadajočih digitalnih potrdil.

8 VPRAŠANJE VARNOSTI KRIPTOSISTEMOV

Kadar govorimo o kriptografskih sistemih, je ključnega pomena njihova varnost. Danes obstaja mnogo različnih načinov in poti, kako 'napasti' oz. 'razbiti' kriptografski sistem ali šifrirni algoritem. Cilj takih napadov je samo en, in sicer ugotoviti skriti ključ, ki je potreben za dešifriranje sporočila. Kako varen je nek kriptografski sistem, nam pove to, koliko časa ga nihče ne 'razbije'.

Napadalec lahko poizkuša:

- dešifrirati določeno sporočilo in na ta način priti do uporabnih informacij;
- odkriti tajni ključ, kar mu omogoča dešifriranje vseh sporočil, ki so šifrirana s tem ključem;

[26] Eliptična krivulja (ang. Elliptic Curve Cryptosystem – ECC) je množica točk, ki rešijo enačbo $y^2 = x^3 + ax + b$. Uporabljajo se pri asimetrični kriptografiji. Ta razred kriptosistemov je alternativa RSA, njegova glavna prednost so krajši ključi (Jurišić, Tonejc, 2001: 60).

- odkriti šibkost šifrirnega postopka, kar mu omogoča dešifriranje vseh sporočil, ki so bila šifrirana s tem postopkom.

(http://www.ltfe.org/pdf/Varnost%20v%20telekomunikacijah.pdf, 15. 3. 2006)

Napadi na šifrirne postopke se razlikujejo glede na to, kaj ima napadalec ob napadu na voljo, ločimo:

- napad na osnovi enega ali več šifropisov;
- napad, pri katerem ima napadalec na voljo enega ali več parov čistopisa in šifropisa;
- napad, pri katerem ima napadalec na voljo šifropise poljubnega števila izbranih čistopisov.

(http://www.ltfe.org/pdf/Varnost%20v%20telekomunikacijah.pdf, 15. 3. 2006).

Glede na varnost, ki jo nudijo šifrirni postopki, ločimo:

- teoretične[27] varne postopke, ki jih je nemogoče razbiti, ne glede na vložen čas in sredstva;
- praktično varne postopke, za katere je verjetnost, da bi jih razbili v omejenem času z omejenimi sredstvi dovolj majhna.

(http://www.ltfe.org/pdf/Varnost%20v%20telekomunikacijah.pdf, 15. 3. 2006)

IBM-ovi ustvarjalci varnostnih sistemov delijo napadalce v tri skupine:

- 1. razred (pametni 'outsiderji'): to so običajno zelo inteligentni ljudje, ki pa samo izkoriščajo obstoječe šibkosti sistema;
- 2. razred ('insiderji'): so ljudje z izobrazbo in izkušnjami in utegnejo priti do informaciji oz. do naprednih orodij za analizo;
- 3. razred (močnejše organizacije): organizacije, ki sestavijo ekipe specialistov, ki lahko opravijo temeljite analize sistemov in iznajdejo napade na te sisteme.

(Jurišić, Monitor 2001: 56)

[27] Edini znan teoretično varen postopek je postopek z enkratno uporabo ključa (ang. one time key pad). Gre za postopek, pri katerem je ključ popolnoma naključen in enak dolžini sporočila. S preizkušanjem vseh možnih ključev bi napadalec dobil vsa možna sporočila, vendar ne bi mogel ugotoviti, katero sporočilo je pravo (http://www.ltfe.org/pdf/Varnost%20v%20telekomunikacijah.pdf, 15. 3. 2006).

Predlagane minimalne dolžine ključev, potrebnih za varen simetrični sistem, kot sta DES in IDEA:

- da bi zagotovili ustrezno zaščito pred resnimi grožnjami, mora biti ključ dolg vsaj 75 bitov;
- da bi zagotovili ustrezno zaščito za naslednjih 20 let, morajo biti ključi dolgi vsaj 90 bitov.

Tabela 9.1: Povprečen čas za napad z grobo silo (angl. Brute Force Attack) – ocene glede na tehnologijo iz leta 2000.

Dolžina ključa (v bitih)	Posamični napadalec A	Majhne skupine B	Raziskovalna omrežja C	Velika podjetja D	Vojaške obveščevalne službe E
40	DNEVI	URE	MINUTE	MILISEKUNDE	MIKROSEKUNDE
56	LETA	TEDNI	DNEVI	MINUTE	MILISEKUNDE
64	TISOČLETJA	STOLETJA	DESETLETJA	URE	SEKUNDE
80	∞	∞	TISOČLETJA	STOLETJA	DNEVI
128	∞	∞	∞	∞	∞

A posameznik ima en PC in programsko opremo ***(220–228 ključev/s),***
B majhna skupina, 16 PC-jev ***(224–232 ključev/s),***
C raziskovalna omrežja, 256 PC-jev ***(228–236 ključev/s),***
D veliko podjetje z 1.000.000 dolarjev za strojno opremo ***(248 ključev/s),***
E vojaška obveščevalna organizacija z 1.000.000.000 dolarjev za strojno opremo in napredno tehnologijo ***(260 ključev/s).***
Vir: Jurišić, Monitor 2001: 51

8.1 VARNOSTNI MODELI

Kako varni so kriptografski sistemi, lahko ocenimo na podlagi različnih varnostnih modelov:

- ***absolutna varnost*** (*ang. unconditional security*) ali tudi popolna tajnost (ang. Perfect secrecy) – pogoj za absolutno varnost je, da je ključ vsaj toliko dolg, kot je dolgo sporočilo. Danes nam noben kriptosistem ne nudi absolutne varnosti;

- ***računalniška varnost*** (*ang. computational security*) – model predvideva, da imajo napadalci manj zmogljive računalniške sisteme kot mi in če imajo oni 'super' zmogljive računalniške sisteme, lahko naše kriptografske algoritme razbijejo samo z 'megasuper' zmogljivimi računalniškimi sistemi;
- ***dokazljiva varnost*** (*ang. provable security*) – o taki varnosti govorimo takrat, ko lahko dokažemo, da je 'razbijanje' take šifre ekvivalent reševanju težkih matematičnih problemov. Dokaz temelji le na matematičnih predvidevanjih;
- ***dejanska varnost*** (*ang. pratical security*) – model temelji na modelu računalniške varnosti s to razliko, da se ocenjuje varnost kriptografskih sistemov na podlagi že storjenih napadov. O taki varnosti govorimo takrat, ko je imel najmočnejši napad *N* operacij in je *N* visoko število.

(Jerman-Blažič, Schneider, Klobučar, 2004: 9)

Kriptografija je interdisciplinarna znanstvena veda, ki je dosegla vrhunec v zadnjih nekaj letih. To seveda ne pomeni, da ni potrebno raziskovati naprej tako v teoretičnem kot tudi v praktičnem smislu. Vsako novo odkritje s tega področja predstavlja nove izzive tako za matematike, strokovne delavce in znanstvenike kot tudi za 'napadalce' in 'razbijalce' kriptografskih sistemmov. Z vsakim uspešnim 'razbitjem' kriptografskega sistema nastane nov varnostni model.

8.2 UPORABA KRIPTOANALIZE

O uporabi kriptoanalize je napisanega dokaj malo, kar je ravno obratno, kot velja za kriptografijo. Po 16. stoletju, ko so se pojavile bolj zapletene šifre, se je počasi začela razvijati kriptoanaliza. Razvijala se je vzporedno s kriptografijo. Posledica 'razbitih' šifer je bila, da so nastajale nove in s tem tudi nove oblike kriptoanalize. V praksi sta kriptografija in kriptoanaliza kot dve strani istega kovanca. Med njima vseskozi poteka vzajemna igra, ko se ena stran krepi druga slabi in obratno. Kriptoanalitične tehnike in metode nastajajo nesledljivo hitro, da strokovnjaki enostavno ne morejo slediti vsem novim tehnikam in metodam. Kriptoanalize se da naučiti le z veliko vaje. Vsak dober kriptograf mora biti najprej dober kriptoanalitik. Marsikdo lahko napiše nov šifrirni algoritem, kar pa predstavlja večji problem, je ta algoritem 'razbiti'. Samo izkušeni kriptoanalitiki lahko zgradijo dober kriptografski algoritem, na tem istem

pa bodo zopet drugi strokovnjaki pridobivali izkušnje in znanje. S pomočjo kriptoanalize ugotavljamo tudi 'čvrstost' kriptosistema.
Kadar poizkušamo dešifrirati neko sporočilo in ne poznamo šifrirnega ključa ter šifrirnega algoritma, govorimo o kriptoanalizi oz. tudi o 'razbijanju' šifer. 'Razbijanje' šifer pomeni iskanje šibkega člena v kriptografskem algoritmu.

Pri kriptoanalizi sta pomembni statistika in entropija jezikov. *»/V/ naravnem jeziku posamezni glasovi oziroma črke ne nastopajo enako pogosto in se pojavljajo samo v določenih kombinacijah. Zato lahko uganemo neko besedo, čeprav ne poznamo vseh črk, ki jo sestavljajo.«* (http://www.sigov .si /tecaj/kripto/kr-entropija.htm, 15. 4. 2006).

Tabela 9.2: Frekvenčna porazdelitev črk v odstotkih v slovenski abecedi

AE	**10,5**
OI	**9**
N	**6,3**
LSR	**5**
JT	**4,7; 4,2**
VKDPM	**3,8 – 3,2**
ZBU	**2**
GČ	**1,5**
HŠ	**1**
CŽF	**< 1**

Vir: http://www.sigov .si /tecaj/kripto/kr-entropija.htm, 15. 4. 2006

Kriptoanalizo delimo glede na uporabljene metode na klasično, simetrične algoritme in druge metode. Primeri so: frekvenčna analiza, Kasiskijev test, index naključij, diferencialna kriptoanaliza, linearna kriptoanaliza, statistična kriptoanaliza, XSL napad, analiza električne aktivnosti itn.

Da je težje 'razbiti' neko šifro je, zelo pomembno, da so podatki o kriptosistemu skriti in dobro zaščiteni. Nikoli ne moremo vedeti, kako dolgo bo kriptosistem popolnoma varen pred napadalci, saj obstajajo številne metode in tehnike, med

katerimi lahko izbirajo. Buchmann (Buchmann, 2000: 72) razlikuje pet različnih napadov na kriptosisteme:

- ***napad na šifrirano sporočilo*** (ang. ciphertext-only attack) – napadalec pozna šifrirno sporočilo, preko katerega poizkuša ponovno pridobiti čistopis ali ključ;
- ***poznavalec čistopisa*** (ang. known-plaintext attack) – napadalec pozna čistopis preko katerega ugotovi, kašno je šifrirano sporočilo in s tem ugotovi, kateri ključ smo uporabili in tako dešifrira tudi druga šifrirna sporočila;
- ***napad na izbrani čistopis*** (ang. chosen-plintext attack) – napadalec lahko šifrira čistopis, vendar ne pozna ključa, poizkuša najti ključ in dešifrirati ostala šifrirna sporočila;
- ***napad na prilagodljive izbrane čistopise*** (adaptive chosen-plaintext attack) – napadalec lahko šifrira čistopis, poizkuša najti ključ in dešifrirati ostala šifrirna sporočila;
- ***napad na izbrano šifrirno sporočilo*** (chosen-ciphertext attack) – napadalec lahko dešifrira sporočilo čeprav nima ključa, ki ga poizkuša najti.

V večini primerov gre pri kriptoanalizi za nepooblaščen dostop do šifrirnih sporočil in s tem se povzroča večja ali manjša škoda.
Države so že zgodaj spoznale kako, koristna je kriptoanaliza za tajne agencije, vojsko, diplomacijo, službe, ki zbirajo in 'razbijajo' podatke drugih držav (npr. The Government Communications Headquarters - GCHQ in National Securuty Agency – NSA).
V ZDA ima FBI poseben oddelek, ki se ukvarja z dešifriranjem sporočil. Pri približno 300 kazenskih primerih je 12 takih, kjer je uporabljena kriptografija (Denning in Baugh 1999: 259 v Kovačič 2003: 72).

Uporaba kriptoanalize v negativnem smislu: Vzemimo za primer, da smo nekomu poslali elektronsko sporočilo, čigar vsebina je patent novega stroja za izdelavo zobotrebcev. Sporočilo smo primerno šifrirali, vendar je napadalec šifro 'razbil', dobil ustrezen ključ in prebral naše sporočilo. Čez eno leto ima izdelan nov stroj za izdelavo zobotrebcev, ki je najhitrejši in najvarčnejši na svetu.

Uporaba kriptoanalize v pozitivnem smislu: S pomočjo kriptoanalize razbijemo šifre in šifrirne algoritme, ki so pomembni za nacionalno varnost (spomnimo se 'razbitja' šifre Enigma med drugo svetovno vojno).

9 ANALIZA UPORABE KRIPTOGRAFIJE IN KRIPTOANALIZE V REPUBLIKI SLOVENIJI

Od osamosvojitve Republike Slovenije je letos minilo petnajst let, kar je relativno kratko obdobje za neko državo. Slovenija je v tem času spremenila politični sistem in zaključila proces tranzicije z vstopom v zvezo NATO in EU.
Čeprav se kriptografija v Sloveniji uporablja na mnogih področjih, še vedno nimamo zakonske ureditve in enotne kriptografske politike oziroma nimamo enotnega standarda, ki bi veljal za celo državo. To seveda ne pomeni, da vladne službe, agencije, ministrstva in uradi ne uporabljajo kriptografske zaščite.

Z vstopom v zvezo NATO in EU je morala Slovenija sprejeti določene sklepe in spremeniti zakonodajo s področja kriptografske zaščite tajnih podatkov in informacij. Slovenija je morala prilagoditi tudi druge varnostne standarde standardom zveze NATO in EU.

Običajna praksa je, da ima država točno določen državni organ, ki je zadolžen za strokovno določanje kriptografske politike, tako glede uvoza in izvoza strojne ter programske opreme in določanja kriptografskih standardov. Na zahtevo zveze NATO je tudi Republika Slovenija sprejela sklep, na podlagi katerega pooblašča **Ministrstvo za obrambo Republike Slovenije**, da opravlja naloge s področja kriptografije, pri izvajanju nalog pa sodeluje z **Uradom Republike Slovenije za varovanje tajnih podatkov kot nacionalno varnostnim organom** (National Security Authority – NSA).

9.1 NACIONALNA VARNOST

Nacionalni varnosti pripisujejo vse države velik pomen in enako velja tudi za Republiko Slovenjo. Temeljni dokument na področju nacionalne varnosti Republike Slovenije je Resolucija o strategiji nacionalne varnosti Republike Slovenije[28](ReSNV), v katerem so opredeljeni nacionalni interesi, varnostna tveganja in viri ogrožanja države, njenih institucij, državljank in državljanov ter usmeritve, ukrepi in mehanizmi za zagotavljanje nacionalne varnosti (Resolucija o strategiji nacionalne varnosti republike Slovenije, Uradni list RS, št. 56-2957/2001).

V ReSNV so viri ogrožanja nacionalne varnosti opredeljeni kot: subverzivna dejavnost, grožnja z agresijo, vojaški napad, množične migracije, **terorizem, organiziran kriminal,** uničevanje okolja, gospodarske blokade, vključno z energetsko krizo, **informacijske** oziroma kibernetične **blokade** ali delovanje, zdravstveno-epidemiološka ogrožanja ter naravne in druge nesreče. Vedno več je nevojaških virov ogrožanja in ti običajno zadevajo politično, vojaško, ekonomsko in informativno raven.

Čeprav je Resolucija o strategiji nacionalne varnosti Republike Slovenije temeljni dokument na področju nacionalne varnosti, ne opredeljuje kriptografske zaščite in ne omenja za to potrebnih organov ali institucij.

9.1.1 Zakon o obrambi (ZObr)

Ker v Sloveniji nimamo izdelane enotne državne kriptografske politike, dejansko ne obstaja noben zakon ali predpis o uporabi kriptografske opreme in zaščite na nacionalni ravni. Kriptografska zaščita je omenja samo v Zakonu o obrambi (v nadaljevanju ZObr-UPB1 – Uradni list RS 103/2004).

---

[28] *»Zagotavljanje varnosti Republike Slovenije izhaja iz nacionalnih interesov ter spoštovanja človekovih pravic in temeljnih svoboščin, upoštevajoč ustavo, zakonodajo, načela pravne države, načela mednarodnega prava ter obveznosti države, sprejete z mednarodnimi pogodbami.« (Uradni list RS, št. 56-2957/2001).*
»Pravni temelj sistema nacionalne varnosti predstavljajo ustava, zakoni in drugi predpisi, sklenjene mednarodne pogodbe ter splošno veljavna načela mednarodnega prava.« (Uradni list RS, št. 56-2957/2001).

Poglavje V. Civilna obramba: Ukrepi državnih organov in organov lokalne samouprave za delo v vojni;

69. člen (naloge vlade):

3) »/V/lada podrobneje predpiše postopek izdelave in vsebino obrambnih načrtov ter načrtovanja proizvodnje in storitev v vojni, organizacijo upravnih zvez in kriptografskega ter protielektronskega zavarovanja prenosa podatkov na področju obrambe.«

72. člen (upravne zveze in varstvo prenosa podatkov):

(5) »/M/inistrstvo organizira tudi kriptografsko in protielektronsko zavarovanje prenosa podatkov v sistemih zvez, ki se uporabljajo za obrambne potrebe.«

Poglavje VIII. Poklicno delo na obrambnem področju

89. člen (sklenitev delovnega razmerja brez objave):

(1) »/D/elovno razmerje na obrambnem področju se lahko brez javne objave sklene za delovna mesta:

- *uradnikov oziroma strokovno tehničnih delavcev, ki opravljajo operativna dela civilne obrambe, upravnih zvez, informatike in telekomunikacij, kriptozaščite in protielektronske zaščite, tehnične zaščite, vojaške, razvojne, obveščevalne in protiobveščevalne ter varnostne naloge.«*

Poglavje IX. Upravne in strokovne zadeve obrambe

102. člen (informacijski in telekomunikacijski sistem):

(3) »/Z/a varovanje tajnih podatkov v informacijskih in telekomunikacijskih sistemih, ki se uporabljajo za obrambne potrebe, in za povezavo teh sistemov z mednarodnimi obrambnimi in vojaškimi organizacijami v skladu z mednarodnimi pogodbami, je pristojno ministrstvo, ki opravlja tudi naloge organa pristojnega za kriptografsko zaščito podatkov, organa za razdeljevanje kriptografskega materiala in organa za zaščito pred neželenim elektromagnetnim sevanjem naprav v informacijskih in telekomunikacijskih sistemih, ki se uporabljajo za obrambne potrebe. Vlada lahko podrobneje določi naloge, s katerimi se zagotavlja izvajanje varovanja tajnih podatkov v informacijskih in telekomunikacijskih sistemih, ki se uporabljajo za obrambne potrebe, kriptografsko zaščito in zaščito pred neželjenim elektromagnetnim sevanjem.«

104. člen (prepoved pridobitne dejavnosti):

(1) »/K/ot pridobitne ali profitne dejavnosti ni dovoljeno opravljati:

- *kriptografskega in protielektronskega varovanja prenosa podatkov na področju obrambe.«*

(Uradni list RS št. 103/2004).

Kot sem že napisala, v Sloveniji nimamo posebnega organa ali službe, ki bi skrbela za strokovno določanje politike na področju kriptologije. Naloge so razpršene po različnih ministrstvih, službah in agencijah. Pri prebiranju literature sem zasledila članek, v katerem je napisano, da v okviru SNAV (Svet za nacionalno varnost) in SSNAV (sekretariat Sveta za nacionalno varnost) delujeta dve skupini, ki sta specializirani medresorski delovni skupini in ji je imenoval SNAV:

- prva je delovna skupina za kriptologijo in kriptoanalizo;
- druga delovna skupina se ukvarja z nacionalnimi grožnjami.

Obe skupini sta pomembni pri oblikovanju predlogov in rešitev na specializiranih področjih, ki so pomembna za zagotavljanje nacionalne varnosti (Šefic, 2004: 100).

Tudi Republika Slovenija ni izjema in v okviru zveze NATO in EU aktivno deluje v sistemu nacionalne varnosti. Kako Slovenija rešuje problem informacijske varnosti in varovanje tajnih podatkov in kaj je morala spremeniti v zakonodaji ter kakšnim standardom se je morala prilagoditi, analiziram v nadaljevanju.

9.2 INFORMACIJSKA VARNOST

V Republiki Sloveniji na področju varnosti informacij v informacijskih in komunikacijskih sistemih vsi predpisi še niso bili sprejeti. Aktivnosti so potekale predvsem na področju prilagajanja in usklajevanju zahtevam zveze NATO in EU (Čaleta 2004: 54).

Informacijska varnost je eno izmed področij, ki ga pokriva Urad Vlade Republike Slovenije za varovanje tajnih podatkov. Informacijska varnost je opredeljena kot določanje ukrepov, ki so potrebni za zaščito tajnih podatkov, ki se obdelujejo, shranjujejo, prenašajo preko različnih komunikacijskih kanalov, pred izgubo tajnosti, celovitosti ali razpoložljivosti.

Pokriva naslednja področja:

INFOSEC – informacijska varnost vsebuje naslednje ukrepe:

- ***COMPUSEC*** – za varovanje tajnosti v računalniških sistemih oziroma računalniška varnost (varnost strojne opreme, varnost programske opreme in varnost programsko strojne opreme);
- ***COMSEC*** – ukrepe za varovanje tajnosti v komunikacijskih sistemih oziroma komunikacijsko varnost:
    1) ***TRANSEC*** – varnost prenosnih sistemov;
    2) ***CRYPTOSEC*** – varnost kriptografskih metod in naprav;
    3) ***EMSEC*** – varnost pri elektromagnetnem sevanju elektronskih naprav.

(http://www.uvtp.gov.si/index.php?id=694, 30. 4. 2006).

9.2.1 Zakon o elektronskem poslovanju in elektronskem podpisu

Državni zbor je 13. junija sprejel Zakon o elektronskem poslovanju in elektronskem podpisu[29] (ZEPEP), ki predstavlja temelj elektronskega poslovanja v Republiki Sloveniji. Zakon ureja novo področje poslovanja gospodarskih subjektov, državljanov in državnih organov. S sprejetjem zakona je bilo vzpostavljeno varno okolje za preverjanje pristnosti elektronsko oblikovanih, shranjenih, poslanih, sprejetih ali kako drugače obdelanih podatkov. Zakon ureja vprašanje pristnosti in podpisovanja ter s tem zagotavljanje pravnega učinka elektronskih podatkov. Elektronsko podpisovanje omogoča prejemniku, da preveri pristnost izvora podatkov, njihovo celovitost in nespremenjenost. Identiteto podpisnika lahko posreduje podpisnik sam ali tretja stranka (oseba ali institucija, ki ji zaupata tako pošiljatelj kot prejemnik) (Silič 2001: 4).

»/Z/akon je v celoti usklajen z določili Modelnega zakona komisije OZN za mednarodno gospodarsko pravo (UNCITRAL) o elektronskem poslovanju in Enotnimi pravili za elektronske podpise ter z določili primarne evropske zakonodaje. Prevzema tudi vse določbe Direktive 1999/93/EC Evropskega

[29] Zakon je bil spremenjen in dopolnjen maja 2004.

parlamenta in sveta EU z dne 13. decembra 1999 o skupnem okviru Skupnosti za elektronske podpise.« (Perenič, 2001: 7).

Cilji Zakona o elektronskem poslovanju in elektronskem podpisu:

- spodbujanje tehnološkega razvoja elektronskega poslovanja;
- odstranjevanje normativnih ovir za elektronsko poslovanje – izenačitev elektronskih oblik s klasično papirno obliko in izenačitev elektronskih podpisov z lastnoročnim podpisom;
- vzpostaviti jasna pravila za izmenjavo elektronskih sporočil;
- vzpostaviti pravila za uporabo elektronskega podpisa in za delovanje overiteljev elektronskega podpisa;
- zagotavljanje, da je slovenska pravna ureditev elektronskega poslovanja in elektronskega podpisa usklajena s podobno tujo, predvsem evropsko in mednarodno ureditvijo in s tem zagotavljanje mednarodno priznavanje elektronskih podpisov (Silič 2001: 5-6).

Načela Zakona o elektronskem poslovanju in elektronskem podpisu:

- načelo nediskriminacije elektronske oblike,
- načelo odprtosti,
- načelo pogodbene svobode strank,
- načelo dvojnosti,
- načelo varstva osebnih podatkov in varstva potrošnikov,
- načelo mednarodnega priznavanja.

(Perenič, 2001: 7).

Vsem projektom, ki se izvajajo v okviru programa e-uprava, je poleg strateške usmeritve skupna tudi skrb za popolno varnost poslovanja z informacijami in tajnimi podatki. V skladu z Zakonom o elektronskem poslovanju in elektronskem podpisu delujeta tudi dva slovenska overitelja digitalnih potrdil, ki spadata pod Ministrstvo za javno upravo:

- SIGEN-CA – izdaja kvalificirana digitalna potrdila za fizične osebe in poslovne subjekte;
- SIGOV-CA – izdaja kvalificirana digitalna potrdila za državne organe.

Izdajatelj SIGEN-CA (angl. Slovenian General Certification Authority), izdaja kvalificirana digitalna potrdila za poslovne subjekte in fizične osebe, in deluje v okviru overitelja na Ministrstvu za javno upravo in je registriran v skladu z veljavno zakonodajo in medsebojno priznan z izdajateljem kvalificiranih digitalnih potrdil za državne organe SIGOV-CA (angl. Slovenian Governmental Certification Authority) (http://www.sigen-ca.si/politika-sigen-ca-fizicne-osebe. php, 1. 3. 2006).

Digitalna potrdila SIGEN-CA in SIGOV-CA so namenjena:

- upravljanju s podatki, dostopu in izmenjavi podatkov, s katerimi upravlja javna uprava;
- varnemu elektronskemu komuniciranju med imetniki kvalificiranih digitalnih potrdil overitelja na Ministrstvu za javno upravo;
- vsem storitvam in aplikacijam, za katere se zahteva uporaba digitalnih potrdil overitelja na Ministrstvu za javno upravo.

(http://www.gov.si/ca/, 30. 4. 2006).

Vrste digitalnih potrdil v Republiki Sloveniji

- za fizične osebe,
- za pravne osebe oz. fizične osebe z dejavnostjo,
- za državne institucije,
- za zaposlen pri pravni osebi oz. pri fizični osebi z dejavnostjo,
- za zaposlene v javni upravi.

http://edavki.durs.si/OpenPortal/Pages/Registration/DigicertRequest.aspx, 1. 3. 2006).

Zakon o elektronskem poslovanju in elektronskem podpisu je usklajen tudi z:

- Direktivo 1999/93/EC, ki jo je izdala EU,
- z določili Modelnega zakona OZN za mednarodno gospodarsko pravo (UNCITRAL) o elektronskem poslovanju,
- enotnimi pravili za elektronske podpise,
- z določili primarne evropske zakonodaje.

Evropska komisija je pooblastila institucijo EESSI (*ang. European Electronic Signature Standardization Initiative*), ki analizira področja za določitev potrebnih standardov. V okviru EESSI delujeta še dve instituciji ETSI (*ang. European Telecommunications Standards Institute*) in CEN (*fr. Comite Euripean de Normalisation*) (Center Vlade Republike Slovenije za informatiko 2003: 18).

9.2.2 Priporočila uporabe kriptografskih algoritmov

Leta 2003 je Center Vlade Republike Slovenije za informatiko[30] izdal brošuro z naslovom: '*Varnostni vidiki aplikacij z uporabo digitalnih potrdil priporočila za aplikacije SIGEN-CA in SIGOV-CA'*. V brošuri je med drugim napisano, katere kriptografske algoritme je priporočljivo uporabljati pri elektronskem podpisovanju in pri uporabi digitalnih potrdil.
V poglavju 7 je napisano:
Aplikacije morajo biti pripravljene tako, da je možno določiti algoritme, dolžine ključev in protokole, ki se uporabljajo, ter jih zamenjati, če se pokaže, da niso več varni. Priporočljivo je uporabljati znane in preverjene kriptografske algoritme:

1. **za zgoščevalno** funkcijo SHA – 1 ali ripemd – 160,
2. **za šifriranje** trojni DES ali AES s 128-bitnim ključem,
3. **za izmenjavo ključa** RSA s 1024-bitnim modulom ali Diffie-Hellman s 1024-bitnim praštevilskim ključem,
4. **za digitalni podpis** RSADSS s 1024-bitnim ključem ali DSA s 1024-bitnim ključem.

(Center Vlade Republike Slovenije za informatiko 2003: 18).

9.3 VAROVANJE TAJNIH PODATKOV

Republika Slovenija se je z vstopom v zvezo NATO in EU zavzela, da bo zadostila minimalnim standardom varovanja tajnih podatkov in informacij. Tako zveza NATO, kot tudi EU določata, da mora vsaka država članica ustanoviti nacionalni varnostni organ, ki bo pristojen za varnost in zaščito tajnih podatkov ter informacij.

[30] Center vlade za informatiko danes spada pod okrilje Ministrstva za javno upravo.

V skladu s 43. členom Zakona o tajnih podatkih je bil 22. 1. 2002 ustanovljen Urad Vlade Republike Slovenije za varovanje tajnih podatkov[31].

Delovna področja Urada Vlade RS za varovanje tajnih podatkov:

- ***osebna varnost*** (varnostno preverjanje oseb, ki dostopajo do tajnih podatkov);
- fizična varnost (varovanje objektov in varnostnih območij za varovanje tajnih podatkov);
- ***dokumentacijska varnost*** (varovanje tajnih podatkov skozi njihovo celotno življenjsko obdobje);
- ***informacijska varnost*** (določanje ukrepov, ki so potrebni za zaščito tajnih podatkov, ki se obdelujejo, shranjujejo, prenašajo preko različnih komunikacijskih kanalov, pred izgubo tajnosti, celovitosti ali razpoložljivosti);
- ***industrijska varnost*** (varovanje tajnih podatkov med gospodarskimi družbami in organizacijami);
- ***usposabljanje*** (organiziranje in usposabljanje oseb, ki dostopajo do tajnih podatkov).

(http://www.uvtp.gov.si/index.php, 30. 4. 2006).

Nacionalno varnostni organ *»/s/krbi za izvrševanje mednarodnih pogodb in sprejetih mednarodnih obveznosti ter na tem področju sodeluje z ustreznimi organi tujih držav in mednarodnih organizacij. Usklajuje dejavnosti za zagotavljanje varnosti nacionalnih tajnih podatkov v tujini in tujih tajnih podatkov na območju Republike Slovenije.«*

Nacionalni varnostni organ opravlja naslednje naloge:

- *izdaja in preklicuje dovoljenja fizičnim osebam za dostop do tujih tajnih podatkov;*
- *izdaja in preklicuje varnostna dovoljenja organizacijam za dostop do tujih tajnih podatkov;*
- *izdaja in preklicuje varnostna dovoljenja za sisteme in naprave za prenos, hranjenje in obdelavo tujih tajnih podatkov v skladu s sprejetimi mednarodnimi pogodbami;*

[31] Urad je slovenski NSA.

- *potrjuje izpolnjevanje predpisanih pogojev za obravnavanje tajnih podatkov s strani posameznega organa ali organizacije tujim državam in mednarodnim organizacijam;*
- *izdaja navodila za ravnanje s tajnimi podatki tuje države ali mednarodne organizacije;*
- *nadzoruje izvajanje fizičnih, organizacijskih in tehničnih ukrepov za varovanje tajnih podatkov tuje države ali mednarodne organizacije in skladno z ugotovitvami nadzora izdaja obvezna navodila za odpravo ugotovljenih pomanjkljivosti, ki so jih organi dolžni nemudoma izvršiti;*
- *od pristojnega inšpektorata zahteva izvedbo inšpekcijskega nadzora pri določenem organu ali organizaciji;*
- *izmenjuje podatke z nacionalnimi varnostnimi organi tujih držav in z mednarodnimi organizacijami.*

(Uradni list št. 28/2006),

S sprejemom Zakona o varovanju tajnih podatkov se problematiko varovanja tajnih podatkov in informacijske varnosti šele začela reševati.

Zakon o tajnih podatkih ne opredeljuje natančno varnostne organizacije, ki mora biti vzpostavljena za to področje, kriptografije in akreditacijskih postopkov za informacijske sisteme in omrežja. Tukaj lahko nastane problem, saj kot sem že napisala v poglavju 6.2, morajo ustrezne službe in agencije vse naprave, ki se uporabljajo za obdelavo in shranjevanje ter obdelavo tajnih podatkov in informacij, ustrezno preveriti.

Ne glede na to, kakšne pristojnosti ima in bo imel Urad Vlade Republike Slovenije za varovanje tajnih podatkov, ne more v celoti preprečiti razkritja tajnih podatkov, lahko pa možnosti bistveno zmanjša. Človek v sistemu varovanja tajnih podatkov igra pomembno vlogo in je hkrati najbolj občutljiv člen, ki brez fizičnih, tehničnih, organizacijskih postopkov in ukrepov ne more zagotoviti optimalne varnosti. Sistem je potrebno graditi tako, da se ukrepi in postopki med seboj dopolnjujejo in da je zagotovljeno večplastno varovanje (Rozman 2003: 4).

9.5 ORGANIZACIJA SEVERNOATLANTSKEGA SPORAZUMA (NATO)

23. julija 2004 je bi sprejet Zakon o ratifikaciji sporazuma med pogodbenicami Severnoatlantske pogodbe[32] o varnosti podatkov (MSPSPV). Sporazum je bil podpisan 6. marca 1997 v Bruslju. V zakonu pogodbenice potrjujejo: izmenjavo tajnih podatkov med pogodbenicami, vzajemno zaščito in varovanje tajnih podatkov, da je potreben splošen okvir za standarde in postopke. V imenu Organizacije Severnoatlantske pogodbe in v svojem imenu so se pogodbenice sporazumele:

Pogodbenice:

1) ščitijo in varujejo:

a) tajne podatke NATA označene kot take, ali tiste, ki jih NATU predloži država članica;

b) tajne podatke, označene kot take, ki jih države članice predložijo drugi državi članici v podporo programu, projektu ali pogodbi NATA;

2) ohranjajo stopnjo tajnosti podatkov, kot so opredeljeni pod točko 1), in storijo vse potrebno, da jih stopnji tajnosti primerno varujejo;

3) ne uporabljajo tajnih podatkov, kot so opredeljeni pod točko 1), v druge namene kot tiste, ki so določeni v Severnoatlantski pogodbi, sklepih in resolucijah, ki se nanašajo na to pogodbo;

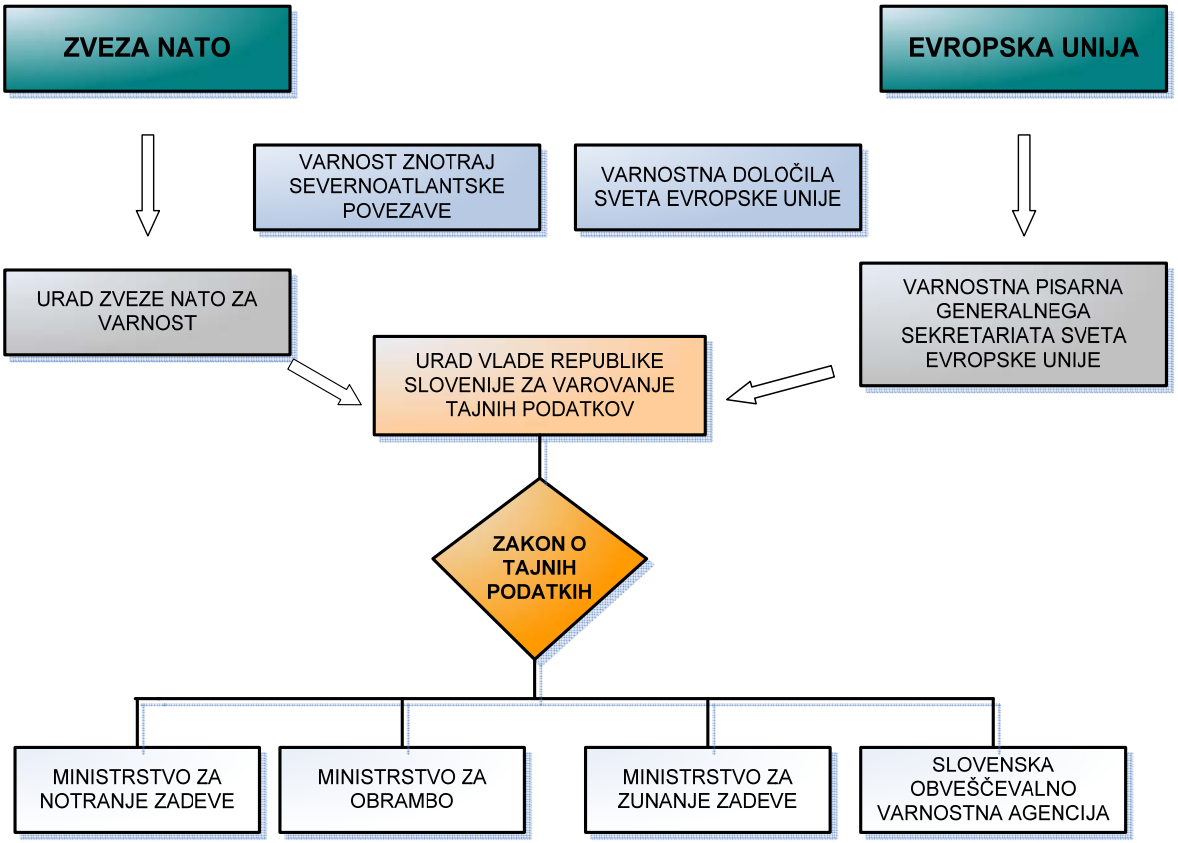
4) ne razkrivajo v točki 1) opredeljenih podatkov stranem, ki niso članice NATA, brez soglasja lastnika podatkov.

(Uradni list št. 83/2004).

V drugem členu zakona je še opredeljeno, da se ustanovi nacionalno varnostni organ za dejavnosti NATA, ki izvaja zaščitne varnostne ukrepe (v Republiki Sloveniji je to Urad Vlade za varovanje tajnih podatkov). Med pogodbenicami se izvajajo varnostni standardi, ki zagotavljajo skupno raven varovanja tajnih podatkov.

[32] Severnoatlanstka pogodba je bila podpisana 4. aprila 1949 v Washingtonu.

Slika 8.11: Sistem varovanja tajnih podatkov v zvezi NATO in EU



Vir: Prirejeno po Černetič, Brožič: 578

9.5.1 Varnostna ureditev zveze nato

Leta 2002 so začeli veljati novi varnostni standardi zveze NATO. Novi dokumenti nadomeščajo prejšnji C-M 55(15)(Final)[33]. Novi varnostni standardi so opredeljeni v dveh dokumentih:

1) **C-M(2002)49** Security Within the North Atlantic Treaty Organisation (NATO) in
2) **C-M(2002)50** Protection Measures for NATO Civil and Military Bodies Deployed NATO Forces and Installations (Assets) against Terrorist Threats.

[33] Pravilnik o varnostnih zahtevah in postopkih za zaščito zaupnih podatkov in srečanj NATO (Security Requirements and Procedures for the Protection of NATO Classified Information and Meetings, CM(55)15(FINAL)) (Anžič in Trbovšek, 2003: 4,5).

Vsebino dokumenta C-M(2002)49 dopolnjujejo direktive, ki obširneje obravnavajo minimalne varnostne standarde. Štiri direktive, ki jih je odobril Severnoatlantski svet:

- **AC/35-D/2000** Directive on Personnel Security – Direktiva o varnostnem preverjanju;
- **AC/35-D/2001** Directive on Physical Security – Direktiva o fizični varnosti;
- **AC/35-D/2002** Directive on Security of Information – Direktiva o informacijski varnosti;
- **AC/35-D/2003** Directive on Industrial Security – Direktiva o industrijski varnosti;

Dve direktivi pa sta odobrila Odbor zveze NATO za varnost in Odbor zveze NATO za posvetovanje, poveljevanje in nadzor, in sicer sta to:

- **AC/35-D/2004** Primary Directive on INFOSEC – Osnovna direktiva za INFOSEC;
- **AC/35-D/2005** INFOSEC Management Directive for CIS – Direktiva za organizacijo CIS[34].

Dokument C-M(2002)50, ki je dodatek k prejšnjemu, navaja smernice za zaščito NATO enot in sredstev pred terorističnimi ogrožanji (Anžič in Trbovšek, 2003: 4,5).

Vlada Republike Slovenije je na podlagi zahtev zveze NATO, 22. 1. 2004 sprejela sklep ***»/o/ določitvi organa, pristojnega za kriptografsko zaščito podatkov, razdeljevanje kriptografskega materiala in za zaščito pred neželjenim elektromagnetnim sevanjem naprav v informacijskih in telekomunikacijskih sistemih, ki se uporabljajo za obrambne potrebe ter o organiziranju kurirske službe za prenos pošiljk s tajnimi podatki NATO.«***

S sprejetjem sklepa pooblašča Ministrstvo za obrambo, *»/d/a v okviru zagotavljanja varovanja tajnih podatkov v informacijskih in telekomunikacijskih sistemih, ki se uporabljajo za obrambne potrebe ter povezavo z organi NATO,*

[34] Communication and Information Systems

opravlja naloge organov:

- **za kriptografsko zaščito tajnih podatkov** (National Communication Security Authority – NCSA);
- **za razdeljevanje kriptografskega materiala** (National Distribution Authority – NDA);
- **za zaščito pred neželjenim elektromagnetnim sevanjem naprav** (National TEMPEST Authority – NTAA);
- **kurirsko službo** (Curier Service).

V drugi točki so opredeljene naloge organa za kriptografsko zaščito tajnih podatkov (NCSA):

- *spremljanje vseh tehničnih informacij ter preverjanje kriptografskih metod in tehničnih rešitev povezanih z zaščito tajnih nacionalnih obrambnih podatkov in podatkov zveze NATO;*
- *zagotavljanje ustrezne in učinkovite izbire, namestitve, upravljanja in vzdrževanja vseh kriptografskih sistemov, opreme, mehanizmov in postopkov za varovanje tajnih nacionalnih obrambnih podatkov in podatkov zveze NATO;*
- *obravnavanje in usklajevanje varnostnih in strokovnih tehničnih zadev na področju kriptografske zaščite s pristojnimi državnimi organi in zvezo NATO;*
- *izdajanje potrdil o varnostni ustreznosti (varnostnih certifikatov) kriptografskih sistemov in opreme kriterijem zveze NATO.*

V tretji točki sklepa so opredeljene naloge organa za razdeljevanje kriptografskega materiala (NDA):

- *uveljavljanje ustreznih postopkov za varno sprejemanje, shranjevanje, razdeljevanje, prenašanje, sledenje, rokovanje in uničevanje kriptografskega materiala za zaščito tajnih nacionalnih obrambnih podatkov in podatkov zveze NATO;*
- *upravljanje z vsem kriptografskim materialom (ključi, algoritmi, opremo, napravami in pripadajočo dokumentacijo) v skladu z nacionalnimi varnostnimi kriteriji ter kriteriji zveze NATO in njenih članic;*

- *izvajanje nalog in opravil prevzemanja, evidentiranja, shranjevanja, uničevanja, razdeljevanja, sledenja in dostave kriptografskega materiala do vseh uporabnikov.*

V četrti točki so opredeljene naloge organa za zaščito pred neželjenim elektromagnetnim sevanjem (NTAA):

- *uveljavljanje ustreznih predpisov in standardov na področju zaščite pred neželjenim elektromagnetnim sevanjem (TEMPEST) v komunikacijskih in informacijskih sistemih;*
- *preverjanje varnostne ustreznosti s stališča neželjenega elektromagnetnega sevanja pri prostorih in opremi za komunikacijske in informacijske sisteme;*
- *izdajanje potrdil o varnostni ustreznosti (varnostnih certifikatov) posameznih prostorov in objektov ter računalniške in komunikacijske opreme varnostnim stopnjam TEMPEST zaščite.*

Peta točka sklepa nalaga Ministrstvu za obrambo, da imenuje kurirsko službo (Courier Service – CS), *ki opravlja prevzem, prenos in dostavo kriptografskega materiala in drugih tajnih podatkov NATO in njenih članic do organa za razdeljevanje kriptografskega materiala in drugih pristojnih državnih organov v Republiki Sloveniji.*

Šesta točka sklepa: *»/M/inistrstvo za obrambo pri izvajanju nalog, določenih s tem sklepom, sodeluje z Uradom Republike Slovenije za varovanje tajnih podatkov kot nacionalnim varnostnim organom (National Security Authority – NSA) in kot organom za varnostno odobritev (delovanja) komunikacijskih in informacijskih sistemov (Security Accreditation Authority – SAA).«*

Sedma točka sklepa: *»/M/inister za obrambo podrobneje določi pristojnosti ter način izvajanja nalog, določenih v 2., 3. in 4. točki tega sklepa, v organizacijski enoti Ministrstva za obrambo, pristojni za informatiko in komunikacijske oziroma kurirske službe iz 5. točke tega sklepa v Generalštabu Slovenske vojske.«*
(Slep Vlade Republike Slovenije, 22. 1. 2004).

9.6 EVROPSKA UNIJA (EU)

Varnostna določila Sveta Evropske unije (Security Regulations of the Council of the Europoean Union, Official Journal of the European Communities (2001/264/EC) L 101/1) so bila sprejeta 19. marca 2001 v Bruslju in so pričela veljati 1. decembra 2001. Za koga vse veljajo varnostna določila? Svet Evropske unije, Generalni sekretariat Sveta Evropske unije in vse države članice. Enako kot zveza NATO varnostna določila določajo, da mora vsaka država članica imeti nacionalno varnostni organ (v Sloveniji Urad Vlade Republike Slovenije za varovanje tajnih podatkov).

9.6.1 Varnostna določila in tehnični ukrepi za zagotavljanje informacijske varnosti v Evropski uniji

1) Varnostna določila urejajo

- organizacijo varnosti v Svetu Evropske unije;
- klasifikacijo in označevanje dokumentov glede na stopnjo tajnosti;
- fizično varnost v objektih in okoliših;
- osnovne principe dostopa do tajnih podatkov in varnostno preverjanje;
- pripravo, distribucijo, pošiljanje, hranjenje in uničevanje tajnih podatkov Evropske unije.

Predpisana je še ustanovitev posebnega registra, kjer se hranijo strogo tajni podatki Evropske unije in varovanje tajnih podatkov s področja informacijske tehnologije in komunikacijskih sistemov (Brožič, 2003: 2).

Za informacijsko varnost v EU je odgovoren Varnostni odbor Sveta EU, ki je sestavljen iz nacionalnih varnostnih organov (npr. Urad Vlade RS za varovanje tajnih podatkov).

9.6.2 Tehnični ukrepi za zagotavljanje informacijske varnosti v Evropski uniji

- nosilci podatkov morajo biti glede na stopnjo tajnosti podatkov ustrezno označeni;

- zagotovljen mora biti nadzor nad dostopom do tajnih podatkov in sledljivost pri pošiljanju;
- pri elektromagnetnem prenosu tajnih podatkov se za zagotavljanje tajnosti, celovitosti in razpoložljivosti izvajajo posebni ukrepi;
- uporaba kriptografskih metod in strojne opreme mora biti posebej odobrena. Pri prenosu podatkov se:
    1) tajnost podatkov stopnje TAJNO EU in višje se zaščiti s kriptografskimi metodami ali produkti, ki jih odobri Svet EU na priporočilo Varnostnega odbora Sveta EU;
    2) tajnost podatkov stopnje ZAUPNO EU ali INTERNO EU zaščiti s kriptografskimi metodami ali produkti, ki jih odobri generalni sekretar na priporočilo Varnostnega odbora Sveta EU ali država članica;
    3) v izrednih primerih se lahko podatki prenašajo v čistopisni obliki.
- namestitev sistemov opravlja le ustrezno preverjeno osebje,
- oprema se namesti v skladu z varnostno politiki Sveta EU;
- tajni podatki stopnje ZAUPNO EU ali višje se zaščitijo tako, da njihova varnost zaradi elektromagnetnega sevanja ni ogrožena.

(Zidar, 2004: 180).

Čeprav je EU postavila infrastrukturo za varovanje tajnih podatkov in informacijske varnosti, še zdaleč ni vse urejeno. Sprejeti so bili le minimalni varnostni standardi, ki so kopija NATO-vih. Pomanjkljivo je opredeljen tehnični del zagotavljanja varnosti tajnih podatkov in informacij. Zidar meni, da še posebno področje kriptografskih sistemov in dodaja: ***»/E/U nima svoje evaluacijske kriptografske avtoritete, kot jo ima NATO. Kriptografija je v EU nekje bolj, drugje malo manj, pa vendar povsod stvar nacionalnega interesa.«*** (Zidar, 2004: 181).

Za kriptografsko zaščito tajnih podatkov in informacij v EU se uporabljajo rešitve, ki jih je predlagal in odobril NATO, natančneje NSA. To pomeni, da NSA točno ve, katere kriptografske sisteme in metode uporablja EU.

Napotki za ureditev področja informacijske varnosti na nacionalnem nivoju so:

- prevzem in uskladitev varnostne politike EU;
- določitev nacionalnih varnostnih avtoritet;
- določitev nacionalne kriptografske avtoritete v okviru katere lahko:
    1) prevzamemo EU merila ali
    2) zgradimo svojo evaluacijsko avtoriteto;
- izvedba postopkov akreditacije;
- postopna vpeljava certificiranih tehničnih rešitev.

(Zidar, 2004: 181).

Akcijski načrt e-Evropa 2005, ki ga je potrdila Resolucija Sveta 18. februarja 2003, med drugim predlaga vzpostavitev prihodnjih struktur na evropski ravni za vprašanja glede varnosti omrežij in informacij (financiranje pregledov, študij, delavnice na temo, kot so varnostni mehanizmi in njihovo medobratovanje, zanesljivost in zaščita omrežij, sodobna kriptografija, zasebnost in varnost pri brezžičnih komunikacijah) (http://www.ris.org/uploadi/editor/1133435246SU RS porocilo_LPSR2004.pdf, 1. 4. 2006).

Tehnični standardi za e-poslovanje v EU, ki so potrebni za potrjevanje tehničnih produktov in za nadzor in potrjevanje e-storitev.

Evropska komisija je za poenotenje pooblastila naslednje institucije:

1) **CEN – EU** Committee for Standardization (www.cenorm.be);
2) **CENELEC – EU** Committee for Electrotechnical Standardization (www.cenelec.org);
3) **ETSI – EU** Telecommunication Standards Institute (www.etsi.org).

(http://lms.uni-mb.si/vitel/14delavnica/predstavitve/ppt-davorka_sel.pdf, 30. 4. 2006).

Zakonodaja e-poslovanja (EU directives of the European Parliament and of the Council):

- *DIRECTIVE 1999/93/EC*, 13 December 1999 on a Community framework for electronic signatures;

- *DIRECTIVE 2002/58/EC*,12 July 2002, concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications);
- *DIRECTIVE 2000/31/EC*, 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on Electronic commerce);
- *DIRECTIVE 2001/115/EC*, 20 December 2001 amending Directive 77/388/EEC with a view to simplifying, modernising and harmonising the conditions laid down for invoicing in respect of value added tax.

Republika Slovenija je na podlagi zahtev zveze NATO začasno in približno uredila vojaško tematiko in podobno se je zgodilo tudi za EU. V okviru teh dveh organizacij se bo morala Slovenija prilagajati njunim standardom in zahtevam. V 'domačem' sistemu nacionalne varnosti pa bo morala zgraditi svojo enotno nacionalno kriptozaščito in urediti politiko ter zakone s tega področja. Na podlagi tega se zdi razumljivo, da bo kriptografske sisteme za lastno uporabo razvijala sama v okviru državne uprave ali v drugih slovenskih podjetjih.

10 KRIOPTOGRAFIJA IN KRIPTOANALIZA TER NACIONALNA VARNOST

10.1 ZAGOTAVLJANJE IN OGROŽANJE NACIONALNE VARNOSTI

Sedaj že lahko trdim, da je kriptologija pomemben del nacionalnovarnostnega sistema. Rezultati in posledice uporabe kriptologije so lahko pozitivne in negativne. V diplomski nalogi sem poizkušala prikazati uporabo različni metod in tehnik kriptologije, s pomočjo katerih zagotavljamo določeno stopnjo varnosti na različnih področjih. Osredotočila sem se predvsem na uporabo kriptologije v smislu zagotavljanja nacionalne varnosti ali kakršne koli druge varnosti. Seveda pa ima vse skupaj tudi drugo stran, in sicer tisto, ki ni več dovolj varna ali bolje legalna. Kriptografska oprema je na voljo vsem, ki jo želijo uporabljati. S tem mislim tudi tiste posameznike, skupine in združbe, ki jo uporabljajo za kršenje zakonov in predpisov,

Obstaja veliko primerov, ko nam uporaba kriptografije in kriptoanalize povzroča veliko težav (kriminalna dejanja, teroristični napadi). Naj navedem primer, ko je teroristična organizacija Hamas preko interneta in z uporabo kriptografije pošiljala zemljevide, slike in druge podrobnosti, ki so potrebne pri načrtovanju terorističnih napadov. Kriptografija in medmrežje se uporabljata tudi pri širjenju otroške pornografije, pri kraji kreditnih in bančnih kartic, v trgovini z mamili, vohunjenju, pranju denarja in vdiranju v računalniške sisteme (Denning in Baugh 1999: 252-274 v Kovačič 2003: 72). Pojavili so se tudi sumi, ki kasneje niso bili dokazani, da je bila kriptografija uporabljena tudi pri načrtovanju napada 11. septembra 2001 (Harrison 2001 v Kovačič 2003: 72).
Na eni strani s pomočjo pravilne uporabe kriptografije in kriptoanalize zagotavljamo nacionalno varnost, na drugi strani kriminalci s pomočjo teh dveh ogrožajo nacionalno varnost.

Področja in primeri uporabe kriptoanalize, ko je ogrožena nacionalna varnost:

- **na področju gospodarske politike** – vdor v bančni sistem – kraja denarja z bančnega računa; pretok komunikacij po telekomunikacijskih omrežjih – razbitje GSM šifrirnih algoritmov – prisluškovanje;
- **področje notranje politike** – vdor v policijsko bazo ali bazo tajne agencije – brisanje dosjejev in dokumentov;
- **na področju obrambne politike** – vdor v vojaško bazo – ogrožanje obrambne strategije neke države; vdor v kontrolni sistem letališča – spreminjanje koordinat;
- **na področju zdravstvene politike** – zamenjava zdravstvene dokumentacije;
- **na področju socialne politike** – vdor v sistem – kraja identitet.

ZDA so želele uvesti kar nekaj ukrepov, ki bi omejevali uporabo kriptografije:

- proizvajalci bi morali v svoje kriptografske proizvode vgraditi bližnjico (ang. trap door), skozi katero bi imeli državni organi dostop do šifriranih sporočil;
- avtorizacija gesel – od uporabnikov bi se zahtevalo, da svoje ključe avtorizirajo pri pooblaščenih agencijah, državni organi pa bi imeli dostop do teh ključev;
- postavljanje kriptografskih standardov, ki bi jih postavila država in si tako omogočila dostop do šifriranih sporočil;

- dovoli se samo uporaba šibke kriptografije, kar bi omogočilo državnim organom hitro 'razbitje' šifre.

Večina teh predlogov je bila pomanjkljivih in niso bili sprejeti (Denning 1997: 184, 187-188 v Kovačič 2003: 75).

V ZDA še vedno poizkušajo omejiti uporabo kriptografije ali pa povečati svoje pristojnosti pri prisluškovanju in prestrezanju sporočil ter tajnih podatkov. Tudi teroristični napad 11. septembra je botroval nekaterim novim idejam o omejitvi uporabe kriptografskih izdelkov, še posebno tistih, pri katerih je državnim organom onemogočen dostop šifriranih sporočil (McCullagh 2001b, 2001c in 2001d v Kovačič 2003: 76).

Tukaj se mi zdi potrebno omeniti še izraz kriptoanarhija, ki se je izoblikoval v zvezi s širjenjem javno dostopne kriptografije in njene zlorabe v kriminalne namene. Zaradi tega država ni zmožna nadzorovati informacij, sestavljati dosjejev, prisluškovati, uravnavati ekonomije in pobirati davkov. S tem ko je državi onemogočen nadzor nad računalniki in telekomunikacijskimi sistemi ter postane vse skupaj bolj dostopno in priročno, lahko vodi v družbeni nered (Denning 1997: 175, 177 v Kovačič 2003: 73).

11 ZAKLJUČEK IN VERIFIKACIJA HIPOTEZ

Pri proučevanju kriptografije, kriptoanalize ter nacionalne varnosti je potrebno upoštevati, da je to obsežno in zapleteno področje. Pri zbiranju virov sem ugotovila, da v Sloveniji primanjkuje kakovostnih dostopnih podatkov s to tematiko, še posebno s stališča nacionalne varnosti. Povsem drugačna situacija je v drugih državah, saj obstaja veliko literature tako v fizični kot v elektronski obliki. Na izdelavo diplomskega dela je vplivalo tudi to, da sem pri uporabi tuje literature naletela na težave predvsem pri prevajanju angleških izrazov v slovenske.

Iz analize lahko povzamem naslednje sklepe in ugotovitve:

[1] Kriptologija se uporablja na vseh področjih komuniciranja in shranjevanja pomembnih in tajnih podatkov. Gre za tehnike in metode, s pomočjo katerih prevajamo nezaščitene podatke v zaščitene in obratno. Obsega področji

kriptografije in kriptoanalize. Glavni cilj kriptografije je zagotavljanje zaupnosti, celovitosti podatkov (zasebnost in verodostojnost), avtentičnosti, preprečevanja tajenja in kontrole dostopa. Je disciplina, ki s pomočjo sredstev in metod preoblikuje podatke in informacije v take oblike, ki so dostopne samo pooblaščenim osebam oziroma osebam, ki imajo ustrezen ključ. Obraten proces je kriptoanaliza, katere glavni cilj je vdiranje v sisteme in 'razbijanje' šifer. S pomočjo kriptoanalize ugotavljamo, kako 'čvrst' je kriptografski sistem. Kriptografski sistemi se uporabljajo tako v strojni kot v programski obliki.

[2] Med največje dosežke v drugi svetovni vojni lahko štejemo projekt '*Ultra*', ki je med drugim vključeval prestrezanje nemških šifriranih sporočil ter njihovo dešifriranje. Uspešnost tega projekta je skrajšala drugo svetovno vojno vsaj za nekaj mesecev.

[3] Kriptografski sistemi se uporabljajo v odprtih in zaprtih sistemih. V odprtih sistemih se uporabljajo standardizirani in javno objavljeni šifrirni algoritmi, ki običajno niso primerni za zaščito informacij in tajnih podatkov na nacionalni ravni. Zaprti sistemi so nadzorovani sistemi, komunikacija poteka v zaprtih krogih, kjer je tajnost prioriteta. Nepisano pravilo je, da se kriptosistemov ne kupuje, ampak se uporabi 'domači' um in se razvije lastne šifrirne algoritme. Kot pravi Zidar (2003: 1): *»/k/riptografija je bila orodje za varovanje najpomembnejših nacionalnih tajnosti in strategij in je v skladu s tem vedno strogo varovana tajnost.«*

[4] Vzrokov za uporabo kriptografije in kriptoanalize je več, najpomembnejša sta zaščita in varovanje pomembnih informacij ter tajnih podatkov.

[5] V obdobju do prve svetovne vojne govorimo o 'ročni' kriptologiji, kjer so se uporabljali svinčnik, papir in domišljija. Obdobje med prvo in drugo svetovno vojno je obdobje novih znanosti in tehnologij. Telefon, telegraf, javni radio, prvi računalniki in začetek novega družbenega sloja tehničnih strokovnjakov in inženirjev je le nekaj dejavnikov, ki so vplivali na razvoj kriptologije. Po razvoju rotorja je bil patentiran najbolj poznan nemški šifrirni stroj Enigma, ki je podoben pisalnemu stroju. Kasneje so se z razvojem večjih in zmogljivejših računalnikov razvijale tudi nove metode in tehnike kriptologije. Moderna kriptografija in kriptoanaliza temeljita skoraj izključno na računalniških programih. Obdelava podatkov in informacij poteka na

nivoju strojnega jezika (zaporedje ničel in enic). Kriptografski in kriptoanalitični programi ne operirajo s črkami in številkami, temveč z biti. Danes uporabljamo kriptosisteme eliptičnih krivulj, njihova glavna prednost sta krajša dolžina ključa in večja varnost. Kriptologija je postala matematična in računalniška disciplina, ki je prodrla na področja, kot so: politika, gospodarstvo, socialna družba in druga. Število subjektov in sistemov, ki so povezana v najrazličnejše komunikacijske sisteme (medmrežje, GSM omrežje), še vedno narašča. S prehodom v informacijsko družbo je postala informacija osnovna dobrina, znanje o informacijski tehnologiji dostopno, komunikacijska tehnologija pa dovolj razvita za odprt pretok in dostop do informacij in komunikacij. Danes družba ne pozna časovne razlike in geografske razdalje, temelji na izdelavi, izmenjavi in uporabi informacij, osnovna oblika prenosa informacij in podatkov je postala multimedijska. Ker prenos večine informacij in podatkov poteka po različnih telekomunikacijskih sistemih in medmrežji so le ti postali ranljivi in lažje dostopni. Informacije in podatki se shranjujejo v elektronski obliki, kar prinaša veliko prednosti, vendar tudi slabosti. S slabostmi mislim predvsem naslednje: če jih ustrezno ne zavarujemo, postanejo ranljivi in dostopni nepooblaščenim osebam. Za zaščito uporabljamo različne kriptografske sisteme (simetrične in asimetrične algoritme), s pomočjo katerih prevajamo informacije in podatke v šifrirne zapise. Pomembna varnostna mehanizma sta tudi digitalni podpis in digitalno potrdilo. Digitalni podpis se uporablja za podpisovanje dokumentov v elektronski obliki in ima enako veljavnost in dokazno vrednost kot lastnoročni podpis, digitalno potrdilo pa zagotavlja verodostojnost javnega ključa, ki ga potrebujemo pri enkripciji in dekripciji. Osnova za zagotavljanje varnosti so varnostne storitve, ki predpisujejo, katera varnostna orodja in mehanizmi so potrebni za zagotavljanje varnosti v različnih sistemih. Na podlagi te ugotovitve lahko potrdim prvo hipotezo, ki se glasi: *'Metode (tehnike) kriptografije in kriptoanalize se razvijajo vzporedno z razvojem informacijske in računalniške tehnologije, le te pa prinašajo nove oblike varnostnih tveganj.'*

[6] Strategija držav je, da v svojem sistemu nacionalne varnosti ustanovijo poseben državni organ (službo, agencijo), ki je pristojen za urejanje

kriptografske politike. Organ strokovno določi pogoje, zahteve in standarde uporabe kriptografske opreme.

[7] Drugo hipotezo, ki se glasi: *'Čeprav se je morala Republika Slovenja z vstopom v zvezo NATO in EU prilagoditi določenim standardom uporabe kriptografske zaščite ter spremeniti zakonodajo, še vedno nima enotnega sistema kriptozaščite',* lahko potrdim na podlagi naslednjih ugotovitev. Kriptologija v Republiki Sloveniji nima dolge tradicije. Čeprav se kriptografska zaščita uporablja na vseh področjih, kjer je potrebna določena stopnja varnosti informacij in podatkov, še vedno niso sprejeti vsi zakoni in predpisi. Odprtih je še veliko vprašanj, zato so vladne organizacije, službe, uradi in ministrstva prepuščeni samim sebi in improvizaciji. Ker Slovenija aktivno deluje (sodeluje) v okviru zveze NATO in EU je to seveda problem. Zveza NATO in EU zahtevata in predpisujeta določene standarde zaščite informacij in tajnih podatkov. Kriptonaprave in kriptosistemi morajo biti certificirani in odobreni s strani varnostne avtoritete NATA in EU. Slovenija je delno uredila zakonodajo glede uporabe kriptografske zaščite s sprejemom Zakona o elektronskem poslovanju in elektronskem podpisu ter imenovanjem Urada Vlade RS za varovanje tajnih podatkov, ki nastopa kot nacionalno varnostni organ (NSA). Urad je med drugim zadolžen za koordiniranje delovanja državnih organov, katerih naloga je vzpostavitev učinkovitega in ustreznega sistema varovanja informacij in podatkov. Večina držav, s katerimi se radi primerjamo, ima v svoji politični strukturi določeno posebno službo ali organ, ki je pristojen za strokovno določanje kriptografske politike (Kovačič 2001: 22). Menim, da bi morala Slovenija prav tako ustanoviti podoben organ, ki bi bil pooblaščen za reševanje kriptografskih potreb državne uprave. Zaposliti bi morali tudi strokovnjake, ki bi sami razvijali kriptografske sisteme za nacionalne potrebe. Lasten razvoj bi bil potreben tudi zato, ker kriptografski sistemi, ki so pomembni s stališča nacionalne varnosti imajo pogosto vgrajene šifrirne algoritme, ki so tajni. Osnovna prednost tega je, da nasprotnik ali nepooblaščena oseba nima nobenih osnovnih tehničnih podatkov, da bi sistem 'razbila' (Zidar 2003: 4). Dejstvo je, če nihče ne pozna šifrirnega mehanizma, ki smo ga implementirali v kriptografski sistem, ne more izvesti napada s preizkušanjem vseh možnih ključev. Lahko trdim, da javno objavljeni in

standardizirani šifrirni algoritmi niso primerni za zaščito informacij in podatkov, ki so nacionalnovarnostnega značaja. Javno objavljeni šifrirnih algoritmov ne poznamo dovolj dobro, ki lahko na prvi pogled izgledajo varni pa čeprav niso. Dejstvo je tudi, da minimalni standardi in kriptografski mehanizmi ter postopki, ki jih predpisujeta EU in zveza NATO, niso primerni za zaščito informacij in podatkov, ki so strateškega pomena za Slovenijo. Slovenija bi morala z ustanovitvijo posebnega organa (službe) izdelati tudi enotno kriptografsko politiko (ki bi opredeljevala tudi uvoz in izvoz kriptografske opreme), izdelati merila za vrednotenje kriptografskih izdelkov in kar je najpomembnejše, izdelati enoten sistem kriptozaščite. Na podlagi te ugotovitve lahko delno potrdim tretjo hipotezo, ki se glasi: *'Kriptografski sistemi so pomembni varnostni mehanizmi, ki se uporabljajo za izpolnitev varnostnih zahtev na področju nacionalne varnosti in so najvarnejši takrat, ko jih država patentira sama.'* Hipotezo potrjujem delno zato, ker se kriptografski sistemi uporabljajo tudi na drugih področjih zasebnega in javnega življenja. Z zasebnim področjem mislim predvsem zaščito elektronskega poslovanja (elektronska pošta, transakcije), zaščito računalniških datotek in programov, internetnega omrežja, z javnim področjem pa zaščito telekomunikacij in pametnih kartic.

[8] Na podlagi analize, ki sem jo opravila v diplomski nalogi, lahko trdim, da kriptografija in kriptoanaliza predstavljata pomemben del nacionalnovarnostnega sistema. Ugotovila sem že, da s pomočjo učinkovite kriptozaščite zagotavljamo minimalno stopnjo varnosti na različnih področjih. Tako kot je kriptologija lahko 'orožje' za obrambo, je lahko tudi 'orožje' za napad. Teroristična organizacija Hamas je s pomočjo šifriranih sporočil pošiljala zemljevide, slike in druge podrobnosti, ki so potrebne pri načrtovanju napada. Kriptoanaliza se uporablja v primerih, kot so: vdori v bančne sisteme, prisluškovanje, vdori v različne vladne organizacije, kraja identitet in še bi lahko naštevala. Mnoge države so uvedle in sprejele ukrepe, ki omejujejo uporabo, izvoz in uvoz kriptografske opreme. V večini držav je uvoz ali izvoz omejen oziroma celo prepovedan. S tako politiko želijo predvsem preprečiti uporabo kriptografske opreme v državah, ki tako ali drugače podpirajo terorizem ali pa so celo vpletene v vojaške spopade. Nekateri viri celo navajajo, da se je kriptografija uporabljala tudi pri

načrtovanju terorističnega napada 11. septembra v ZDA. Prav ta dogodek je v ZDA vzpodbudil nekatere nov ideje o omejitvi uporabe kriptozaščite. Na podlagi te ugotovitve lahko potrdim četrto hipotezo, ki se glasi: *'Kriptografija in kriptoanaliza imata pomembno vlogo na področju nacionalne varnosti, lahko jo zagotavljata ali ogrožata'.*

Republika Slovenija počasi ureja zakonodajo in varnostno politiko, ki bosta opredeljevali področje kriptozaščite. Iz napisanega je razvidno, da nas do ureditve celovitega in učinkovitega kriptosistema, ki bo varoval informacije in tajne podatke, čaka še veliko dela. Podrobno bo potrebno urediti celotno varnostno politiko, ki bo morala upoštevati vse poglede varnosti. Rezultate načrtovanja varnostne politike je potrebno obravnavati kot verigo, kjer pri optimalno zasnovanih ciljih vedno obstaja možnost zloma najšibkejšega člena. Pomembno vlogo pri urejanju tega področja bo gotovo imel Urad Vlade Republike Slovenije za varovanje tajnih podatkov, ki nastopa kot nacionalno varnostni organ (seveda samo v primeru, če ne bo ustanovljen nov organ).
Kriptografske in kriptoanalitične metode so se dobro uveljavile na vseh področjih. Prepričana sem, da se bodo metode in tehnike razvijale vzporedno z napredkom ostale tehnologije ter da bo patentiranih še več programov, kot je PGP, ki je postal standard za učinkovito zaščito informacij in podatkov.

SEZNAM SLIK IN TABEL

12 SEZNAM VIROV

a) Knjige

1) ANŽIČ, Andrej (1997): Varnostni sistem Republike Slovenije. Ljubljana: Uradni list RS.
2) BAUER, L. Friederich (1997): Decrypted Secrets, Methods and Maxims of Cryptology. Germany: Springer-Verlag Berlin Heidelberg.
3) BUCHMANN, Johannes (2000): Introduction to Cryptography. New York, Berlin, Heidelberg: Springer-Verlag.
4) EGAN, Mark in MARHER, Tim (2005): Varnost informacij, Grožnje, izzivi in rešitve. Ljubljana: Založba Pasadena.
5) ČUKLJAŠ, Đuro (1994): Tajno komuniciranje špijuna. Zagreb : Ministarstvo unutarnjih poslova.
6) GRIZOLD, Anton (1999): Obrambni sistem Republike Slovenije. Ljubljana: Visoka policijso-varnostna šola.
7) JERMAN-BLAŽIČ, Borka, SCHNEIDER, Wolfgang, KLOBUČAR, Tomaž (2004): Security and Privacy in Advanced Networking Technologies. Netherlands: IOS Press.
8) KAHN, David (1996): The codebreakers : The story of secret writing. New York: Scribner, cop.
9) KRIČEJ, Dušan (2002): E-uprava na dlani. Ljubljana: Založba Pasadena.
10) KRIPTOGRAFIJA (1977): Beograd: Savezni sekretarijat za narodnu odbranu. (Ime in priimek avtorja v knjigi nista navedena.)
11) KOVAČIČ, Matej (2003): Zasebnost na internetu. Ljubljana: Mirovni inštitut za sodobne družbene in politične študije.
12) MAO, Wenbo (2004): Modern Cryptography: teory and practice. Upper Saddle River (NJ) : Prentice Hall PTR, cop.
13) MENEZES, J. Alfred, van OORSCHOT, C. Paul, VANSTONE, A. Scott (1996): Handbook of Applied Cryptography. Florida, USA: CRC Press, Inc.
14) STAMP, Mark (2006): Information Security: Principles and Practice. Canada: John Wiley & Sons, Inc.
15) SCHNEIER, Bruce (1996): Applied Cryptography, second edition. Canada: John Wiley & Sons. Scribner, cop.

16) SEBAG-MONTEFIORE, Hugh (2002): Enigma : The battle for the code. London: Phoenix.
17) SVETE, Uroš (2005): Varnost v informacijski družbi. Ljubljana: Fakulteta za družbene vede.

b) Strokovni in znanstveni članki

1) ANŽIČ, Andrej (2001): Tajnost kot družbeni fenomen – varnostni vidiki. Varstvoslovje, letnik 3, številka 1–2, stran 33–41.
2) ANŽIČ, Andrej in TRBOVŠEK, Franc (2003): Varnostno preverjanje v NATO po novih standardih. 4. slovensnki dnevi varstvoslovja: Ljubljana: Visoka policijsko-varnostna šola.
3) BROŽIČ, Liliana in ČERNETIČ, Metod (2003): Potrebe po novih znanjih – varovanje tajnih podatkov v Evropski uniji in zvezi NATO. Organizacija, letnik 36, šteilka 8.
4) BROŽIČ, Liliana (2003): Proces vključevanja v Evropsko unijo in zvezo NATO – potrebe po usposabljanju na področju varnosti. 4. slovenski dnevi varstvoslovja: Ljubljana: Visoka policijsko-varnostna šola.
5) ČALETA, Denis (2003): Sistem varovanja tajnih podatkov v Slovenski vojski. 4. slovensnki dnevi varstvoslovja: Ljubljana: Visoka policijsko-varnostna šola.
6) ČALETA, Denis (2004): Konceptualne spremembe na področju varovanja tajnih podatkov v Republiki Sloveniji. 5. slovenski dnevi varstvoslovja: Ljubljana: Visoka policijsko-varnostna šola.
7) ČAS, Tomaž (2005): Varnost, nacionalna varnost, zasebna varnost. 6. slovenski dnevi varstvoslovja: Ljubljana: Visoka policijsko-varnostna šola.
8) JERMAN BLAŽIČ, Aljoša (2004): Informacijska varnost. Ljubljana: Revija Monitor, letnik 14, številka 6, stran 60–68.
9) JURIŠIĆ, Aleksandar in TONEJC, Jernej (2001): Nove tehnologija, Pametne kartice in varnost. Ljubljana: Revija Monitor, letnik 11, številka 6, stran 66–75.
10) JURIŠIĆ, Aleksandar in TONEJC, Jernej (2001): Nove tehnologija, Pametne kartice – Zasebno življenje javnih ključev. Ljubljana: Revija Monitor, letnik 11, Številka 7–8, stran 44–51.

11) JURIŠIĆ, Aleksandar in TONEJC, Jernej (2001): Nove tehnologija, Pametne kartice – 3.del, Napadi in obrambe malih kartic. Ljubljana: Revija Monitor, Letnik 11., številka 9, stran 54–64).
12) JURIŠIĆ, Aleksandar in PERKO, Urban (2005/2006): Klasične šifre in zdravstvene kartice (prvi del). Ljubljana: Presek, letnik 33., št. 1, str. 22–24.
13) KLOBUČAR, Tomaž (2001): Kako se elektronsko podpišemo. Revija Monitor, letnik 11, številka 5.
14) PODEŠVA Vlasta (2001): Vloga akademskih in raziskovalnih omrežij pri razvoju interneta in informacijske družbe. Kranj: Založba Moderna organizacija.
15) PREZELJ, Iztok (2002): Ogrožanje nacionalne varnosti Republike Slovenije in vključevanje v Nato. Teorija in praksa, 39, 3, str. 426–441.
16) ROZMAN, Janez (2003): Urad Vlade Republike Slovenije za varovanje tajnih podatkov, kot nacionalni organ za varovanje tajnih podatkov. 4. slovensnki dnevi varstvoslovja: Ljubljana: Visoka policijsko-varnostna šola.
17) ŠEFIC, Boštjan (2004): Svet za nacionalno varnost in njegova vloga v sistemu nacionalne varnosti Republike Slovenije. 5. slovensnki dnevi varstvoslovja: Ljubljana, Visoka policijsko-varnostna šola.
18) ZIDAR, Vojko (2003): Dileme kriptosistemov. 4. slovensnki dnevi varstvoslovja: Ljubljana, Visoka policijsko-varnostna šola.
19) ZIDAR, Vojko (2004): Organizacija informacijske varnosti v EU in doma. 5. slovenski dnevi varstvoslovja, Ljubljana: Fakulteta za policijsko-varnostne vede.

c) Viri z medmrežja

1) Center for Democracy & Technology (2005): http://www.cdt.org/crypto/ (12. 1. 2006).
2) Center Vlade RS za informatiko (1996–2006): Uporaba kriptografije v internetu: http://www.sigov.si/tecaj/kripto/ (15. 9. 2005–15. 6. 2006)
3) Certifikatna agencija, Halcom-ca (2006): http://www.halcom-ca.si/slo/infrastruktura_podpis.html (20. 1. 2006).
4) Codes and Ciphers Heritage Trust (2005): http://www. Bletchleyparkheritage.org.uk/ModSec.htm (06. 1. 2006).

5) Cryptanalysis (2005): http://en.wikipedia.org/wiki/Cryptanalysis (21. 12. 2005).
6) Cryptography and Liberty 1999: http://www.gilc.org/crypto/crypto-survey-99.html (15. 4. 2006).
7) Deželna banka Slovenije d.d. (2004): DBS NET, Varnost poslovanja: https://dbsnet.dbs.si/eban/docs/Varnost_poslovanja.pdf (01. 2. 2006).
8) DOBNIKAR, Aleš (2003): Digitalna potrdila SI*CA namen, zakonodaja, standardi: http://lms.uni-mb.si/vitel/14delavnica/ predstavitve / ppt-davorka_sel.pdf (30. 4. 2006).
9) Enigma (2006): http://sl.wikipedia.org/wiki/Enigma_%28naprava%29 (06. 1. 2006).
10) Encryption (1997), http://www.eco.utexas.edu/faculty/ Norman/ BUS. FOR/ course.mat/SSim/ index.html (5. 1. 2006).
11) Evropska unija: http://europa.eu.int/
12) Famous people in the history of Cryptography: http://web.it. kth.se/ ~ rom/ cryptopeople.html (5. 1. 2006).
13) History of cryptography (2006): http://en.wikipedia.org/wiki/ History_of_ cryptography#Cryptography_from_1800_to_World_War_II (5. 1. 2006).
14) KOVAČIČ, Matej: Zasebnost na internetu, 3. del: http://www.ljudmila. org/matej/knjiga/zasebnost_3del.pdf (7. 1. 2006).
15) Microsoft (2006): Izboljšajte varnost s pametnimi karticami: http://www.microsoft.com/slovenija/windowsxp/pro/funkcije/pametne_kartice.mspx (1. 3. 2006).
16) Mitsubishi Electric Global (2006): http://global. mitsubishielectric. com/ misty/tour/stage1/ (5. 1. 2006).
17) National Cryptologic Museum (2006): http://www.nsa.gov/museum/ (5. 1. 2004).
18) National Security, Cryptography, and Personal Security: http://gsulaw.gsu.edu/lawand/papers/su95/dbcrypt2.html (10. 10. 2006).
19) NATO Slovenija: http://nato.gov.si/slo/
20) NATO: http://www.nato.int/
21) One-time pad (OTP) (2006): http://en.wikipedia.org/wiki/One-time_pad (5. 1. 2006).

22) Overitelj digitalnih potrdil, Ministrstvo za javno upravo (2006): SIGEN-CA: http://www.sigen-ca.si/politika-sigen-ca-fizicne-osebe.php (1. 3. 2006).
23) PELL, Oliver: Cryptology, http://www.ridex.co.uk/cryptology/ (10. 10. 2005).
24) PBS (2005): http://www.pbs.org/wgbh/nova/decoding/enigma.html (6. 1. 2006).
25) OSREDKAR, Radko: Kriptografija. Revija življenje in tehnika, objavljeno na: http://www.druga.org/~rusty/clanki/razno/kriptografija.shtml?razno (6. 1. 2006).
26) RIKSOFT, Software development & services (2006): Crittografia, http://www.riksoft.com/indexok.asp?Goto=crileon.htm (5. 1. 2006).
27) Raba interneta v Sloveniji (RIS) (2006): Proizvodnja pametnih kartic se bo povečala za 20%: http://www.ris.org/main/rubrika3/readrub3.php?sid=224 (1. 3. 2006).
28) STEGEL, Tine (2005): Varnost v telekomunikacija: http://www.it-akademija.net/kodiranje.pdf (21. 12 .2005).
29) The World (2004): http://world.std.com/~franl/crypto.html (10. 10. 2005).
30) Thiemo Mättig (2006): Enigma: http://maettig.com/?page=Studium/Enigma (6. 1. 2006).
31) TOMAŽIČ, Sašo: Varnost v telekomunikacijah in kako jo zagotoviti: http://www.ltfe.org/pdf/Varnost%20v%20telekomunikacijah.pdf(20. 1. 2006).
32) Uradni list RS: http://www.uradni-list.si.
33) University of Nebraska, Department of Computer Science and Engineering (2006): http://cse.unl.edu/~bholley/Cypher%20Tutorial.html (5. 1. 2006).
34) Vlada Republike Slovenije, Urad za varovanje tajnih podatkov (2006): Informacijska varnost: http://www.uvtp.gov.si/index.php?id=694 (30. 4. 2006).
35) VRTOVEC, Tomaž (2000): Varnostni vidiki telekomunikacijskih sistemov in storitev, Seminarska naloga: http://www-lt.fe.uni-lj.si/vaje/vaje_2000-2001/kso1/seminarji/KSO1_2000_Vrtovec_Varnostni_vidiki_TK_sistemov_in_storitev.pdf (15. 6. 2006).
36) ŽUMER, Maja (2006): Uvod v informacijsko tehnologijo: http://www.ff.uni-lj.si/oddelki/biblio/ uvinfznan . htm, 20. 1. 2006).

d) Dokumenti

1) Resolucija o strategiji nacionalne varnosti Republike Slovenije (ReSNV), Uradni list RS, št. 56-2957/2001.
2) Security into NATO, dokument C-M(2002)49, North Atlantic Council, 17. junnij 2002.
3) Security regulations 2001/264EC, Council Decision 19. merec 2001.
4) Sklep Vlade Republike Slovenije o določitvi organa, pristojnega za kriptografsko zaščito podatkov, razdeljevanje kriptografskega materiala in za zaščito pred neželjenim elektromagnetnim sevanjem naprav v informacijskih in telekomunikacijskih sistemih, ki se uporabljajo za obrambne namene, ter o organiziranju kurirske službe za prenos pošiljk s tajnimi podatki NATO. 58. redna seja, 22. 1. 2004.
5) Uredba Sveta (ES) št. 394/2006 z dne 27. februarja 2006 o spremembi in posodobitvi Uredbe (ES) št. 1334/2000 o vzpostavitvi režima Skupnosti za nadzor izvoza blaga in tehnologije z dvojno rabo, Uradni list Evropske unije, 13. 3. 2006.
6) Zakon o elektronskem poslovanju in elektronskem podpisu (ZEPEP-UPB1), Uradni list RS, št. 98/2004.
7) Zakon o obrambi, Uradni list RS, št. 103/2004.
8) Zakon o ratifikaciji sporazuma med pogodbenicami severnoatlantske pogodbe o varnosti podatkov (MSPSPV), Uradni list RS, št. 83/2004.
9) Zakon o tajnih podatkih uradno prečiščeno besedilo (ZTP-UPB1), Uradni list RS, št. 135/2003, Zakon o spremembah in dopolnitvah Zakona o tajnih podatkih (ZTP-B) Uradni list RS, št. 28/2006.

e) Ostalo

1) Annual International Cryptology Conference (1998): Advances in Cryptology – CRYPTO ¨99. Santa Barbara, Springer.
2) Annual International Cryptology Conference (1999): Advances in Cryptology – CRYPTO ¨99. Santa Barbara, Springer.
3) BRITANNICA DELUXE EDITION (2005): Elektronska izdaja: United Kingdom.

4) Center Vlade Republike Slovenije za informatiko (2003): Varnostni vidiki aplikacij z uporabo digitalnih potrdil SIGEN-CA in SIGOV-CA, Priporočila za aplikacije. Verzija: 1.0.
5) ČRNČEC, Damir (2003): Tajnost podatkov: (varnostno preverjanje in obveščevalno-varnostne službe). Magistrsko delo. Ljubljana, Fakulteta za družbene vede.
6) GUTMANN, Peter: Cryptography and Data Security. University of Auckland http:// www.cs.auckland. ac.nz/~ pgut001.
7) KOVAČIČ, Klemen (2001): Primerjava metod kriptografske zaščite informacij. Diplomska naloga. Ljubljana: Fakulteta za policijsko-varnostne vede.
8) PERENIČ, Gorazd (2001): Zakon o elektronskem poslovanju in elektronskem podpisu (ZEPEP in Uredba o pogojih za elektronsko poslovanje in elektronsko podpisovanje, Kratka pojasnila k zakonu. Ljubljana: Vlada Republike Slovenije, Center za informatiko.
9) Priročnik o zvezi NATO (2001): Office of information and Press NATO – 1110 Brussels – Belgium.
10) SILIČ, Marin (2001): Zakon o elektronskem poslovanju in elektronskem podpisu (ZEPEP in Uredba o pogojih za elektronsko poslovanje in elektronsko podpisovanje, Uvodna beseda. Ljubljana: Vlada Republike Slovenije, Center za informatiko.
11) SLOVAR SLOVENSKEGA KNJIŽNEGA JEZIKA (2002, elektronska izdaja v 1.0) SAZU in ZRC SAZU, Inštitut za slovenski jezik Frana Ramovša in avtorji: Ljubljana: DZS d.d.
12) SOKLIČ, Jure (2002): Vloga kriptografije v času druge svetovne vojne. Diplomska naloga. Ljubljana, Fakulteta za družbene vede.
13) VOJNA ENCIKLOPEDIJA (1974), Vojnoizdavački zavod, Beograd.
14) ŽIVEC, Andrej (2005): Zaščita tajnih podatkov. Diplomska naloga. Ljubljana: Fakulteta za policijsko-varnostne vede.