Gimnazija Vič

Tržaška cesta 72, Ljubljana

Šifriranje od Julija Cezarja do sodobne kriptografije

Jaka Čop, 1. b

Mentorja:

- Marina Trost, prof. informatike
- Jernej Čop, univ. dipl. matematik

Ljubljana: šolsko leto 2013/14

Povzetek

V nalogi bomo poskušali predstaviti zgodovino šifriranja od Julija Cezarja do danes. Če bomo izpustili kakšno dobro metodo šifriranja, ali ne bomo menili kakšnega pomembnega šifrerja/dešifrerja se opravičujem. Nalogo smo napisali, da bi bralcem predstavili zgodovino šifriranja in jim pomagali razumeti pomembnost današnjega šifriranja. Mislim, da bomo po pregledu projektno nalogo in bomo znali bolj ceniti pomembnost dobrega šifriranja, v prvi svetovni vojni je igralo ključno vlogo v zmagi zaveznikov, današnje dni pa je neprecenljivo.

Kazalo

1 Uvod **4**

2 Prva Šifriranja **5**
2.1 Cezarjanka 5
2.1.1 Monoalfabetska substitucija 6
2.2 Dekriptiranje šifriranega sporočila 8
2.3 Tajna pisava Marije Stuart 9

3 Mehanizirano šifriranje **12**
3.1 Dekriptiranje enigme 12

4 Moderno šifriranje **22**
4.1 Alice in Bob se predstavita 22
4.1.1 Matematika RSA 24

5 Zaključek **27**

Tabele

1 Cezarjev premik: premik za 3 mesta 5
2 Individualni ključi 17
3 Tabela povezanosti 1 17
4 Tabela povezanosti 2 17

Slike

1 Nomenklator Marije Stuart. Sestavljen je iz šifrirne abecede in kodnih besed. 10
2 Šifrirni stroj Enigma 15
3 Marian Rejewski 21
4 Asimetrično šifriranje 23
5 Alice in Bob 26

1 Uvod

„Že tisočletja se kralji, kraljice in generali zanašajo na hitre in zanesljive poti sporočanja, da bi lahko vodili svoje države in vojske. In že od nekdaj tudi vedo, kako hude so lahko posledice, če bi njihova sporočila prišla v napačne roke. Tedaj bi države tekmice ali nasprotnikova vojska izvedele za dobro varovane skrivnosti in odločilne informacije. Nevarnost, da bi nasprotnik lahko prestregel takšna pomembna sporočila, je bila spodbuda za razvoj raznih šifrirnih postopkov. Te tehnike prikrivanja naj bi zagotovile, da bo sporočilo znal prebrati samo pravi prejemnik.

Želja, da bi bi določena sporočila ostala tajna, je povzročila, da so države uvedle svoje tajne službe, ki naj bi razvile najboljše mogoče šifre in bile odgovorne za varno prenašanje sporočil. Hkrati s tem pa so nasprotnikovi dekripterji poskušali ukrasti te šifre in z njimi tudi razne skrivnosti. Dekripterji so jezikovni alkimisti, z miti obdano pleme, ki poskuša iz vrste simbolov brez pomena pričarati smiselne besede. Zgodovina tajnih pisav, kodov in šifer je zgodovina stoletja starega boja med šifrerji in dekripterji, duhovne oboroževalne tekme, ki dramatično vpliva na potek zgodovine.

Nenehni boj med šifrerji in dekripterji je spodbudil vrsto znanstvenih prebojev. Eni nenehno iščejo nove šifrirne postopke, drugi pa razvijajo vse močnejše metode za napad nanje. Obe strani, ena, ki išče vedno nove šifrirne postopke, in druga, ki jih poskuša čim prej streti, uporabljata celo vrsto znanstvenih disciplin in postopkov, od matematike do jezikoslovja in od iformatike do kvantne teorije. Šifrerji in dekripterji po svoje bogatijo ta strokovna področja, njihovo delo pa pospešuje tehnični razvoj, zlasti računalništva. Šifre so vpletene v zgodovino, odločale so o bitkah in povzročale smrt kronanih glav ...“

2 Prva Šifriranja

2.1 Cezarjanka

Cezarjeva šifra ali cezarjanka je ena najbolj znanih in najbolj preprostih šifer ter najstarejših starorimskih šifer. Če stte mislili, da je šifro razvil Julij Cezar se motite! Razvil jo je Cicerov osvobojeni suženj Tiron. Ker jo je veliko uporabljal za šifriranje svojih sporočil se šifra imenuje po njemu.

Gre za monoalfabetsko substitucijsko šifro, saj za vsako črko odprtega besedila šifrirni ključ določi drugo črko. V primeru cezarjeve šifre šifrirni ključ določa za koliko mest se premakne šifrirana abeceda glede na odprto. Pošiljatelj in prejemnik sporočila morata uporabiti isto število zamenjave.

Primer: šifrirni ključ(premik za 3 mesta)

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

Tabela 1: Cezarjev premik: premik za 3 mesta

Pa šifrirajmo besedo PONEDELJEK, s šifrirnim ključem 3.
P $\Rightarrow$ T, O $\Rightarrow$ S, N $\Rightarrow$ R, ...

Dobimo besedo: TSRHGHOMHN

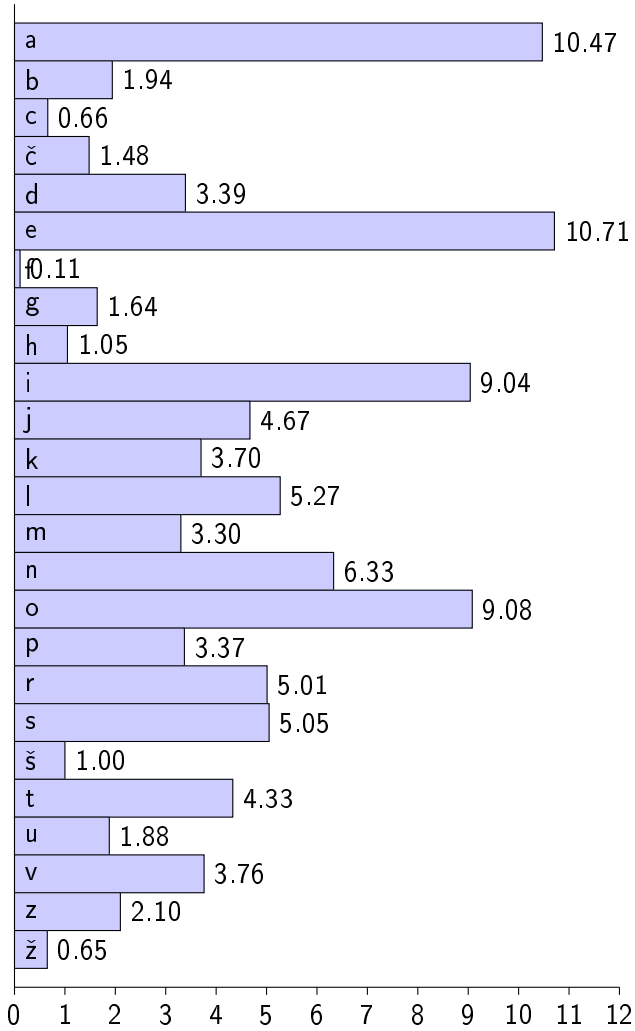
Na prvi pogled se zdi beseda nerazpoznavna, a je tako šifro lahko razvozlati saj moraš ugotoviti samo številko zamika abecede, tukaj pa je samo 22 različnih možnosti(uporabljena je abeceda brez šumnikov), za kar ti ne bi smelo vzeti preveč časa. Boljšo varnost bi lahko ustvarili s tem, da bi šifrirani abecedi naključno razporedili črke, o tem pa v naslednjem poglavju.

2.1.1 Monoalfabetska substitucija

Nadrejeni pojem za substitucijo, pri kateri šifrirana abeceda sestoji iz črk, drugih simbolov in/ali številk, je monoalfabetska šifra. Vse šifre s substitucijo, ki smo jih do zdaj spoznali v tej nalogi, spadajo v to vrsto monoalfabetskega šifriranja.

Možnost, da dekriptiramo šifrirano sporočilo, ob predpostavki, da poznamo jezik, v katerem je besedilo napisano, je v tem, da poiščemo drugo sporočilo v istem jeziku, ki je dovolj dolgo, da z njim popišemo en ali dva lista papirja in potem preštejemo, kako pogosto se v njem pojavljajo posamezne črke. Najpogostejši črki rečemo prva, drugi najpogostejši druga itn., dokler nismo prešteli vseh črk v odprtem besedilu.

Potem si natanko ogledamo skrivno besedilo, ki ga želimo dekriptirati, in razvrstimo po številu tudi njegove simbole. Najdemo najpogostejši simbol in mu dodelimo vrednost prve črke iz preizkusnega odprtega besedila, drugi najpogostejši simbol bo postal druga črka, tretji najpogostejši tretja črka in tako naprej, dokler nismo tako obdelali vseh simbolov kriptograma, ki ga želimo odpreti.



Frekvenčna analiza črk v slovenski abecedi.

2.2 Dekriptiranje šifriranega sporočila

PCQ VMJYPD LBYK LYSO KBXBJXWXV BXV ZCJPO EYPD KBXBJYUXJ LBJOO KCPK. CP LBO LBCMKXPV XPV IYJKL PYDBL, QBOP KBO BXV OPVOV LBO LXRO CI SX'XJMI, KBO JCKO XPV EYKKOV LBO DJCMPV ZOICJO BYS, KXUYPD: „DJOXL EYPD, ICJ X LBCMKXPV XPV CPO PYDBLK Y BXNO ZOOP JOACMPLYPD LC UCM LBO IXZROK CI FXKL XDOK XPV LBO RODOPVK CI XPAYOPL EYPDK. SXU Y SXEO KC ZCRV XK LC AJXNO X IXNCMJ CI UCMJ SXGOKLU?“

OFYRCDMO, LXROK IJCS LBO LBCMKXPV XPV CPO PYDBLK.

Zamislimo si, da smo to šifrirano besedilo prestregli in da ga moramo dekriptirati. Vemo, da gre za angleško besedilo. ki je šifrirano s pomočjo monoalfabetske substitucije, toda o ključu ne vemo ničesar. Vseh mogočih ključev skorajda ni mogoče preizkusiti, zato moramo pač uporabiti frekvenčno analizo, ki smo jo pojasnili v prejšnjem poglavju. V nadaljevanju bomo postopoma posredovali navodilo za dekriptiranje tega šifriranega besedila, toda kdor si upa, lahko to opravi tudi na lastno pest.

Prva reakcija kriptoanalitika, ki bi dobil v roke takšno šifrirano besedilo, bi seveda bila, ugotoviti frekvenco vsake posamezne črke. S tem bi dobil tabelo 1. Kot smo pričakovali, se posamezne črke pojavljajo različno pogosto.

2.3 Tajna pisava Marije Stuart

Zjutraj 15. oktobra 1586 je stopila škotska kraljica Marija Stuart v prenapolnjeneo sodno dvorano na gradu Fotheringhay. Dolgoletni zapor in začetek revmatičnega obolenja sta jo močno prizadela, vendar ni izgubila svojega dostojanstva, svoje obvladljivosti in očitno gosposkega nastopa. Naslonjena na svojega zdravnika je odšla mimo sodnikov, visokih uradnikov in gledalcev do prestola sredi dolge, ozke dvorane. Prestol je imel za znak spoštovanja, vendar se je motila. Prazen prestol je simboliziral kraljico Elizabeto, Marijino nasprotnico in tožnico. Z blagim nasiljem so odpeljali Marijo naprej na drugo stran na drugo stran dvorane, do škrlatno rdečega žametnega stola, ki je bil namenjen za obtožene.

Marijo Stuart, škotsko kraljico, so obtožili izdajstva. Obdolžili so jo, da je sodelovala pri načrtovanju umora kraljice Elizabete I. znamenom, da se sama polasti angleške krone. Sir Francis Walsingham, minister, ki je bil pristojen za Elizabetino varnost, je dal druge zarotnike že zapreti, od njih izsilil priznanja in jih dal usmrtiti. Zdaj je hotel dokazati, da je bila Marija srce zarote; s tem je bila enako kriva in si je zaslužila smrt.

Walsingham je natanko vedel, da mora kraljico Elizabeto prepričati o Marijini krivdi, če jo hoče dati usmrtiti. Elizabeta je sicer prezirala Marijo, vendar je imela dobre razloge za to, da se ni odločila za smrtno kazen. Marija je bila škotska kraljica in mnogi so dvomili, da je angleško sodišče pristojno za to, da bi voditeljico tuje države obsodilo na smrt. Usmrtitev Marije pa bi bila tudi mučen vzorčni primer – če je bilo državi dovoljeno, da bi usmrti to kraljico, bodo imeli uporniki manj pomislekov, da bi ubili drugo monarhinjo, namreč kraljico Elizabeto samo. Poleg tega pa sta bili Elizabeta in Marija sestrični; to krvno sorodstvo pa je pripomoglo, da se Elizabeta ni odločila za to skrajno potezo. SKratka, Elizabeta bi dopustila usmrtitev Marije samo v primeru, če bi Walsingham lahko brez kančka dvoma dokazal, da je bila vpletena v morilsko zaroto.

Zarotniki so bili skupina mladih katoliških plemičev, ki so hoteli Elizabeto, protestantko, odstraniti in namesto nje na prestol posaditi katoličanko Marijo. Za sodišče ni bilo nobenega dvoma, da je bila Marija za zarotnike svetel lik, toda ali je v resnici odobrila to dejanje, še ni bilo dokazano. Marija pa je v resnici blagoslovila to zaroto. Walsingham je bil zdaj pred nalogo, da dokaže otipljivo povezavo med Marijo in zarotniki.

Marija, oblečena v črno svilo, je sedela sama pred sodniki. V primeru izdajstva obtoženi niso smeli imeti zagovornika niti niso smeli navesti nobene priče. Za pripravo obrambe Mariji niso dovolili niti pomoči tajnika. Vsekakor pa je vedela, da njen položaj ni povsem brezupen, saj si je iz previdnosti z zarotniki dopisovala samo v skrivni pisavi. Ta je spreminjala besede v verige simbolov, ki niso imeli nobenega pomena. Walsingham je morda zaplenil pisma, vendar je bila Marija trdno prepričana, da tistih simbolov nikoli ne bo mogel razvozlati.

Če pa bo njihov pomen ostal skrit, pisem nikoli ne bodo mogli uporabiti kot dokaz proti njej. Vsekakor je vse to temeljilo na domnevi, da tajne pisave niso mogli prebrati. Na Marijino nesrečo pa Walsingham ni bil samo Elizabetin prvi minister, temveč tudi vodja tajnih agentov v Angliji. Prestregel je Marijina pisma zarotnikov in pri tem natanko vedel, kdo ima potrebno znanje, da bi jih lahko razvozlal. Thomas Phelippes je bil največji strokovnjak za dekriptiranje šifriranih besedil v državi; že več let je dekriptiral sporočila zarotnikov in zbiral dokaze za njihovo obsodbo. Če bi lahko dekriptiral tudi obremenjujoča pisma med Marijo in zarotniki, potem bi bila zapisana smrt. Če pa je bila Marijina tajna pisava dovolj močna, da bo lahko ohranila njene skrivnosti, bi morda ostala pri življenju. Ni bilo prvič, da je trdnost kakšne tajne pisave odločala o življenju ali smrti.

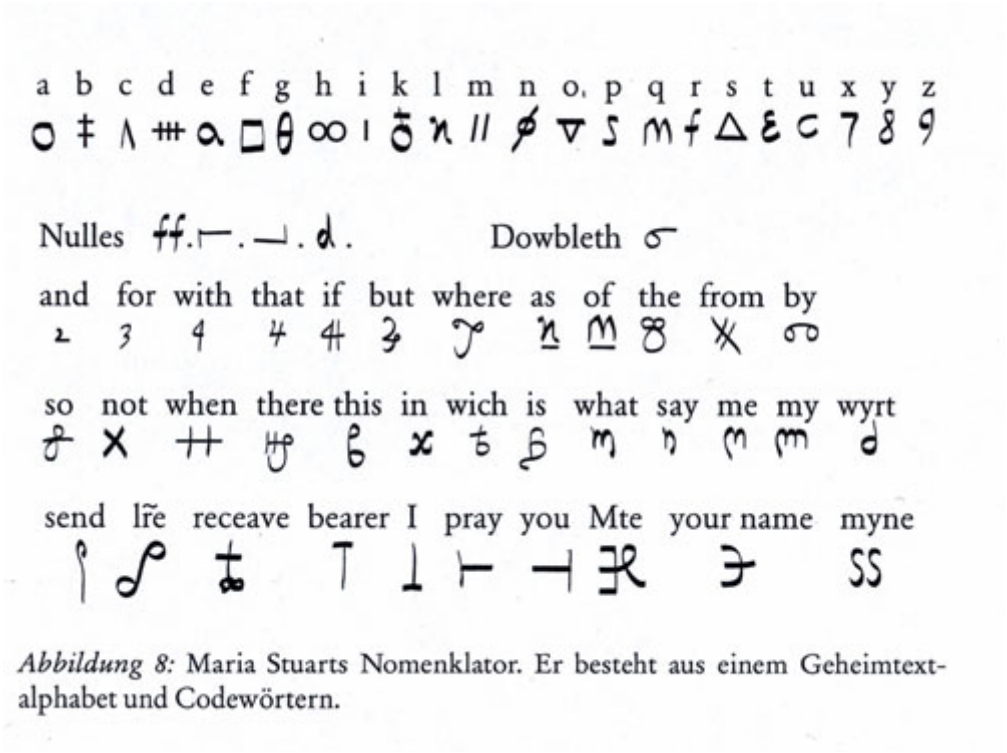


Abbildung 8: Maria Stuarts Nomenklator. Er besteht aus einem Geheimtextalphabet und Codewörtern.

Slika 1: Nomenklator Marije Stuart. Sestavljen je iz šifrirne abecede in kodnih besed.

Marija in Babington (mož s katerim je kovala zaroto) sta se zaneslana to, da bo njuna šifra skrila njune načrte, vendar st živela v času, ko je napredek na področju kriptoanalize oslabil kriptografijo. Njuna šifra bi ju zagotovo varovala pred vsiljivimi pogledi kakšnega laika, proti strokovnjaku za frekvenčno analizo pa ni imela možnosti. Na klopeh za gledalce je sedel Phelippes in brez besed opazoval, kako so predložili dokaze, ki jih je izbral

iz dekriptiranih pisem.

8. februarja 1587 se je v veliki dvorani gradu Fotheringhay zbrala tristoglava množica, da bi bila navzoča pri obglavljanju Marije Stuart. Walsingham se je odločil, da bo vlogo Marije kot mučenice kar najbolj zmanjšal, zato je vse kar je bilo povezano z usmrtitvijo, ukazal sežgati, da nobena relikvija ne bi prišla v javnost. Vsekakor pa je tudi Marija mislila na to, da bo iz svojega zadnjega nastopa naredila potezo odpora, še enkrat podkrepila katoliško vero in spodbudila svoje privržence.

3 Mehanizirano šifriranje

3.1 Dekriptiranje enigme

Tudi po prvi svetovni vojni so angleški kriptoanalitiki v Room 40 nadzorovali nemške radijske zveze. Toda od leta 1926 naprej so slišali samo radijska poročila, s katerimi si niso znali pomagati. Enigma se je uveljavila in čim več teh naprav so uporabljali Nemci, tem manj uspehov so dosegli ljuuje v Room 40. Tudi Američani in Francozi so poskušali streti sporočila, šifrirana z enigmo, vendar prav tako brez uspeha. Nemčija je tedaj imela najvarnejši vojaški telekomunikacijski sistem na svetu. Kriptoanalitiki zahodnih sil, ki so bili med prvo svetovno vojno še krepko pri stvari, so hitro odnehali. Še deset let pred tem so se zaradi grozečega poraza noč in dan ukvarjali z nemškimi šiframi. Očitno sta strah in sovraštvo ključni gonilni sili in zelo ugodno delovno okolje za uspešne dekripterje.

Ena država pa si ni mogla privoščiti lenarjenja. Po prvi svetovni vojni je Poljska spet postala samostojna država, toda poljaki so kmalu spoznali, da je njihova na novo pridobljena neodvisnost spet ogrožena. Na vzhodu je ležala Sovjetska zveza, ki si je prizadevala širiti svoj komunizem, na zahodu pa je bila Nemčija, ki je želela spet pridobiti ozemlja, ki jih je bila po vojni prisiljena odstopiti Poljski. Tako ukleščena Poljska je bila hvaležna za vsako informacijo o obeh nasprotnikih, zato je na novo organizirala dekriptersko službo, tako imenovani Biuro Szyfrov. Če je nujnost mati izumov, potem je sovraštvo mati kriptoanalize. Udarna moč Biuroja Szyfrov se je razločno pokazala z uspehom v poljsko-sovjetski vojni leta 1919 in 1920. Samo v avgustu leta 1920, ko so sovjetske armade že stale pred vrati Varšave, dekriptirali več kot 400 sovražnikovih sporočil. Nadzorovanje nemškega radijskega prometa je bilo prav tako uspešno, dokler niso leta 1926 nemci začeli uporabljati enigmo za šifriranje njihovih sporočil.

Za dekriptiranje nemški radijskih zvez je bil odgovoren stotnik Maksymilian Ciezki, vnet patriot, ki je odrasel v mestu Szamotuty, središču poljskega nacionalizma. Vendar Ciezki ni imel na voljo nobene verzije enigme, brez poznavanja žičnih povezavv tej vojaški napravi pa ni imel možnosti za dekriptiranje sporočil nemške vojske. Zaradi tega se je znašel v takšni stiski, da je nekoč v nemočnem besu celo najel jasnovidca, ki naj bi iz prestreženih radijskih pogovorov pričaral kakšen smisel. Ni treba posebej poudarjati,da se tudi jasnovidcu ni posrečil tisti preboj, ki bi ga potrebovali. Tako je ostal prihranjen za Nemca Hansa-Thilo Schmidta, ki je bil razočaran nad svojo domovino in je pripravil pot za napad na enigmo.

Hans-Thilo Schmidt se je rodil leta 1888 v Berlinu kot drugi sin uglednega profesorja in njegove plemiške žene. Schmidt se je odločil za kariero v vojski in ji služil med 1. svetovno vojno, toda pri drastičnih redukcijah zaradi versajske pogodbe ga je vojska uvrstil med tiste, ki so bili odveč. Nato je

poskusil srečo kot poslovnež, vendar je moral tovarno mila med hudo inflacijo zapretiin je ostal z družine brez vseh sredstev.

Uspeh njegovega starejšega brata Rudolpha je samo še povečal njegov obup. Tudi Rudolph je bil med vojno zaposlen v vojski, vendar je v njej delal še naprej. V dvajsetih letih je naredil hitro kariero in je nazadnje napredoval do štabnega poveljnika vojaških komunikacij. Rudolph je bil tisti, ki je odobril uporabo enigme v vojski.

Po propadu svojega podjetja je bil Hans-Thilo prisiljen prositi brata za pomoč, in Rudolph mu je priskrbel delo v berlinskem šifrirnem centru, v službi, ki je bila odgovorna za šifrirano komunikacijo v vojski. Ta šifrirni center je bil tajna komandna centrala za enigmo, v kateri so se izmenjavale strogo zaupne informacije. Ko je Schmidt nastopil novo delo, je pustil svojo družino na Bavarskem, kjer so bili življenjski stroški nižji. Živel je sam v dragem Berlinu, obubožan in brez prijateljev, zavidal je svojemu bratu in bil poln zamer proti državi, ki ni potrebovala njegovega dela. Posledice so bile neizogibne. Schmidt je nekaj denarja zaslužil s tem, da je tajne informacije o enigmi prodajal tujim oboroženim silam, s čimer se je hkrati maščeval, spodokopaval varnost države in škodil uradu svojega brata.

8.11.1931 se je Schmidt nastanil v hotelu Grand v belgijskem mestu Verviers. Bil je dogovorjen s francoskim agentom, ki je delal pod imenom Rex. Za vrednost 10.000 mark (po današnji vrednosti približno 20.000 dolarjev) je Schmidt dovolil agentu, da je fotografiral dva dokumenta: Nvodila za uporabo šifrirnega stroja Enigma in Navodila za uporabo ključev šifrirnega stroja Enigma. Ti dokumenti sicer niso vsebovali natančnega opisa žičnih povezav v valjih, a so vsebovali dovolj potrebnih podatkov za njihovo razvozlanje.

Zaradi Schmidtove izdaje so zavezniki lahko izdelali natančen duplikat nemške enigme. Vsekakor pa to ni zadostovalo za dekriptiranje z enigmo šifriranih sporočil. Trdnost šifre ni odvisna od tega ali stroj ostane v tajnosti, temveč od varovanja tajnosti o njegovi vsakokratni nastavitvi (tj. od ključa). Če hoče kriptoanalitik dekriptirati prestreženo sporočilo, mora ne samo imeti duplikat enigme, temveč mora tudi ugotoviti, kateri od več milijard ključev je bil uporabljen za šifriranje posameznega sporočila.

Francoska tajna služba je očitno opravila svojo domačo nalogo, saj je pridobila obveščevalca in dobila dokumente, ki so vsebovaliinformacije o žičnih povezavah v enigmi. Francoski kriptoanalitiki pa očitno niso imeli ne volje, ne sposobnosti, da bi znali pravilno oceniti te najnovejše podatke. Po uspehu v prvi svetovni vojni so trpeli zaradi samoprecenjevanja in pomanjkanja motivacije. Bureau du Chiffre je menil, da ni potrebno niti to, da bi izdelal duplikat vojaške enigme, saj je bil prepričan, da je naslednja ovira, namreč najti ključ za določeno z enigmo šifrirano sporočilo, nepremagljiva.

Naneslo je tako, da so Francozi pred desetimi leti podpisali s Poljsko vojaški sporazum. Poljaki so pokazali zanimanje za vse, kar je bilo povezano

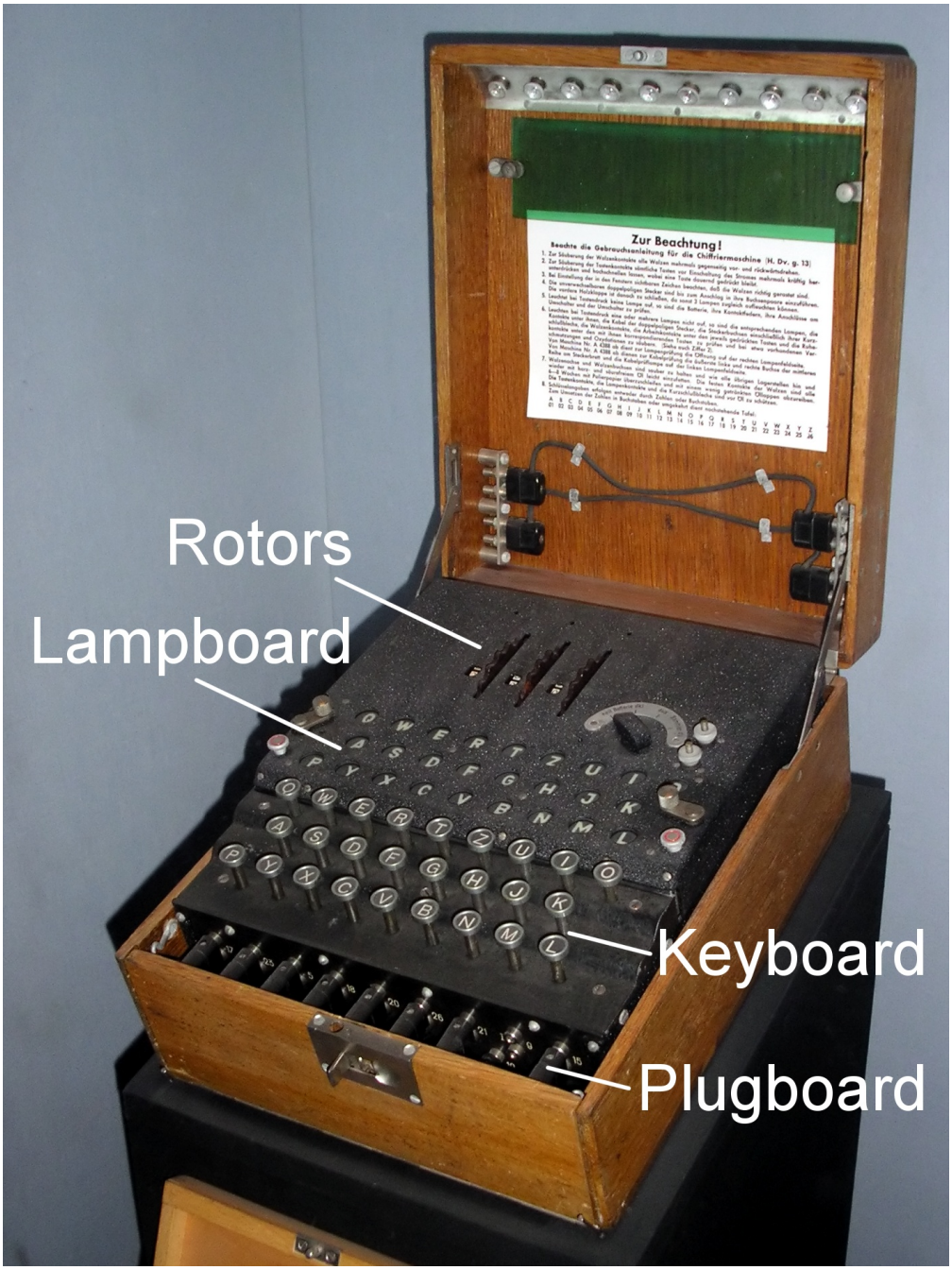
z enigmo, zato so Francozi izročili svojim zaveznikom fotografije Schmidtovih dokumentov in ljudem v Biuro Szyfrow prepustili brezupno nalogo, da bi strli enigmo. Dokumenti so bili zgolj začetna pomoč, to so vedeli tudi Poljaki, v nasprotju s Francozi pa so se bali invazije in so zaradi tega imeli dovolj razlogov, da ne opustijo nobene priložnosti. Poljaki so se zagrizli v misel, da mora obstajati kakšna bljižnica, po kateri bi našli ključ za sporočilo šifrirano z enigmo. Treba je samo dovolj truda, iznajdljivosti in bistroumnosti pri iskanju te poti.

Scmidtovi dokumenti niso razkrili samo notranje povezave v valjih, natanko so bili opisani tudi ključi, ki so jih uporabljali Nemci. Operaterji enigem so vsak mesec dobili novo knjigo ključev, ki je za vsak dan predpisovala določen ključ. Za prvi dan v nekem mesecu je knjiga ključev naprimer določala naslednji dnevni ključ:

1. Povezave na stikalni ploščici: A/L–P/R–T/D–B/W–K/F–O/Y
2. Položaj valjev: 2-3-1
3. Osnovna nastavitev valjev: Q-C-W

Položaj valjev in osnovna nastavitev valjev se imenuje konfiguracija valjev. Za ta določen dnevni ključ je moral šifrer svoj šifrirni stroj Enigma nastaviti takole:

1. Povezave na stikalni plošči: Črki A in L povezati s kablom na stikalni ploščici in ju s tem zamenjati; enako narediti s pari črk P in R, T in D, B in W, K in F, ter nazadnje še O in Y.
2. Položaj valjev: Valj 2 vstavi v prvo odprtino za valje, valj 3 v drugo odprtino in valj 1 v tretjo odprtino.
3. Osnovna nastavitev valjev: Na zunanjem obroču vsakega valja je vgravirana abeceda, s pomočjo katere ga lahko postavimo v določen položaj. V zgornjem primeru bi šifrer tako dolgo vrtel valj v prvi odprtini, da bi bil zgoraj Q, valj v drugi odprtini tako dolgo, da bi bil zgoraj C, in valj v tretji odprtini tako dolgo, da bi bil zgoraj W.



Slika 2: Šifrirni stroj Enigma

Ena od možnosti je bila, da bi celoten radijski promet enega dneva šifrirali z dnevnim ključem. Tedaj so šifrerji z enigmo en cel dan na začetku vsakega sporočila nastavili vsakokratni dnevni ključ. Vsako radijsko sporočilo so najprej odtipkali v šifrirni stroj; šifrirano besediloso si zapisali in ga izročili

radiotelegrafistu, da ga je poslal naprej. Na strani prejemnika pa je sporočilo najprej dobil radiotelegrafist in ga izročil človeku, ki je delal z enigmo. Ta ga je spet odtipkal v svoj stzroj, na katerem je že prej nastavil dnevni ključ. Črke, ki so se po vrsti prikazovale na ploščici z lučkami, so setavljale odprto besedilo.

Ta postopek je bil dovolj varen, njegova slabost pa je bila v tem, da se dnevni ključ uporablja vedno znova, morda za pošiljanje kar nekaj sto sporočil, ki se naberejo vsak dan. Če se za šifriranje ogromnega števila sporočila uporablja en sam ključ, je za kriptoanalitika navadno lažje kako ga razvozlati. Velika količina besedil, ki so enako šifrirana, dajejo kriptoanalitiku večjo možnost, da odkrije ključ. Že pri preprostejših postopkih smo videli,da je preprosteje dekriptirati mono alfabetsko šifro, če je na voljo več strani šifriranega besedila in ne samo nekaj stavkov.

Na prvi pogled se zdi tak sistem neprebojen, vendar poljski kriptoanalitiki niso izgubili poguma. Bili so pripravljeni izkoristiti vsako možnost samo, da bi našli kakšno šibko točko v enigmi ter v sistemu individualnih ključev. Biuro Szyfrow je organiziral tečaj iz kriptografije ter nanj povabil 20 matematikov. Trije od teh so pokazali večji talent od ostalih in Biuro jih je zaposlil. Najbolj nadarjen med njimi je bil Marjan Rejewski. Med šolanjem je strl celo vrsto šifer, nazadnje pa so mu predstavili domnevno neprebojno enigmo. Rejewski je delal popolnoma sam in je vse svoje moči osredotočil na to, da bi Scherbiusovo napravo spoznal do najmanjše podrobnosti. S pogledom matematika si je posebno natanko ogledal njen način delovanja ter proučeval učinkovanje valjev in stikalne plošče. To delo je zahtevalo ne le logično razmišljanje, temveč tudi navdih.

Strategija, ki jo je izbral Rejewski, je temeljila predvsem na dejstvu, da je ponavljanje sovražnik varovanja tajnosti. Ponavljanja izdajajo določene vzorce, ti pa so ljubljenčki kriptoanalitikov. Najbolj očitna ponavljanja pri sporočilih, šifriranih z enigmo so bili individualni ključi, ki so bili na začetku vsakega sporočila. Če je šifrer na primer izbral individualni ključ ULJ, potem ga je šifriral dvakrat in iz ULJULJ morda dobil PEFNWZ, zaporedje črk, ki je bilo potem poslano na začetku vsakega sporočila. Nemci so to ponavljanjepredpisali zato, da bi preprečili napake zaradi interference, ali zaradi napačnega vnašanja podatkov. Da bodo s tem ogrozili varnost šifriranja niso pomislili.

Rejewski je dobil vsak dan na pisalno mizo kup prestreženih sporočil, vsa so se začenjala s šestimi črkami individualnega ključa iz treh črk, ki so bili vsi šifrirani po dogovorjenem dnevnem ključu. Tako je naprimer dobil štiri radijska sporočila, ki so se začenjala z naslednjimi individualnimi ključi:

1. sporočilo	L	O	K	R	G	M
2. sporočilo	M	V	T	X	Z	E
3. sporočilo	J	K	T	M	P	E
4. sporočilo	D	V	Y	P	Z	X

Tabela 2: Individualni ključi

Prva črka	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
Druga Črka										P				M				R	X							

Tabela 3: Tabela povezanosti 1

Prve in četrte črke so zagotovo šifrirane iste črke sporočila, namreč prve iz individualnega ključa, tako tudi druge in pete, ter tretje in šeste. V prvem radijskem sporočilu sta torej L in R isti črki. Vzrok zakaj je ta črka različno šifrirana, najprej kot L in potem kot R, je preprosto to, da se je prvi valj med eno in drugo črko premaknil za tri korake in s tem spremenil pot šifriranja.

Dejstavo, da sta L in R šifri za isto črko, je dalo Rejewskemu namig o prvotni nastavitvi enigme. S to osnovno nastavitvijo, ki je ni poznal, je šifriral prvo črko dnevnega ključa, ki je prav tako ni poznal, v L, poznejši položaj valjev, prav tako nepoznan, vendar tri korake oddaljen od osnovne nastavitve, pa je šifriral isto črko v R.

Ta ugotovitev se morda zdi še nejasna, ker je še preveč neznank, ki so pri tem pomembne, kaže pa vsaj to, da sta črki L in R, pogojno s temeljno nastavitvijo enigme, namreč z dnevnim ključem, nujno povezani. Z vsakim novim prestreženim sporočilom je odkrival nove povezave med prvo in četrto črko ponovlenega individualnega ključa. V vseh teh odnosih se zrcali osnovna nastavitev enigme. Drugo radijsko sporočilo na zgornjem seznamu, nam pove, da sta M in X med seboj povezana, tretje pa povezuje J in M, četrto pa D in P. Rejewski je vse te odnose strnil v posebni tabeli. Za dosedanja štiri radijska sporočila kaže tabela povezanost med (L, R), (M, X), (J, M), (D, P):

Če je prisluškovalna služba dala Rejewskemu v enem dnevu dovolj sporočil je lahko izpolnil abecedo teh povezav:

Rejewski ni poznal dnevnega ključa in tudi ni vedel, kateri individualni ključi so bili izbrani, vendar je vedel, da rezultirajo v tej tabeli odnosov. Če bi bil dnevni ključ drugačen, bi bila tudi ta tabela popolnoma drugačna. Naslednje vprašanje je bilo, ali je mogoče s pomočjo te tabele odkriti dnevni

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

Tabela 4: Tabela povezanosti 2

ključ. Rejewski je začel iskati vzorce v tabeli, strukture, ki bi morda kazale na dnevni ključ. Nazadnje je začel raziskovati določen vzorec, ki ga je dobil iz črkovnih verig. V zgornji tabeli , na primer, je A v zgornji vrstici povezan s F v spodnji. Rejwski je poiskal zdaj F v zgornji vrstici, ugotovil je da je povezan z W, zato je poiskal W v zgornji vrstici. In ta W je bil končno spet povezan z A, s katerim je začel. Veriga je bila zaključena.

Rejewski je enako storil še z drugimi črkami abecede in sestavil različne verige. Napisal jih je skupaj in za vsasko zapisal število povezav v vsaki verigi:
A ⇒ F ⇒ W ⇒ A 3 povezave
B ⇒ Q ⇒ Z ⇒ K ⇒ V ⇒ E ⇒ L ⇒ R ⇒ I ⇒ B 9 povezav
C ⇒ H ⇒ G ⇒ O ⇒ Y ⇒ D ⇒ P ⇒ C 7 povezav
J ⇒ M ⇒ X ⇒ S ⇒ T ⇒ N ⇒ U ⇒ J 7 povezav

Ugotovil je, da se verige vsak dan spreminjajo. Včasih je dobil veliko kratkih verig, drugič malo dolgih. Seveda so se spreminjale tudi črke v verigah. Lastnosti verig so bile očitno posledica vsakokratnega dnevnega ključa - kar je po zapleteni poti dosežen učinek kabelskih povezav na plošči s stikali, položaja valjev in nastavitve valjev. Vsekakor je še vedno obstajalo vprašanje, kako bi Rejewski iz teh verig dobil dnevni ključ. Kateri od 10 000 000 000 000 000 možnih dnevnih ključev tiči za posameznim vzorcem verig? Število možnosti je bilo kratko malo preveliko.

Na tej točki je Rejewski sprejel pomembno ugotovitev. Plošča s stikali in konfiguracija valjev skupaj sicer vplivata na natančno sestavo verig, toda vpliv in druge je mogoče v določeni meri razdvojiti. Posebno ena lastnost verig je odvisna izključno od položaja in nastavitve valjev in nima nobene povezave z povezavami na stikalni plošči: namreč število povezav znotraj verig. Vzemimo zgornji primer in naredimo tako, kot je zahteval dnevni ključ, namreč s pomočjo povezave na stikalni plošči zamenjamo črki S in G. Če spremenimo ta sestavni del dnevnega ključa, in sicer tako, da odstranimo kabel, ki zamenjuje S in G, in namesto tega zamenjamo T in K, se verige spremenijo takole:
A ⇒ F ⇒ W ⇒ A 3 povezave
B ⇒ Q ⇒ Z ⇒ T ⇒ V ⇒ E ⇒ L ⇒ R ⇒ I ⇒ B 9 povezav
C ⇒ H ⇒ S ⇒ O ⇒ Y ⇒ D ⇒ P ⇒ C 7 povezav
J ⇒ M ⇒ X ⇒ G ⇒ K ⇒ N ⇒ U ⇒ J 7 povezav

Nekaj črk v verigah se spremeni, število povezav v vsaki verigi pa ostane enako. Rejewski je odkril lastnosti verig, v katerih se odraža samo konfiguracija valjev. Celotno število konfiguracij valjev je število možnih položajev valjev (6), pomnoženo s številom nastavitev valjev (17.576), torej 105.456. Zdaj se Rejewskemu ni bilo treba več ibadati z vprašanjem kateri od 10 000 000 000 000 000 dnevnih ključev je dal določeno skupino verig. Lahko se

je ukvarjal z drastično preprostejšim problemom: katera od 104.456 možnih konfiguracij tiči za številom povezav znotraj določene skupine verig? To število je še vedno veliko, vsekakor pa stomilijardkrat manjše od skupnega števila ključev.

Rejewski je ravnal takole. Vohunu Hansu-Thilo Schmidtu se je moral zahvaliti, da je lahko delal z identičnim, na novo izdelanim šifrirnim strojem enigma. Njegovi ljudje so se vrgli na delo in začeli preverjati vsako od 104.456 možnih konfiguracij valjev in si zapisovali vsakokrat nastalo dolžino verig. Potrebovali so celo leto, da so sestavili katalog, toda takoj ko je Biuro zbral vse podatke, je Rejewski končno začel z dekriptirati z enigmo izdelane šifrate.

Vsak dan si je ogledal šifrirane individualne ključe, prvih šest črk vseh prestreženih sporočil, in sestavil svoje tabele. Ko jih je imel pri roki, je lahko črke povezal v verige in za vsako verigo določil število povezav. Tako je na primer z analizo prvih in četrtih črk dobil štiri verige z 3, 9,7 in 7 povezavami. Druga in peta črka sta dali verige štiri verige z 2, 3, 9 in 12 povezavami. Tretje in šeste črke pa so dale pet verig s 5, 5, 5, 3 in 8 povezavami. Dnevnega ključa Rejewski sicer še vedno ni vedel, vendar je vedel, da je ta dnevni ključ oblikoval tri skupine verig z naslednjimi značilnostmi:

4 verige iz prvih in četrtih črk, s 3, 9, 7 in 7 povezavami 4 verige iz drugih in petih črk, s 2, 3, 9 in 12 povezavami 5 verig iz tretjih in šestih črk, s 5, 5, 5, 3 in 8 povezavami

Zdaj si je Rejewski lahko pomagal s svojim katalogom, saj so bile v njem vse konfiguracije valjev, urejene po vsakokrat nastalih verigah. Takoj, ko je našel vnos v katalog s pravilnim številom verig in pravilnim številom povezav, je poznal konfiguracijo valjev, ki jo je predvideval vsakokratni dnevni ključ. Verige so bile hkrati nekakšni prstni odtisi, ki so pripeljali na sled konfiguracije valjev. Rejewski je delal kot nekakšen detektiv, ki na prizorišču zločina najdeprstni odtis in ga potem s pomočjo banke podatkov poveže s kakšnim osumljencem.

Rejewski je zdaj sicer našel valjčni del dnevnega ključa, povezav na stikalni plošči pa še vedno ni poznal. Čeprav obstaja skoraj sto milijard možnosti za te povezave, je bila naloga sorazmerno preprosta. Rejewski je najprej nastavil valje na svoji enigmi skladno s pravkar odkritim delom dnevnega ključa za valje. Potem je odstranil vse kable na stikalni plošči, ki tako ni več vplivala na šifriranje. Nazadnje je vzel prestrežen šifrat in ga vnesel v enigmo. Dobil je večinoma nesmisel saj je manjkala kabelska povezava na stikalni plošči in tudi ta ni bila znana. Toda tu in tam so se le pojavili besedam podobni deli, na primer alkultilbernil - verjetno bi moralo pisati "Ankunft in Berlin"(prihod v Berlin). Če je bila ta domneva pravilna, sta morali biti črki R in L med seboj povezani, to je, s kablom na stikalni plošči zamenjani, črke A, K, U, F,T, I, B in E pa ne. Z analizo nadaljnjih zaporedij črk je bilo mogoče odkriti še druge pare črk, ki so bile na stikalni plošči med seboj zamenjane. Rejewski je imel zdaj v rokah povezave na stikalni plo-

šči skupaj s konfiguracijo valjev, torej popoln dnevni ključ. S tem je lahko dešifriral vsako sporočilo tistega dne.

Rejewski je iskanje dnevnega ključa silno popreprostil s tem, ko je problem konfiguracije valjev ločil od od problema povezav na stikalni plošči. Vsaka zase sta bili obe zadevi rešljivi. V začetku smo ocenjevali, da bi trajalo dlje od življenjske dobe vesolja, da bi preizkusili vsak možni ključ enigme. Rejewski je potreboval samo eno leto, da je sestavil katalog dolžine verig, od takrat naprej pa je lahko odkril dnevni ključ, še preden je bil dan pri koncu. Zdaj, ko je poznal ta ključ je lahko sporočila bral kot pravi prejemnik.

Z epohalnim uspehom Rejewskega je nemški radijski promet postal odprta knjiga. Poljaki niso bili v vojni z Nemci, vendar so čutili, da jim grozi invazija, in jim je silno odleglo, ko so razrešili skrivnost enigme. Zdaj so lahko ugotovili kakšne načrte imajo nemški generali, in so tako imeli več možnosti za uspešno obrambo. Od tega dela Rejewskega je bila odvisna usoda poljskega naroda, in svoje države res ni razočaral.

Slika 3: Marian Rejewski

4 Moderno šifriranje

4.1 Alice in Bob se predstavita

„Prišel sem v pisarno Rona Rivesta," se spominja Leonard Adleman. Ron je v roki držal članek, zaradi katerega je bil precej razburjen. Tisto kar je Ron Rivest držal v rokah, je bil članek Diffieja in Hellmana, v katerem sta predstavila svojo idejo enosmernega šifriranja. Nazadnje je Rivest prepričal Adlemana, da se v tem problemu skrivajo zanimiva matematična vprašanja, in odločila sta se, da bosta poiskala enosmerno funkcijo, ki bo ustrezala zahtevam. Pri tem lovu je sodeloval tudi Adi Shamir. Vsi trije so delali kot raziskovalci v osmem nadstropju MIT-ovih laboratorijev za računalniške vede.

Rivest, Shamir in Adleman so sestavljali odlično ekipo. Rivest, računalniški strokovnjak, je imel to izredno sposobnost, da je znal sprejeti nove ideje in jih uporabiti na področjih, na katera ne bi nihče pomislil. Shamir, prav tako računalniški strokovnjak, je imel bliskovit razum in je bil sposoben vse nepomembno pustiti ob strani in se osredotočiti na glaven problem. Adleman, kot matematik vzdržljiv, temeljit in potrpežljiv, je bil pristojen predvsem zato, da je odkrival napake v idejah Rivesta in Shamirja.Rivest in Shamir sta eno leto razvijala ideje, Adleman pa je to leto preživel tako, da je ovrgel prav vse njune ideje. Trojka je počasi izgubljala upanje, vendar je vedela,da so neuspehi ključni na poti do uspeha in njihova prizadevanja so bila kmalu nagrajena.

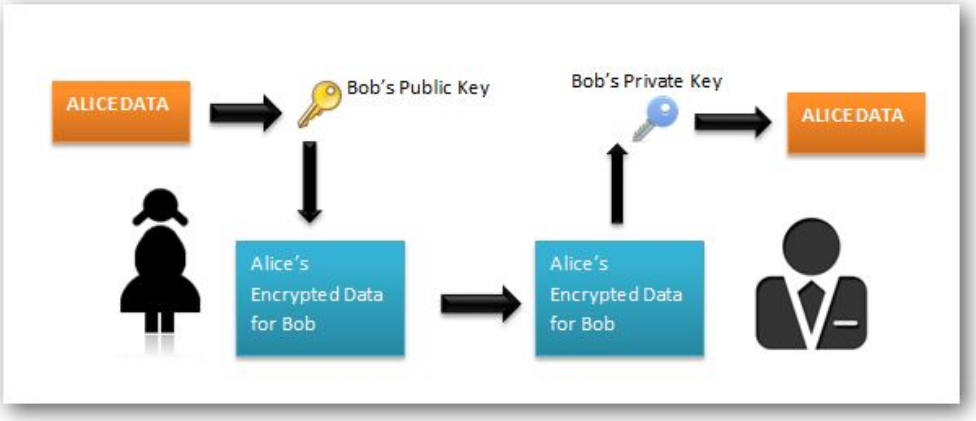
Aprila leta 1977 so Rivest, Shamir in Adleman v hiši nekega študenta preživljali praznik judovske paše. Popili so precej vina in se okoli polnoči odpeljali domov. Rivest ni mogel zaspati in je z matematičnim učbenikom legel na kavč. Začel je razmišljati o problemi s katerim se je že dolgo ukvarjal. ALi je mogoče razviti asimetrično šifriranje? Ali je mogoče najti takšno enosmerno funkcijo, ki jo je mogoče obrniti samo če ima naslovnik določeno informacijo?? Nenadoma se je megla zbistrila in ideja je bila tu. Preostanek noči je preživel z matematičnim obdelovanjem svoje ideje in še pred prvim svitom je imel napisan popoln znanstveni članek. Rivestu se je posrečil preboj, vendar njegov uspeh ne bi bil mogoč brez dolgoletnega sodelovanja z Adlemanom in Shamirjem. Na koncu članka je navedel avtorje po abecedi: Adleman, Rivest in Shamir.

Naslednje jutro je Rivest izročil dokument Adlemanu, ki je kot ponavadi poskušal ovreči argumentacijo, vendar tokrat ni mogel najti nobene napake. Samo proti seznamu avtorjev je ugovarjal:„ROnu sem rekel naj moje ime črte, saj je bila to vendar njegova iznajdba, ne moja. Toda Ron je temu ugovarjal in začela sva se prepirati. Nazadnje sva se dogovorila, da bom dokument odnesel domov in ga natančno pregledal. Naslednji dan sem ROnu predlagal, naj me imenuje na tretjem mestu. Vem še, da sem si mislil, da bo to zanimiv

članek, ki bo nosil moje ime.“ Adleman se je zelo motil. Postopek, ki so ga poimenovali ne ARS, ampak RSA.

Kaj so znanstveniki pravzaprav iskali, da bi v praksi lahko uporabljali asimetrično šifriranje.

1. Alice mora sestaviti javni ključ, ki ga bo javno izročila Bobu (in drugim), da bo lahko šifriral njej namenjena sporočila. Javni ključ mora biti enosmerna funkcija, torej mora biti praktično nemogoče, da bi kdo to funkcijo obrnil in dešifriral sporočilo za Alice.
2. Alice mora imeti možnost za dešifriranje njej namenjenih sporočil. Za ta namen potrebuje zasebni ključ, poseben košček informacije, ki ji bo omogočil obrniti javni ključ. Tako ima Alice (in samo Alice) možnost za dekriptiranje njej namenjenih sporočil.



Slika 4: Asimetrično šifriranje

4.1.1 Matematika RSA

Sledi opis čisto matematične funkcije za šifriranje s postopkom RSA.

1. Alice izbere dve velikanski praštevili, p in q. Praštevili naj bi bili zelo veliki, zaradi preprostosti pa bomo kot primer vzeli, da je Alice izbrala p=17 in q=11. Ti števili mora skrbno ohraniti samo zase.
2. ALice pomnoži praštevili med seboj in dobi novo število, v tem primeru N=187. Zdaj izbere še eno število, e, na primer e=7.(e in (p-1)*(q-1)) naj bi bili brez skupnega delitelja, vendar je to že tehnična podrobnost.
3. Zdaj lahko Alice e in N objavi v javnem seznamu. Ker sta obe števili potrebni za šifriranje, morata biti dostopni vsem, ki želijo šifrirati sporočilo za Alice. Tvorita tako imenovani javni ključ. (Število e ni rezervirano za Alice, lahko je sestavni del tudi drugih javnih ključev. Vsekakor pa morajo biti vrednosti N, ki so odvisne od vsakokrat izbranega p in q, za vsak ključ drugačne.)
4. Da bi sporočilo lahko šifrirali, ga moramo najprej spremeniti v število M. Tako lahko na primer besedo po kodi ASCII spremenimo v binarno število, ki ga potem za namen šifriranja lahko obravnavamo kot decimalno število M. Ta M šifriramo in dobimo tajno besedilo po naslednji formuli.
$$C = M^e \pmod{N}$$
5. Vzemimo, da želi Bob poslati samo simboličen znak za poljuben X. V kodi ASCII je predstavljen kot 1011000, kar ustreza decimalnemu številu 88. Zato je M=88.
6. Da bi sporočilo šifriral, Bob najprej poišče Alicein javni ključ, torej N=187 in e=7. Ti števili lahko vstavi v šifrirano formulo Alice namenjenega sporočila. Pri M=88 dobimo formulo
$$C = 88^7 (\mathrm{mod} 187)$$
7. Žepni računalnik ni dober za takšne izračune, saj zaslon sploh ne more prikazati naravnost astronomski številk. Vsekakor pa obstaja dober trik za izračunavanje potenc v modularni aritmetiki. Ker je 7=4+2+1, vemo tudi naslednje:
$$\begin{aligned} 88^7 \bmod 187 &= [88^4(\mathrm{mod}187) \times 88^2(\mathrm{mod}187) \times 88^1(\mathrm{mod}187)] \bmod 187 \\ 88^1 &= 88(\mathrm{mod}187) \\ 88^2 &= 77(\mathrm{mod}187) \\ 88^4 &= 132(\mathrm{mod}187) \\ 88^7 &= 11(\mathrm{mod}187) \end{aligned}$$
Zdaj Bob pošlje Alice šifrirano besedilo, C=11

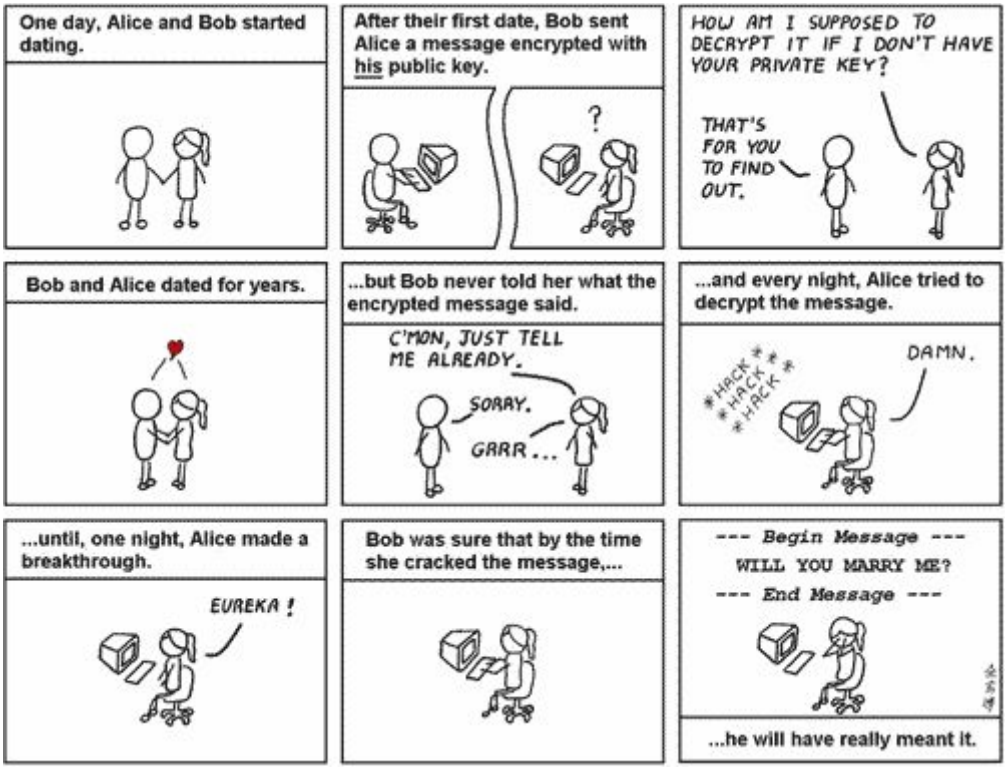
8. Vemo, da so eksponenti v modularni aritmetiki enosmerne funkcije, zato se je zelo težko vrniti iz C=11 in odkriti prvotno sporočilo M Eve sporočila torej ne more odpreti.
9. Alice pa lahko sporočilo prebere, ker ima za to potrebne podatke: vrednosti p in q. Najprej izračuna posebno število d, tako imenovani ključ za dešifriranje, imenovan tudi zasebni ključ. Število d se izračuna po naslednji formuli:

$$\begin{aligned} e \times d &= 1(\mathrm{mod}(p-1) \times (q-1)) \\ 7 \times d &= 1(\mathrm{mod}16 \times 10) \\ 7 \times d &= 1(\mathrm{mod}160) \\ d &= 23 \end{aligned}$$

   (Vrednosti d ne dobimo neposredno, s tako imenovanim Evklidovim algoritmom pa sorazmerno preprosto in hitro).
10. Da bi sporočilo dešifrirala, Alice preprosto uporabi naslednjo formulo:

$$\begin{aligned} M &= C^d(\mathrm{mod}187) \\ M &= 11^{23}(\mathrm{mod}187) \\ M &= 11^1(\mathrm{mod}187) \times 11^2(\mathrm{mod}) \times 11^4(\mathrm{mod}187) \times 11^6(\mathrm{mod}187)](\mathrm{mod}187) \\ M &= [11 \times 121 \times 55 \times 154](\mathrm{mod}187) \\ M &= 88 \\ M &= X \text{ v ASCII} \end{aligned}$$

   Rivest, Shamir in Adleman so s tem ustvarili posebno enosmerno funkcijo, ki jo je mogoče obrniti samo, če poznamo tajni vrednosti p in q. Vsak uporabnik te funkcije ju lahko priredi zase z izbiro vrednosti p in q, ki med seboj pomnoženi dasta N. S tem osebnim N lahko šifriramo sporočila, ki jih lahko dešifrira samo upravičeni prejemnik, ker pač samo on pozna p in q in s tem tudi ključ za dešifriranje d.



Slika 5: Alice in Bob

5 Zaključek

Zgodovina nas uči, da so ljudje začeli šifrirati besedila kmalu potem, ko so izumili pisavo. Izumljali so vedno nove metode, ki so bile zmeraj bolj zapletene. Od skrivnih pisav, enostavnih zamenjav črk in znakov preko bolj zapletenih zamenjav z uporabo ključev, kot je na primer Vigenèrjeva šifa, kjer se ista črka vsakič znova transformira v drugo črko. Dešifrerji so vse uspeli dešifrirati.

Z uporabo strojev se je šifriranje mehaniziralo. Najbolj znana je uporaba nemške Enigme med drugo svetovno vojno. In tudi to je uspelo bistrim umom dešifrirati. Najprej Marian Rejevski in za njim Alan Turing. Slednji velja za očeta računalnika. Z uporabo „velikih“ strojev – imenovanih „bombe“ je skupina pod vodstvom Alana Turinga v Bletchley parku dnevno računala ključe Enigme in s tem omogočala zaveznikom, da so lahko brali nemška sporočila. Žalostna usoda, ki je po vojni zaradi homoseksualnosti doletela Alana Turinga – zaradi pritiska javnosti je naredil samomor – se najbolje odraža v komentarju nekega lorda, ki je Turinga vseskozi tudi in predvsem moralno podpiral: „Kaj bi šele bilo, če bi se to razvedelo prej. Utegnili bi celo izgubiti vojno.“

Razvoj šifriranja v sedanjem času narekujejo računalniki. Vendar pa razvoj metod še vedno temelji na bistrosti človeškega uma. Sodobne metode uporabljajo matematiko in velika praštevila. Uporaba slednjih nam je prinesla asimetrično šifriranje, ki služi ne samo šifriranju sporočil, ampak tudi elektronkemu podpisovanju dokumentov, ki je že z zakonom izenačeno lastnoročnemu podpisovanju.

Ne glede na to, kako bistri in iznajdljivi so bili šifrerji skozi zgodovino – in vedno korak pred dešifrerji – so jih slednji vedno „ujeli“. Sodobne metode lahko „bežijo“ z uporabo vedno daljših ključev – z uporabo vedno večjih praštevil, vendar jim vedno večja računalniška moč združena v gruče računalnikov vedno bolj „diha za ovratnik“. Kako dolgo še, bo zgolj daljšanje ključev vzdržalo napade dešifrerjev?

Literatura

[1] BUCHMANN, J. A., 2004, Introduction to cryptography, Springer-Verlag NY

[2] OETIKER, Tobias, 2006, Ne najkrajši uvod v LaTeX2e

[3] SINGH, Simon, 2006, Knjiga šifer

[4] SINGH, Simon: The Code Book, Crypto CD ROM

[5] Wikibooks, Open book for an open world: `http://en.wikibooks.org/wiki/Cryptography`

[6] Wikipedia, the Free Encyclopedia: `http://en.wikipedia.org/`

[7] Wikipedia, Cryptography Portal: `http://en.wikipedia.org/wiki/Portal:Cryptography`

[8] `http://simonsingh.net/cryptography/`

[9] Journey into Cryptography: `https://www.khanacademy.org/math/applied-math/cryptography`

[10] Uporaba kriptografije v internetu: `http://www.si-ca.si/kripto/index.htm`