ISTORIJA KRIPTOGRAFIJE, KRIPTOGRAFSKIH ALGORITAMA I PAMETNIH KARTICA

Milena Jovanović[1]

1. UVOD

Historia est magistra vitae – istorija je učiteljica života, kažu stari Rimljani. Smisao ove poslovice se vidi i u istorijskom pregledu kriptografije, nauke o sigurnosti informacija koja predstavlja znanje "tajnog pisanja", tj. znanje prevođenja informacija u onoj formi koja će biti čitljiva samo onima kojima je informacija namijenjena, dok će za ostale biti neupotrebljiva. Istorija kriptografije je neobično zanimljivo područje ljudskog djelovanja, vrlo mistificirano, obavijeno velom tajni. U ljudskoj je prirodi imati tajne, a kada se žele saopštiti tada nastupa moć kriptografije, nauke u kojoj su ljudi kroz istoriju imali nevjerovatan broj kreativnih ideja, možda kao ni u jednoj drugoj oblasti.

U dalekoj prošlosti kriptografija se često povezivala sa crnom magijom, demonima i zlim silama. Nije tačno utvrđeno gdje su stvarni počeci kriptografije, ali je jedna od prvih poznatih praktičnih primjena oko 2000 g.p.n.e u Egiptu, gdje su korišćeni nestandardni hijeroglifi za ukrašavanje grobnica preminulih vladara, koji su opisivali njihov život i veličali uspjehe za vrijeme njihove vladavine. Ovi hijeroglifi su bili kodirani sa svrhom ne da se sakrije tekst, već da bi se tekst učinio važnim i dostojnim kralja. Ali vremenom ti zapisi su postajali sve komlikovaniji, pa se na kraju prestalo sa njihovom upotrebom [1].

Kriptografija je korišćena u staroj Indiji na taj način što su vladari koristili tajne šifre za komunikaciju sa svojim špijunima širom zemlje. Rane indijske šifre su se uglavnom zasnivale na jednostavnoj suspstituciji, često na osnovu fonetike. Neke od tih šifri su se koristile u govoru ili kao govor znakova. To je prilično slično “svinjskom latinskom” (eng. pig latin – igpay atinlay), gdje se prvo slovo stavlja na kraju riječi i dodaje se slog “ay”.

Kriptografska istorija Mesopotamije je slična egipatskoj, u smislu da su se i ovdje koristili znakovi (klinasto pismo) za kodiranje teksta. Tehnika takvog zapisivanja se koristila i u kulturama Asiraca i Vavilonaca. U Bibliji se ponekad koristi hebrejska šifra koja se zasniva na principu zamjene prvog i zadnjeg slova abecede, i obratno. Ta metoda se

[1] Mr Milena Jovanović, Elektrotehnički fakultet Podgorica..

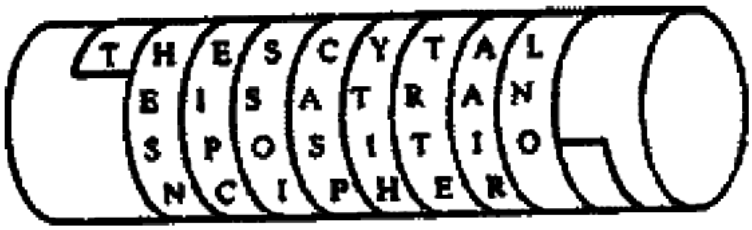
naziva "atbash". Na primjer, riječ "KRIPTOGRAFIJA" se upotrebom ove šifre pretvara u "PIRKGLTIZURQZ".

ABCDEFGHIJKLMNOPQRSTUVWXYZ
ZYXWVUTSRQPONMLKJIHGFEDCBA

Tabela 1. Atbash kod za engleski jezik

Stari Kinezi su koristili ideografsku prirodu svog jezika za sakrivanje pravog značenja riječi. Poruke su često bile transformisane u ideograme (ideogram - poruka prenesenog značenja, pravo značenje zna samo primalac poruke) u svrhu privatnosti.

Spartanci su koristili način kriptovanja koji se sastojao od tankog lista papirusa koji se motao oko *scytale* – kraj drške kosilice. Na papirusu bi ispisivali slovo ispod slova, a tajna poruka se nalazila u nizovima slova koji su paralelni osi drške. Da bi se poruka mogla pročitati, potreban je štap istog poprečnog presjeka i dužine.



Slika 1. Prikaz "spartanskog kraja drške kosilice"

Julije Cezar upotrebljavao je tzv. Cezarovu šifru kojom je cijelu abecedu ciklično pomjerio za dva mjesta udesno. Ovakav način kodiranja se zove transpozicija.

Starogrčku metodu kodiranja razvio je Polybius (sada se ta metoda zove Polybius-ov kvadrat). Slova abecede se postavljaju u 5*5 kvadrat, a redovi i kolone se numerišu od 1 do 5 tako da se svako slovo može predstaviti sa parom reda i kolone. Ovi su se parovi mogli lako signalizirati bakljama ili rukama. Dekriptovanje se vrši pridruživanjem odgovarajućeg slova abecede svakom od parova.

1 2 3 4 5	
1|A B C D E	B = 21
2|F G H I J	H = 32
3|K L M N O	N = 43
4|P Q R S T	S = 44
5|U V W X Y/Z	V = 25

Tabela 2. Polybius-ov kvadrat

Treba napomenuti da se paralelno sa razvojem kriptografije razvila i oblast - kriptoanaliza, kojoj je cilj da analizom kriptovane poruke odgonetne njen sadržaj, bez potpunog poznavanja šifre [2].

Prvi koji su značajnije doprinijeli napretku kriptoanalize bili su Arapi. Qalqashandi je autor koji je zapisao tehniku za razbijanje šifri koja se koristi još i danas. Tehnika se zasniva na tome da se zapišu svi znakovi iz kodiranog teksta i prebroji koliko puta se pojavio svaki od tih znakova u tekstu. Ako sada na te podatke primijenimo podatak koliko se često koje slovo pojavljuje u jeziku kojim je pisana poslata poruka, možemo otkriti koji simbol kodirane poruke predstavlja koje slovo abecede jezika poslate poruke, a to znači i napisati poslatu poruku. Ova tehnika omogućava razbijanje bilo koje šifre zasnovane na monoalfabetskoj supstituciji ako ima dovoljno kodiranog teksta.

U srednjem vijeku do prvog većeg napretka dolazi u Italiji, konkretno u Veneciji koja 1452. godine osniva državnu instituciju čija je jedina namjena bila kriptografija. Leon Battista Alberti je poznat kao otac zapadne kriptologije zbog svog izuma polialfabetne supstitucije (bilo koja tehnika kodiranja koja dopušta da više različitih znakova u kriptovanom tekstu predstavlja jedan znak poslatog teksta). Primjena te metode značajno otežava dekodiranje primjenom metode analize frekvencije pojavljivanja znakova [3].

2. RAZVOJ KRIPTOGRAFIJE (16. – 21. VIJEK)

U šesnaestom vijeku tehnika kodiranja se unapređuje korišćenjem Trithemius-ove tablice koju je razvio istoimeni njemački fratar 1518. godine i objasnio u šest knjiga pod nazivom *Polygraphia* (tzv. kodne knjige) [4]. U petoj knjizi Trithemius razvija tablicu koja je u svakom redu ponavljala cijelu abecedu, ali je abeceda u svakom sljedećem redu bila ciklično pomjerena za jedan znak udesno. Da bi se poruka kodirala, prvo slovo poruke se kodiralo prvim redom tablice, drugo drugim, itd. Takva metoda proizvodi kodiranu poruku u kojoj su sve raspoložive šifre iskorišćene prije nego što su ponovljene.

1553. godine Giovanni Battista Belaso unaprijeđuje ovu tehniku upotrebom ključa koji se zapisuje iznad originalnog teksta, i to tako da svako slovo ključa stoji iznad jednog slova originalnog teksta. Slovo ključa koje je iznad slova teksta koji se želi kriptovati, određuje red iz Trithemius-ove tablice kojim ćemo kodirati to slovo. Dakle, ako je slovo u originalnom tekstu *b*, a iznad njega je slovo ključa *r*, za kodiranje slova *b* ćemo koristiti red u Trithemius-ovoj tablici koji počinje sa *r*.

Najpoznatiji kriptograf ovog vremena bio je Blaise de Vegnere (1523. - 1596.) koji je 1585. godine napisao *Traicte des Chiffres*, djelo u kojem je upotrijebio Trithemius-ovu tablicu, ali je promijenio način njene upotrebe [5]. Jedna od njegovih metoda koristila je originalni tekst kao ključ za kodiranje samog sebe, dok je druga koristila kodirani tekst kao ključ. Način na koji su korišćeni ovi ključevi poznat je kao raspoređivanje ključeva (*key scheduling*), i on se koristi pri kreiranju jednog od najpoznatijih kriptografskih algoritama današnjice - DES algoritma.

U Engleskoj je kriptografija uzela maha tek za vrijeme Kraljice Elizabete. U Londonu je organizovana tajna služba sa 53 zaposljena agenta čiji je cilj bio da zaštite kraljicu od stranih neprijatelja, kao i zavjerenika unutar zemlje. Najpoznatiji kriptoanalitičar tog vremena Anthony Bacon, koji je mogao da analizira kodove na pet jezika, dekodirao je uhvaćenu poruku od škotske Kraljice Mary, koja je dovela do njenog vješanja zbog izdaje.

Brat Anthony Bacon-a, Francis Bacon, opisao je šifru koja danas nosi njegovo ime (biliteralni kod) i koja je poznata kao 5-bitno binarno kodiranje.

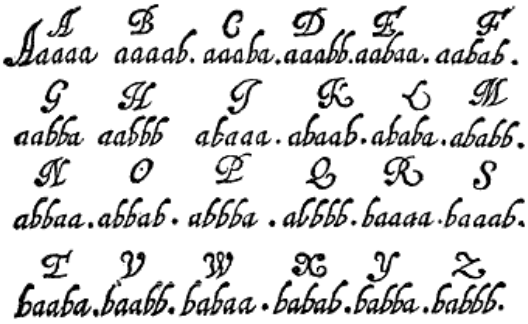


Tabela 3. Primjer biliteralne abecede

1628. godine Francuz Antoine Rossignol je pomogao svojoj vojsci da pobijedi Hugenote tako što je dekodirao zarobljenu kodiranu poruku. Nakon ove pobjede, još je mnogo puta razbijao kodove za francusku vladu. Kreirao je dvije liste za razbijanje kodova: "jednu u kojoj su elementi originalnog teksta u poretku od a do z, a kodirani elementi bez poretka, i drugu u kojoj se vrši dekodiranje kada su kodirani elementi u poretku od a - z ili od manjih prema većim brojevima, a originalni tekst bez poretka." Kada je Rossignol umro 1682. godine, njegov sin, a kasnije i unuk, nastavili su njegov posao. U ovo doba se u Francuskoj već mnogo ljudi bavi kriptografijom, pa vlada osniva agenciju pod nazivom Cabinet Noir (mračni kabinet) kojoj je bio cilj izrada sigurnih šifri, a još više probijanje suparničkih.

Ipak, najpoznatiji Cabinet Noir nalazio se u Beču, a zvao se "Geheime Kabinets - Kanzlei". Ova je organizacija čitala svu poštu koja je stizala stranim veleposlanstvima u Beču, kopirala ih, ponovo zatvarala i vraćala u poštansko sanduče to isto jutro. Taj isti kabinet se bavio dekodiranjem i ostalih presretnutih vojnih i političkih poruka, a ponekad bi pročitao i do 100 pisama dnevno. Engleski "Mračni kabinet" formirao je John Wallis 1701. godine, koji je i prije za englesku vladu razbijao kodove, ali pod raznim drugim neslužbenim funkcijama. Nakon njegove smrti 1703. godine njegov unuk William Blencowe, koga je on podučavao, preuzeo je njegovu funkciju i bila mu je dodijeljena titula dekoderanta. Engleski Cabinet Noir ima dugu i uspješnu karijeru u svijetu kriptografije.

U kolonijama evropskih velesila nije bilo centralizovane kriptografske organizacije kao što je to u Evropi bio Cabinet Noir. Dekodiranjem su se uglavnom bavili zainteresovani pojedinci i sveštenstvo. 1775. godine američki revolucionari su presreli pismo koje je poslao dr. Benjamin Church i za koje su sumnjali da je kodirana poruka Britancima, ali je nisu uspjeli dekodirati. Kod su razbili Elbridge Gerry, koji je kasnije postao peti potpredsjednik SAD-a, i Elisha Porter. Poruka je dokazala da je Church zaista želio upozoriti Britance, pa je kasnije prognan.

Benedict Arnold V, američki general koji se borio za nezavisnost Amerike od Britanskog Carstva, napravio je kod za koji je svaki od korisnika imao isti primjerak "Knjige šifri". Svaka riječ originalnog teksta zamijenila bi se brojem koji je označavao

njen položaj u knjizi (npr. 3.5.2 znači stranica 3, red 5, riječ 2). Čovjek s kojim se Arnold dopisivao pomoću tog koda je uhvaćen i obješen, pa se Knjiga šifri nije mnogo koristila. Za oca američke kriptologije smatra se James Lovell koji je bio na strani boraca za nezavisnost i razbio mnoge britanske šifre, od kojih su neke omogućile pobjedu pobunjenika. Jedna od poruka koje je on dekodirao je čak omogućila konačnu pobjedu u završnom dijelu rata za nezavisnost.

Najznačajniji kriptografski izum osamnaestog vijeka je Thomas Jefferson-ov instrument za kodiranje sa točkovima (*wheel cipher*), a jako slični ovom su se koristili u mornarici SAD-a do prije nekoliko godina [6]. Ovaj instrument se sastoji od skupa točkova, pri čemu je svaki sa nasumičnim rasporedom slova abecede, a najvažnija stvar jeste raspored točkova na osovini. Naime, poruka se kodira tako što se okretanjem točkova slože slova koja čine poruku u jednom redu, točkovi se zatim međusobno fiksiraju, a bilo koji drugi red slova se koristi kao kodirana poruka. Dekodiranje se vrši tako što se na istom takvom instrumentu, sa istim točkovima i istim rasporedom točkova na osovini poređaju slova koja čine kodiranu poruku u jedan red, zatim se točkovi međusobno fiksiraju i okreću, dok se ne pojavi poruka koja ima lingvističkog smisla. Vjerovatnoća pojave dvije lingvistički smislene poruke je minimalna. Ovakav način kodiranja poruka siguran je samo za jednokratnu upotrebu, jer je razbijanje koda moguće statističkim napadima, ako se isti točkovi koriste na isti način više puta.

Slika 2. Thomas Jefferson-ov instrument za kodiranje sa točkovima

Nakon izuma telegrafa 1844. godine dolazi do naglih promjena na području kriptografije - komuniciranje telegrafom bilo je vrlo nesigurno, pa su kvalitetne šifre postale nužnost pri prenosu tajnih informacija, posebno za vrijeme rata. U početku se koristila Vigenere-ova šifra sa kratkom ponavljajućom ključnom riječi, ali je 1863. godine Francuz Friedrich W. Kasiski otkrio rješenje za razbijanje svih periodičnih polialfabetnih kodova, koji su do tada smatrani neprobojnima. Ta metoda se sastojala u pronalaženju ponovljenih nizova znakova u kodiranom tekstu. Udaljenost među tim ponavljanjima se koristi za računanje dužine ključa nalaženjem najvećeg zajedničkog djelitelja svih izračunatih dužina među ostvarenim ponavljanjima. Jednom kad saznamo dužinu ključa (N), možemo upotrijebiti statistiku na svakom N-tom znaku. Frekvencija upotrebe tog

znaka implicira koje slovo on predstavlja u toj zbirci simbola kodiranog teksta. Ova vrsta ponavljanja može se desiti sasvim slučajno, pa je nekada potrebno nekoliko pokušaja za nalaženje prave dužine ključa ovom metodom, ali je i to značajno efikasnije od prethodno korišćenih metoda. Ova tehnika probijanja čini kriptoanalizu polialfabetne supstitucije prilično jednostavnom.

Playfair sistem kodiranja su izumjeli Charles Wheatstone i Lyon Playfair 1854. godine, i to je bio prvi sistem koji je koristio parove znakova u kodiranju [7]. Abeceda se nasumično smješta u kvadrat veličine 5*5 slova, a tekst koji se želi kodirati dijeli se u parove međusobno susjednih slova. Slova koja čine par nalaze se u kvadratu, a zatim se formira kvadrat čiji su dijagonalno suprotni vrhovi slova koja čine par. Preostala dva vrha kvadrata čine zamjenski par kodiranog teksta. Kod je vrlo jednostavan za upotrebu, ali nije složen za razbijanje. Prava vrijednost ovog sistema kodiranja je upotreba parova slova čime je uticaj statistike jezika u kojem je pisana originalna poruka bitno smanjen, pa se time povećavaju i vrijeme i količina kodiranog teksta potrebnih za probijanje koda. Sistem se često koristio u drugom svjetskom ratu, i bio je posebno primjenjivan od strane SAD protiv Japana.

IKMNQ
LPBYF
CWEDX
GZAHU
RSTOV

KRIPTOGRAF = KR IP TO GR AF
SILKOTRGUB = SI LK OT RG UB

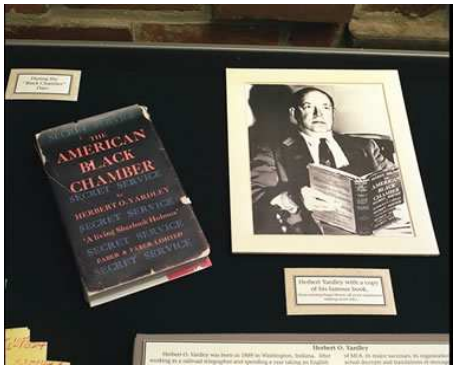
Tabela 4. Primjer playfair sistema

Tokom američkog građanskog rata (1861. - 1865.) kodovi nijesu bili naročito složeni. Mnoge tehnike su se sastojale samo od pisanja riječi drukčijim redosljedom i zamjene naziva ključnih lokacija i imena. Kad je Sjever centralizovao kontrolu nad kodovima, Jug je dozvolio svojim zapovjednicima da odlučuju sami o načinima kriptovanja. Zapovjednici su masovno koristili Vigenere-ov kod, što je često dovodilo do situacija da kriptoanalitičari na Sjeveru brže probiju šifru i pročitaju poruku od Južnjaka. Južnjaci su koristili tri ključa za kodiranje većine svojih poruka tokom rata: "Manchester Bluff", "Complete Victory", "Come Retribution". Ove su riječi vrlo brzo otkrili trojica kriptoanalitičara Tinker, Chandler i Bates, tako da su poruke kodirane tim ključevima redovno dekodirane. Upotreba uobičajenih, često korišćenih riječi za ključ je uzrokovala probijanje mnogih kodova.

Izum radia 1895. godine je značio veliku promjenu na području kriptografije, kao što je to predstavljao izum telegrafa 1844. godine. Najveći problem kod slanja kodiranih poruka radiom je bio taj da je poslate poruke svako mogao uhvatiti, pa nije više bilo fizičke sigurnosti podataka koju je pružao telegram. Francuzi su do prvog svjetskog rata imali mnogo radio "sobica" i presretali su većinu njemačkih radio poruka.

Slika 3. Unutrašnjost "sobice" za presretanje radio poruka

Početak 20. vijeka je obilježilo iščekivanje neizbježnog ratnog sukoba, pa su se u sklopu ratnih priprema ulagala velika sredstva i u kriptoanalizu. Najveći pomak naprijed napravila je Engleska koja je u vrijeme početka rata bila u mogućnosti da probije većinu neprijateljskih kodova. Najveći uspjesi su postignuti u razbijanju njemačkih mornaričkih kodova - probijanje tih kodova je bilo znatno olakšano jer su Njemci često za ključeve koristili riječi političkog ili nacionalističkog karaktera, mijenjali ključeve u pravilnim razmacima, odavali lako uočljive znakove da su promijenili ključeve, itd.



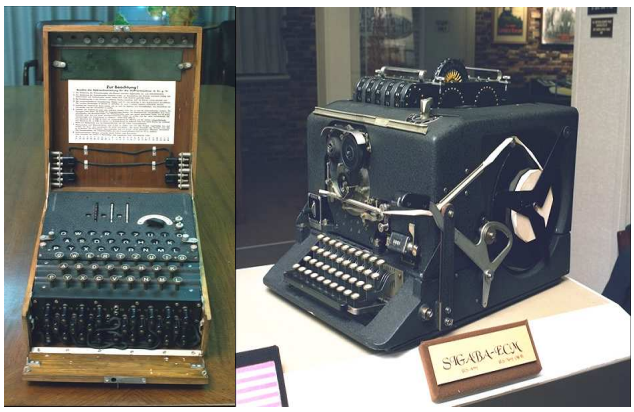
Slika 4. Herbert Osborne Yardley i njegova knjiga "Američki mračni kabinet"

1917. godine Amerikanci su formirali kriptografsku organizaciju MI-8 (Military Intelligence, Department 8) na čelu sa Herbert Osborne Yardley-em, koja je vršila analizu svih vrsta tajnih poruka, uključujući tajne tinte, šifre i kodove [8]. Nastavili su vrlo uspješno djelovati i nakon prvog svjetskog rata, ali je 1929. godine Herbert Hoover odlučio da zaustavi njihov rad jer je smatrao nepristojnim "čitanje tuđe pošte". Yardley je očajnički

tražio posao tokom velike ekonomske krize da bi prehranio porodicu, pa je napisao knjigu u kojoj je opisao djelovanje MI-8. Naslov knjige je bio "Američki mračni kabinet" koja je postala bestseller. Mnogi su ga kritikovali zbog objavljivanja državnih tajni i veličanja svojih djela tokom rata.

Sve do 1917. godine poruke koje su slate telegrafom bile su kodirane Baudot kodom za ispisivanje na teletipkaču [9]. Američka kompanija za telefon i telegraf (AT&T) bila je zabrinuta zbog lakog čitanja tako poslanih poruka, pa je Gilbert S. Vernam razvio uređaj koji je povezivao električne pulseve originalnog teksta sa električnim pulsevima ključa i na taj način proizvodio kodirani tekst. Ovaj sistem je bio težak za upotrebu, jer su u to vrijeme ključevi bili nezgrapni. Upotreba uređaja u kodiranju je značajno promijenila prirodu kriptografije i kriptoanalize. Kriptografija je postala usko vezana za dizajn strojeva, a važnost tih strojeva je uzrokovala i njihovu zaštitu. Osnovni sistemi kodiranja ostaju isti, ali metode kodiranja postaju pouzdane i elektromehaničke.

Sljedeći veliki napredak u elektromehaničkoj kriptografiji bio je izum specijalnog rotora. Njega čini debeli disk sa dvije strane, od kojih je svaka sa 26 kontakata odvojenih izolacionim materijalom. Pri tome je svaki kontakt sa strane za unos poslatog teksta žicom nasumično spojen sa jednim kontaktom sa druge strane za izlaz kodiranog teksta. Svakom kontaktu pridruženo je jedno slovo alfabeta. Električni impuls sa kontakta na strani poslatog teksta rezultiraće nasumičnim slovom sa druge strane rotora. Ovakav jednostavni rotor obavlja monoalfabetnu supstituciju i ugrađen je u uređaj u koji korisnik unosi javni tekst preko pisaće mašine. Jedna među najpoznatijim elektromehaničkim mašinama sa rotorima je Enigma, koju su Njemci koristili za kodiranje poruka u toku Drugog Svjetskog rata. Britanska vlada je 1974. godine dozvolila objavljivanje teksta o razbijanju Enigme, ali ni do danas nijesu poznati svi detalji [10].

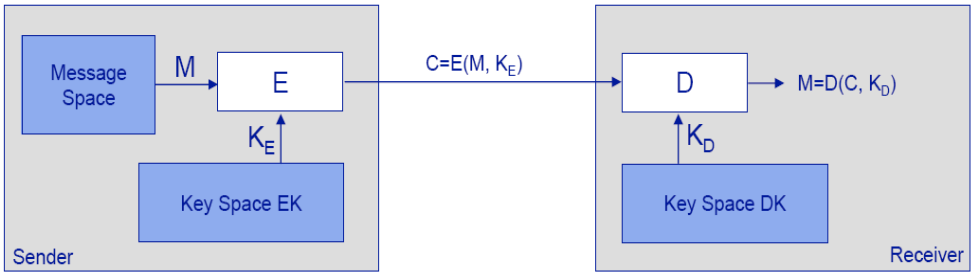


Slika 5. Enigma i njen američki suparnik M-134-C SIGABA

3. KRIPTOGRAFSKI ALGORITMI

Tek su se razvojem računara otvorile mogućnosti implementacije složenih algoritama koji bi bili nezamislivi u doba metoda supstitucije, transpozicije, elektromehaničkih mašina. Prvim većim napretkom u komjuterskom dobu smatra se razvoj IBM-ovog (*International Business Machines*) algoritma Lucifer 1970. godine pod vođstvom Dr. Horsta Feistela [11]. NBS (*National Bureau of Standards*) 1972. godine uočava potrebu za standardom kriptovanja podataka i nakon konsultacija sa NSA (*National Security Agency*), 15. marta 1973. godine otvara službeni konkurs. Međutim, pokazalo se da nijedan od pristiglih kandidata nije ispunjavao stroge kriterijume konkursa, pa se otvara novi konkurs 27. oktobra 1974. godine. Na ovom konkursu je IBM prijavio algoritam DEA (*Data Encryption Algorithm*), razvijen na osnovama algoritma Lucifer. 1976. god. ovaj algoritam je proglašen standardom kriptovanja i preimenovan u DES (*Data Encryption Standard*) i još uvijek predstavlja jedan od najčešće korišćenih i spominjanih algoritama kriptovanja.

Metode kriptovanja svih kriptografskih algoritama se po Kerckhoff-ovom principu zasnivaju na upotrebi ključa, koji uz pomoć logičkih operacija nad binarnim zapisom podataka kriptuje datu poruku. Ključ je najvažniji dio u kriptovanju i dekriptovanju poruka. Zaštita kriptovane poruke zavisi od zaštite ključa, a ne od zaštite algoritma. U zavisnosti od načina korišćenja ključa, razvile su se dvije klase algoritama [12]. Jedna je simetrična klasa, a druga je asimetrična klasa. Osnovna razlika je u tome da simetrični algoritmi koriste isti ključ za enkripciju i dekripciju neke poruke ($K_E = K_D$), ili se ključ za dekripciju može lako proizvesti iz originalnog ključa za enkripciju koji mora biti tajni. Sigurnost komunikacije zavisi od toga koliko sigurno učesnici komunikacije čuvaju taj ključ. Asimetrični algoritmi koriste različite ključeve za enkripciju i dekripciju iste ($K_E \neq K_D$), a još se nazivaju i algoritmi sa javnim ključem (*public-key algorithms*) ili algoritmi za razmjenu ključeva. Razlog ovakvom nazivu je taj što je ključ za enkripciju javan, tako da svako može da enkriptuje poruku, ali je ključ za dekripciju privatan, tako da samo ovlašćeni primalac može dekriptovati poruku.



Slika 6. Princip rada simetričnih i asimetričnih algoritama

Zamisao o kriptografiji javnih ključeva javnosti su predstavili Whitfield Diffie i Martin Hellman kroz svoj rad "Novi pravci u kriptografiji" koji je objavljen 1976. godine [13]. U to vrijeme je postojala samo simetrična kriptografija, a kao standard kriptovanja i osnovni algoritam baziran na simetričnoj kriptografiji postojao je DES sa 64-bitnim ključem. Diffie

i Hellman su svoj rad zaključili sa primjedbom: "Vještina u razbijanju kodova je uvijek bila na strani profesionalaca, ali je inovacija, posebno izumi novih metoda kriptovanja, dolazila od strane amatera."

Inspirisani radom Diffie-a i Hellman-a, a sami potpuni početnici u kriptografiji, Ronald R. Rivest, Adi Shamir i Leonard M. Adleman su napisali RSA algoritam, koji je naziv dobio po inicijalima svojih tvoraca. RSA predstavlja praktični kod sa javnim ključevima koji se mogao koristiti i za kodiranje poruka i za digitalni potpis, a bazirao se na teškoći faktorizacije velikih brojeva [14]. Rad je objavljen u časopisu Scientific American 1977. godine. U članku u kojem je opisan RSA nalazila se i ponuda da se pošalje potpuna tehnička specifikacija svakome ko pošalje adresiranu kovertu sa plaćenom poštarinom. Došlo je na hiljade takvih koverata iz cijelog svijeta. U NSA-u (*National Security Agency*) je prigovoreno zbog slanja te specifikacije u inostranstvo, pa je distribucija RSA algoritma jedno vrijeme zaustavljena. Tvorci RSA algoritma nijesu bili upoznati sa odredbom o tajnosti patenata, pa su rad objavili prije prijave za međunarodni patent.

1990. godine Xuejia Lai i James Massey su u Švajcarskoj objavili "Prijedlog za novi Standard za kodiranje blokova podataka", tj. prijedlog za IDEA-u (*International Data Encryption Algorithm*), koji je trebao zamijeniti algoritam DES. IDEA koristi 128-bitni ključ i operacije koje je lako implementirati na računaru, čineći ga u praksi vrlo efikasnim.

U periodu od 1990. – 1998. godine nastaju svi simetrični algoritmi iz grupe DES: TDEA (*Triple Data Encryption Algorithm*), Blowfish, Feal, Ice, Khufu, MacGuffin, NewDES, RC2, RC5, Shark.

Početkom 90-tih američka vlada, tačnije NIST (*National Institute of Standards and Technology*) uviđa potrebu za novim standardom u enkripciji koji bi zadovoljavao sigurnosne zahtjeve u dolazećim godinama i zamijenio dotadašnji standard, više ne tako sigurni DES algoritam. Na izboru za AES (*Advanced Encryption Stanadard*) algoritam 2000. godine, za pobjednika je izabran Rijndael koji je nazvan po prezimenima svojih tvoraca Vincent Rijmen-a i Joan Daemen-a [15]. NIST je kao svoje razloge odabira Rijndael-a naveo vrlo dobro ponašanje u hardware i software implementaciji u različitim uslovima, odličan key-setup i niske memorijske zahtjeve. U 2006. godini AES je proglašen za najpopularniji i najčešće korišćeni simetrični algoritam kriptovanja. Precizno govoreći, AES se razlikuje od Rijndael-a jer koristi fiksnu dužinu bloka od 128 bita, dok Rijndael koristi promjenljivu dužinu bloka od 128, 192 ili 256 bita. Dužina ključa je promjenljiva za oba algoritma (128, 192 ili 256 bita).

Do danas AES grupu simetričnih algoritama čine sljedeći algoritmi: Cast, Deal, Frog, E2, Magenta, Mars, Serpent, Twofish, Loki91, Loki97, RC6, Safer. Najpoznatiji asimetrični algoritmi su RSA, ElGamal, Diffie-Hellman, KEA (*Key Exchange Algorithm*), RPK (*Raike Public Key*), Rabin, Blum-Goldwasser, Menezes-Vanstone...

Primarna prednost asimetričnih algoritama je ta što se privatni ključ ne mora slati ni pokazivati bilo kome, što nije slučaj kod simetričnih algoritama gdje se tajni ključ mora poslati učesniku komunikacije, što za sobom povlači rizik otkrivanja podataka tokom njihovog slanja. Dalja prednost asimetričnih algoritama je mogućnost kreiranja digitalnog potpisa. Značajna mana asimetričnih algoritama je ta što su po svojoj prirodi sporiji, tj. implementacija na računaru se sporije odvija od implementacije simetričnih algoritama.

4. PAMETNE KARTICE

U današnje vrijeme kriptografija se koristi da zaštiti personalne podatke: u bankarstvu, zdravstvu, mobilnoj telefoniji, e-trgovini, itd. Raznovrsne operacije u ovim oblastima zasnivaju se na upotrebi kartice džepne veličine sa ugrađenim integrisanim kolom koja se popularno zove pametna kartica (*smart card*). Naziv govori malo o mogućnostima koje se danas mogu ostvariti pomoću pametnih kartica. Preteče današnjih kartica pojavile su se u Americi ranih pedesetih godina prošlog vijeka i predstavljale su simbol bogatstva, posjedovala ih je samo probrana elita. Sadržavale su jednostavne podatke koje je bilo teško krivotvoriti. Kartice s magnetnom trakom predstavljale su prvo značajnije poboljšanje, a pojavom elektronike i mikroelektronike omogućena je izrada uređaja na malom silicijumskom čipu, površine nekoliko kvadratnih milimetara, koji je moguće ugraditi na identifikacijsku karticu.

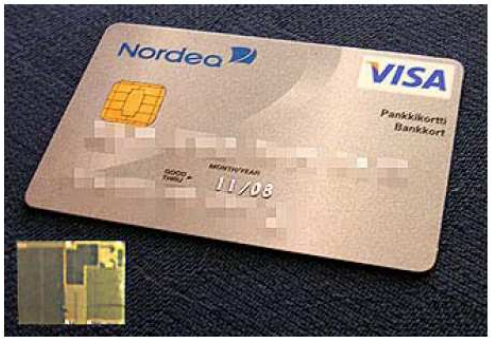
Slika 7. Primjena kriptografije

Prva takva ideja javila se 1968. godine u Njemačkoj (Jurgen Dethloff, Helmut Grotrupp), a 1970. godine u Japanu dr Kunitaka Arimura je predstavio prvi patent konceptualne zamisli pametne kartice. Ipak, začetnikom pametne kartice smatra se francuski novinar Roland Moreno koji je 1974. godine registrovao idejni patent kartice sa integrisanim sklopom (*IC Card*), koja je kasnije dobila naziv - pametna kartica. Zbog toga i ne čudi što je prva komercijalna primjena pametne kartice ostvarena u Francuskoj: francuski PTT 1984. godine izdaje prvu telefonsku karticu.

Pod pojmom pametne kartice uglavnom se misli na mikroprocesorske kartice zbog "inteligencije" koju pruža ugrađeni čip. Kao što i sam naziv govori, mikroprocesorske kartice sadrže MPU (*Microprocessor Unit*) jedinicu, poznatu i kao CPU (*Central Processing Unit*) jedinicu, koja značajno podiže nivo sigurnosti jer, omogućava ugradnju kriptografskih algoritama i primjenu širokog skupa zaštitnih mehanizama. Optičke i kartice s magnetnom trakom su memorijske kartice – mogu čuvati različite podatke, ali ih ne mogu obrađivati. Prema načinu prenosa podataka i mehanizmu pristupa, pametne kartice se dijele na kontaktne, beskontaktne, kombinovane i napredne kartice [16].

Od 1970. godine do danas vidljiv je stalan napredak u mikroprocesorskim mogućnostima i rastu broja različitih područja njihove primjene. Glavni uzroci širenja

njihove primjene su sve niža cijena, veća dostupnost i nedovoljna sigurnost kartica s magnetnom trakom.



Slika 8 – Izgled kontaktne mikroprocesorske pametne kartice

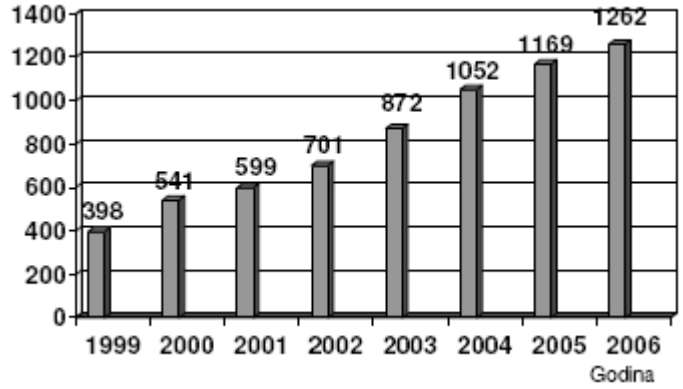
1977. godine troje komercijalnih proizvođača (Bull CP8, SGS Thomson, Schlumberger) počinje s razvojem pametnih kartica. 1986. godine Bank of Virginia i Maryland National Bank izdaju 14 000 kartica, a First National Palm Beach Bank i Mall Bank izdaju 50 000 Casio kartica svojim klijentima. Godinu dana kasnije je razvijena prva aplikacija pametne kartice Američkog ministarstva poljoprivrede za široko tržište – Peanut Marketing Card. U Holandiji je 1992. godine pokrenut nacionalni program elektronskog novčanika – Danmont.

Najveće finansijske organizacije Europay, Mastercard i Visa udružuju svoje napore u cilju primjene pametne kartice u finansijskoj industriji. Rezultat je EMV (*Europay Mastercard Visa*) specifikacija 1994. godine [17]. Preko milion i po VISACash bankovnih kartica je izdato za olimpijske igre u Atlanti 1996. godine. MasterCard i Visa sponzorišu rješavanje problema inter-operabilnosti pametnih kartica – razvijena su dva rješenja: Java Card (Visa) i Multi-application Operating System MULTOS (MasterCard).

Uloga pametnih kartica u novčanim transakcijama je očito neizbježna. Inter-operabilnost, standardizacija i razvoj su izazovi postavljeni današnjim pametnim karticama. Ti izazovi nijesu jednostavni - uz pomoć industrije javiće se inovativna rješenja koja spajaju nove tehnologije, poput interaktivne televizije, pametnih mobilnih telefona, ručnih digitalnih organizatora, elektronskih novčanika i interneta.

1995. godine je postojalo preko 3 miliona korisnika mobilnih telefona sa SIM karticama. Mobilna telefonija 1998. godine izdaje GSM (*Global System for Mobile communications*) specifikaciju koja otvara novo veliko područje primjene pametne kartice [18].

Dokumentovati noviju istoriju pametnih kartica (od 1999. godine do danas) nije jednostavno. Na tržištu svakim danom ima sve više rješenja za različite primjene pametne kartice. Prihvatanje i primjena tehnologije pametnih kartica razlikuje se od zemlje do zemlje i nacionalni sistemi još nijesu kompatibilni.



Slika 9. Broj prodatih pametnih kartica u svijetu izražen u milionima

Usljed zahtjeva na sve široj primjeni pametnih kartica javlja se potreba za bržim razvojem kartičnih aplikacija. Sigurnosni zahtjevi se neprestano mijenjaju, nema proizvođača pametnih kartica koji može reći da je njegov proizvod otporan na sve moguće (buduće) napade. Pristup sigurnosti pametnih kartica sve više se okreće standardizaciji. Prepoznavanje opasnosti, njihova specifikacija i protivmjere implementirane prema standardima, znatno će pojednostaviti korišćenje i razumijevanje s jedne strane, a otežati gubitak informacije s druge. Sigurnosna evaluacija rješenja treba početi u što ranijoj fazi izrade, i teći paralelno s razvojem u cilju pristupačnog i pouzdanog rješenja. Nezavisnost proizvođača mikromodula pametnih kartica i proizvođača kartičnih operacijskih sistema uzrokovaće niže cijene kartičnih sistema. Od pametnih kartica se u budućnosti očekuje raširena upotreba na svim područjima ljudskih djelatnosti, objedinjavanje više usluga na jednoj kartici i lakše poslovanje uz maksimalnu sigurnost.

5. ZAKLJUČAK

U radu je izložen razvoj kriptografije tokom širokog istorijskog razdoblja – od starih Egipćana do današnjih dana. Prikazane su metode kriptovanja koje su se vremenom usavršavale – od hijeroglifa do složenih kriptografskih algoritama. Dat je spisak najpoznatijih kriptografskih algoritama i njihova podjela prema upotrebi ključa. Razvoj tehnologije doveo je do stvaranja relativno sigurnog medija prenošenja informacija - pametne kartice. Data je lista najvećih proizvođača pametne kartice i sve njene aplikacije.

LITERATURA

[1] www.cypher.com.au/crypto_history
[2] Data Encryption Page: www.anujseth.com/crypto/
[3] Alan G. Konheim: "Cryptography: A Primer", John Wiley & Sons, 1981.
[4] www.apprendre-en-ligne.net/crypto/tritheme/

[5] "Cryptologia", Taylor & Francis, 2006.
[6] www.lewis-clark.org/content/cryp_wheel-Jefferson
[7] www.bryson.ltd.uk/cgi-bin/playfair
[8] en.wikipedia.org/wiki/Herbert_Osborne_Yardley
[9] Richard W. Hamming : "Coding and Information Theory", Prentice-Hall, 2000.
[10] John Savard's Home Page: www.quadibloc.com/
[11] J.L.Smith: "The Design of Lucifer, A Cryptographic Device for Data Communications", IBM Research Report, 1972
[12] W. Rankl, W. Effing: "Smart Card Handbook", John Wiley & Sons, 2003.
[13] Whitfield Diffie, Martin Hellman: "New Directions in Cryptography", IEEE International Symposium on Information Theory, Sweden, 1976
[14] www.rsa.com/rsalabs/
[15] J. Nechvatal, E. Barker, L. Bassham: "Report on the Development of the Advanced Encryption Standard", NIST October 2000.
[16] Bruce Schneier: "Applied Cryptography", John Willey & Sons, 1996.
[17] www.emvco.com
[18] The International Engineering Consortium: "Global System for Mobile Communications", web profum tutorials, 1998.