KRIPTOGRAFIJA

SNOVNE PRIPRAVE ZA KRIPTO-KROŽEK (ALI MATEMATIČNE DELAVNICE) V OSNOVNIH IN SREDNJIH ŠOLAH

Ljubljana, avgust 2004 Nataša Jerman

UVOD

Kriptografija se v našem vsakdanjem življenju pojavlja več kot pa si morda predstavljate. Pomislite le na bančništvo (klik, ...), pri prenosu podatkov prek telefona (wap), pri internetu, ... Pa vendar večina ljudi še nikoli ni pobliže spoznala kriptografije, vemo sicer, da se veliko uporablja, ne vemo pa, kako sploh lahko s kriptografijo zagotovimo varnost, ne poznamo niti njenih osnovnih »prijemov«.

Moj namen je bil ustvariti skupek priprav, ki bi učencem približale kriptografijo že v osnovni šoli, predstavljena pa naj bi jim bila bolj prek igre. Velikokrat se izkaže, da se za na videz enostavnimi igrami nahaja ogromno matematike, ogromno matematičnih zank in enačb. Moj cilj ni učence oziroma dijake naučiti teh matemtičnih ozadij, temveč jim kriptografijo čim bolj približati, ustvariti v nijh vedoželjnost, zanimanje, da bi zvedeli še kaj več, kar lahko s samostojnim iskanjem tudi najdejo, oziroma jim lahko mi na njihovo željo to predstavimo. Moj namen je torej v otroku vzbuditi neko željo po novem znanju, po novih ugotovitvah ter vednost, da je otrok dobil majhen občutek kako zanimiva je kriptografija.

Pred vami se nahaja skupek snovnih priprav, ki sem jih pripravila kot projekt pri predmetu Kriptografija, ki sem ga poslušala na podiplomskem študiju matematike. Pred vami se nahaja 11 priprav, ki so postavljena v logičnem vrstnem redu.

Začnemo z uvodno uro, kjer povemo malo zgodovinjskega ozadja kriptografije, pokažemo, kako daleč sega in povemo nekaj primerov v zgodovini, ki bi lahko bili brez uporabe kriptografije precej drugačni. Otroci se v tej uri tudi prvič srečajo s pojmom simetrična in asimetrična kriptografija.

V drugi uri, ki je bolj praktična, učenci (dijaki) sestavijo skupine in ustvarjajo nevidna črnila. Ta ura je zelo zanimiva, sploh če vmes vpletemo še zgodbico o tem, da so bili v času 2. svetovne vojne volilni lističi na volitvah v Nemčiji označeni z nevidnim črnilom. Hitler je dal nato volilne lističe pregledati in ukazal ubiti vse, ki so glasovali proti njemu. So pri nas tudi kdaj bili označeni?

Tretja ura je ura nenavadnih, »bizarnih« načinov pošiljanja sporočil. Načini pošiljanja so enostavni, dijaki znova sestavijo skupine, poskusijo kako metoda deluje in jo proti koncu ure predstavijo ostalim sošolcem.

V četrti uri spoznamo eno izmed bolj »simpatičnih« skrivnih pisav - pigpen (prašičja ograjica), ki so jo uporabljali v 1. svetovni vojni. Dijaki jo v tej uri spoznajo,zvedo, kako lahko sestavijo svojo »ograjico« in si pošiljajo skrivna sporočila.

Tako. V peti in šesti uri se posvetimo čisto klasični kriptografiji. Spoznamo, kaj sploh je klasična kriptografija, kakšne metode šifriranja štejemo kot klasično kriptografijo. V tej uri spoznamo pomični tajnopis, ki se precej enostavno šifrira in dešifrira, če imamo v rokah kriptografski prstan. Sedma ura je namenjena njegovi izdelavi.

Osma ura je bolj infomativna. Učenci (dijaki) s pomočjo zgodbice o Kraljici Mary spoznajo, kako hitro zlomljiva je klasična kriptografija in da je lahko celo človeško življenje odvisno od tega ali bodo lahko dešifrirali neko sporočilo. To uro lahko spustimo in zgodbo samo povem na koncu ure klasične kriptografije.

V naslednjih dveh urah spoznamo idejo, ki je čisto klasičen pomični tajnopis spremenila. Spoznamo novo metodo, imenovano Vigenerjev tajnopis, nadgradnjo pomičnemu tajnopisu. Ljudje so dolgo časa verjeli, da je ta metoda nezlomljiva in da je to višek kriptografije. Pa se je izkazalo, da temu ni tako.

Tako v enajsti uri spoznamo gospoda Babbagea in njegov način, ki je razbil Vigenerjev tajnopis. Spoznamo princip, s katerim je mogoče razbiti vsak tajnopis, ki je bil zašifriran s pomočjo Vigenerja.

Zadnje tri ure so primerne za boljše učence v višjih razredih OŠ ali pa za dijake, ki so že spoznali delo z moduli (če z moduli še niso delali, eno uro namenimo tem, da spoznajo module in z njimi malce računajo).
Ko so razbili Vigenerjev tajnopis, se je v ljudeh spet pojavil dvom – ali sploh obstaja kakšen varen način kodiranja, kaj, kar se ne bi dalo zlomiti. Tako so se matematiki dolgo časa ukvarjali z ugotavljanjem, kako sestaviti ključ, ki bo nezlomljiv. Tako so matematiki Rivest, Shamir in Adelman sestavili nov način kodiranja, ki je pod določenimi pogoji nezljomljiv. V dveh urah skušamo po podobnih korakih, kot so do njega prišlji njegovi izumitelji, spoznati princip delovanja RSA-ja. Spoznamo kako deluje in zakaj je v bistvu nezlomljiv.

Ker se v modernih časih vse preveč ukvarjamo z elektronsko pošto, z elektronskimi dokumenti v 14 uri, to je v zadnji uri, spoznamo princip RSA digitalnega podpisa, ki nam zagotavlja pristnost pošiljatelja.

Tako to je bil kratek uvod v to, kar naj bi v pripravah našli. Upam, da bodo ure čim bolj aktivne, zanimive in produktivne. Veliko zabave in novih znanj z vašimi učenci (oziroma dijaki) vam želim!

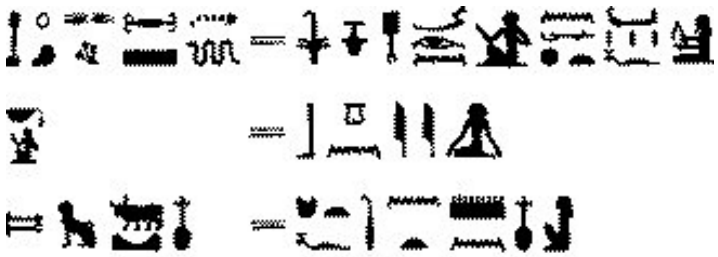
KRIPTOGRAFIJA - splošen pregled

KRIPTOS = skrito
GRAPHIA = pisanje

⇒ KRIPTOGRAFIJA = skrivno pisanje

Kaj sploh je kriptografija? Kot nam že sam prevod besede po delih pove, je to neke vrste skrivno pisanje. Osnovni namen kriptografije je omogočiti dvema človekoma, da se sporazumevata tako, da njun nasprotnik ne bo mogel dobiti oziroma razumeti sporočila. Ali ljudje skrivajo svoja sporočila že zelo dolgo? Da, seveda.

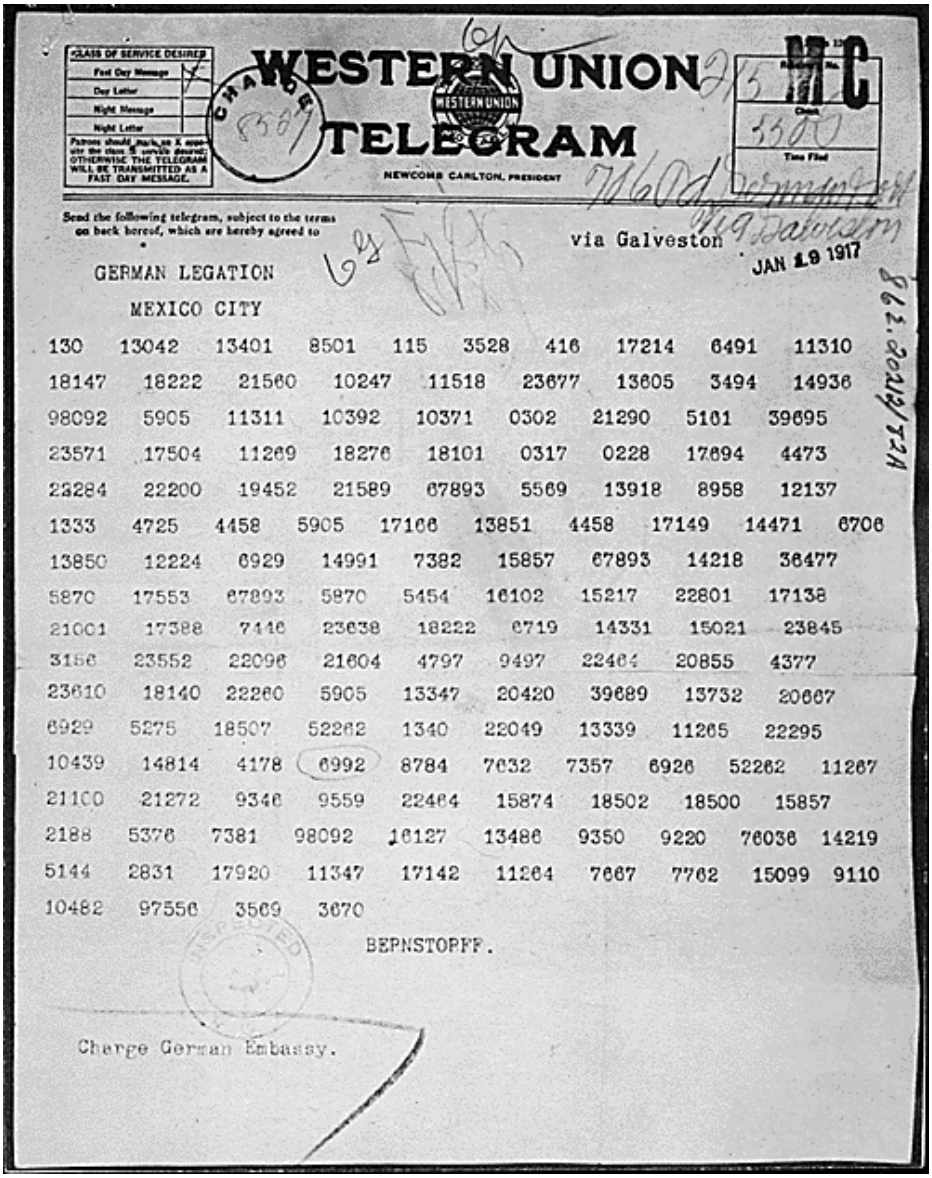
Skrito pisanje najdemo v vseh obdobjih zgodovine. Da bi opisali celotno zgodovino kriptografije, bi morali napisati kar nekaj debelih knjig, zato bomo mi omenili le nekaj izmed njih. Začetke kriptografije vidimo že zelo zgodaj – kot primer lahko navedemo nam neznane jezike, risbe, ki so krasile stene jam, egipčanski hieroglifi, ...



Slika 1: Egipčanski hieroglifi

Bolj zahtevno kriptografsko znanje se je začelo v obdobju I. Svetovne vojne, saj so malo pred vojno izumili radio. Že takrat so iz štaba v štab vohuni prenašali sporočila, nasprotnikovi vohuni pa so bili vseskozi na preži, če bi jim slučajno uspelo prestreči katero izmed mnogih sporočil. Ko se je pojavil radio, je bilo obema stranema jasno, da je to velika prednost. Glavni generali so se lahko preko radija pogovarjali z bataljoni po vseh frontah, z njimi imeli vseskozi stike in poznali vse nove spremembe na bojiščih. Edini problem, ki se je tu pojavil je bil, da se je lahko nasprotnik brez večjih težav lahko priklopil na frekvenco nasprotnika in prisluškoval vsem pogovorom. Nevarnost prisluškovanja je težila po nekem novem načinu kadiranja, saj vsi do tedaj znani načini šifriranja niso bili varni. Tako so bila vse sporočila, ki jih je uspela dobiti ena ali druga stran, zelo hitro dešifrirana. Pomembnost dešifriranja teh sporočil se dobro pokaže pri primeru Zimmermanovega telegrama.
V začetku leta 1917 so Nemci pripravljali novo ofenzivo na Angleže, vendar so vedeli, da bodo pri invaziji potopili tudi nekaj ameriških ladij. Amerika je bila v tistem trenutku še nevtralna, vendar so se Nemci zavedali, da lahko v primeru potopitve ameriških ladij Amerika stopi na stran Angležev.Prav zaradi tega je nemški zunanji minister Zimmerman odločil, da bo poslal telegram v Mehiko. V telegramu je zapisal, da v primeru, da gre Amerika po ofenzivi v boj proti njim, želi, da Mehika in Nemčija postaneta zaveznici. Nemčija naj bi v tem primeru pomagala

Mehiki osvojiti nazaj ozemlja, kot so Texas, Arizona, ... S tem bi Nemci zagotovili, da večina ameriških čet ostala doma, saj bi morala braniti domače meje. Domač teritorij je bil Ameriki jasno bolj pomemben kot angleške bitke.
Tako je 16. januarja Zimmerman poslal zašifriran telegram z zgornjo ponudbo. Telegram so prestregli Angleži, ga dešifrirali in posredovali Ameriki. Od tistega trenutka dalje Amerika ni bila več nevtralna, ampak je stopila na stran angležev.



CLASS OF SERVICE DESIRED
Fast Day Message
Day Letter
Night Message
Night Letter
Patrons should check one class of service desired; OTHERWISE THE TELEGRAM WILL BE TRANSMITTED AS A FAST DAY MESSAGE.

CHARGE 8507

WESTERN UNION
TELEGRAM
NEWCOMB CARLTON, PRESIDENT

NC
Check 1300
Time Filed

Send the following telegram, subject to the terms on back hereof, which are hereby agreed to

via Galveston

JAN 19 1917

GERMAN LEGATION
MEXICO CITY

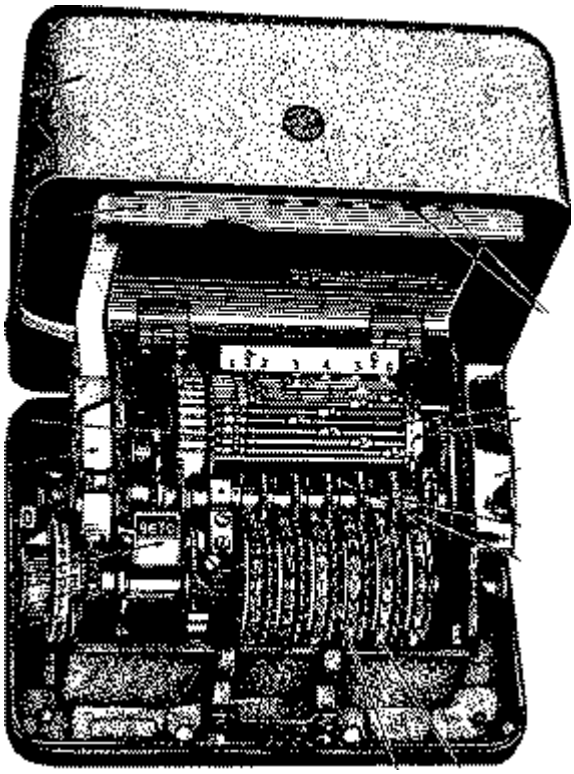
130 13042 13401 8501 115 3528 416 17214 6491 11310
18147 18222 21560 10247 11518 23677 13605 3494 14936
98092 5905 11311 10392 10371 0302 21290 5101 39695
23571 17504 11269 18276 18101 0317 0228 17694 4473
23284 22200 19452 21589 67893 5569 13918 8958 12137
1333 4725 4458 5905 17166 13851 4458 17149 14471 6706
13850 12224 6929 14991 7382 15857 67893 14218 36477
5870 17553 67893 5870 5454 16102 15217 22801 17138
21001 17388 7446 23638 18222 6719 14331 15021 23845
3156 23552 22096 21604 4797 9497 22464 20855 4377
23610 18140 22260 5905 13347 20420 39689 13732 20667
6929 5275 18507 52262 1340 22049 13339 11265 22295
10439 14814 4178 6992 8784 7632 7357 6926 52262 11267
21100 21272 9346 9559 22464 15874 18502 18500 15857
2188 5376 7381 98092 16127 13486 9350 9220 76036 14219
5144 2831 17920 11347 17142 11264 7667 7762 15099 9110
10482 97556 3569 3670

BERNSTORFF.

Charge German Embassy.

Slika 2: Zimmermanov telegram

V I. in II. Svetovni vojni so strokovnjaki izdelali kar nekaj kodirnih naprav – kriptografski prstan, Enigma, Fish, ...



Slika 3: motor Enigme

Zanimiv nov način skrivanja sporočil so si izmislili Američani med II. Svetovno vojno. Ta način je bil način, pri katerem so vsa sporočila prenašali po radiu. Ljudstva, imenovano Navajo, so Američanom postali zelo zanimivi, saj jih je bilo zelo malo in so govori čisto poseben, skoraj izumrl jezik. Tako so ljudi iz plemena Navajo usposobili za posiljanje sporočil – v njihovem jeziku so govorili, nihče jih ni razumel, nekatere izmed njihovih besed so dobile popolnoma drugačen pomen -za vojaške zadeve so imeli imena živali, ipd. Prav zaradi malega števila Navajo govorcev, je bil ta način pošiljanja sporočil zelo varen. Nihče ni niti približno razumel, o čem govorijo.

Slika 4: Navajo govorec pošilja sporočilo

Slika 5: Navajo govorci kod

V splošnem pa že stoletja kralji, kraljice, vladarji in generali zanašajo na pošiljanje skrivnih sporočil, zato, da sovražniki ne bi izvedeli, kaj nameravajo. Vedeli so, kakšne bi lahko bile posledice, če bi pisma prišla v napačne roke. Bistvene informacije bi lahko (ali pa so) sprmenile potek vojen, izbor vodilnih v državah... Ravno zaskrbljenost, da bi lahko nasprotnik prestregel še tako skrivno sporočilo, je spodbujala razvoj kriptografije.

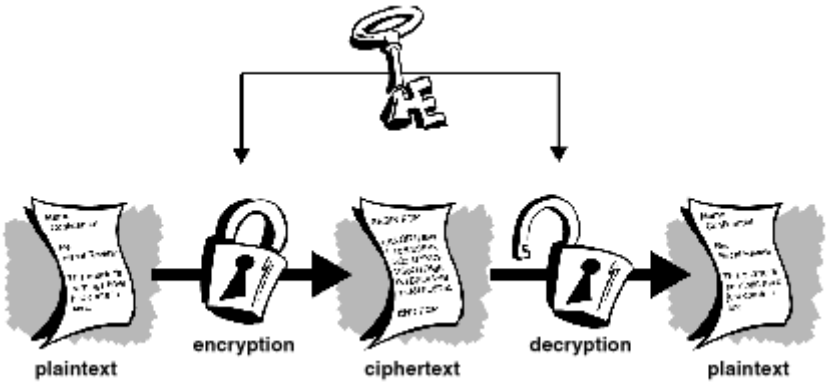
Tudi v današnjem času vlade, vohuni, FBI in podobne organizacije pošiljajo šifrirana sporočila – za to imajo zaposlene kriptografe, ki se dan in noč za zmogljivimi računalniki ukvarjajo z izumljanjem novih načinov kodiranja in razbijanjem že obstoječih.

Postavi se nam vprašanje: »Kako sploh doseči varen prenos sporočila?« Ena izmed izmed možnosti, ki pa ni prava kriptografija je steganografija – to je način, pri katerem sporočila ne spreminjamo, ampak ga le skrivamo pred drugimi. Sem spada pisanje z nevidnim črnilom, skrivanje sporočil v dvojnih predalih, tetoviranje sporočil na glavo, ki jih potem skrijejo z lasmi, ... V tem primeru je problem, ko nasprotnik prestreže sporočilo. Takrat ga enostavno prebere in zve vse. Zato je nastala težnja, da bi nasprotnik kljub temu, da prestreže sporočilo, ne znal prebrati vsebine.

Kako zgornje doseči? Recimo, da želi Anita poslati sporočilo svojemu novemu fantu, Bojanu. Oskar, Anitin bivši fant, je še vedno ljubosumen in hoče Anito nazaj, zato prisluškuje vsem njunim pogovorom in prestrega sporočila. Originalno sporočilo, ki ga želi poslati Anita, imenujemo čistopis. Čistopis je lahko kakršno koli zaporedje znakov, črk, številk, angleški tekst, slovenski tekst... Ker želi Anita sporočilo varno poslati, čistopis zašifrira s pomočjo šifrirnega ključa. Oskar, ki ključa ne pozna, sporočila ne more prebrati. Medtem ko bo Bojan z uporabo šifrirnega ključa sporočilo brez problema prebral sporočilo.

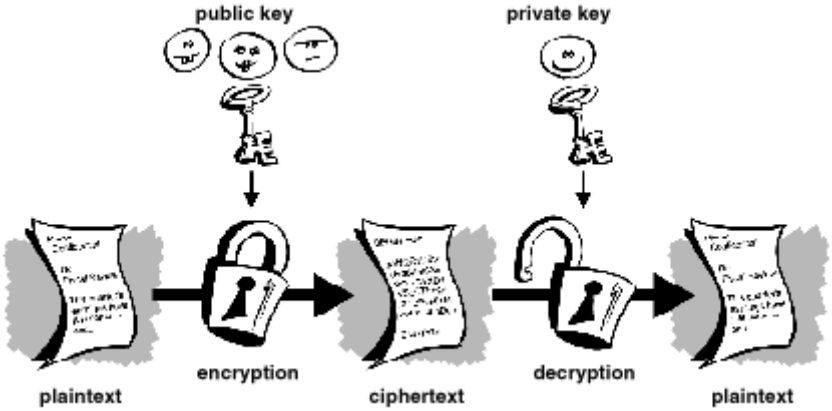
Poznamo dve veji kriptografije – simetrično in asimetrično. Razlika med njimi je v šifrirnih ključih. Poskusimo razložiti razliko med simetrično in asimetrično kriptografijo kar z navadnimi ključi, ključavnicami in škatlo.

O simetrični kriptografiji govorimo, kadar imata pošiljatelj in prejemnik ISTI ključ. Anita torej zapiše sporočilo, ga zaklene s ključem v škatlico. Škatlico nato po pošti pošlje Bojanu, ki ima doma identičen ključ, ta z njim odklene škatljico in prebere sporočilo.



Slika 6: simetrična kriptografija

Pri asimetrični kriptografiji pa je zagotovljena še večja varnost kot pri simetrični. Pri asimetrični potrebujemo dva ključa – eden od teh dveh je privatni, drugi pa javni. Javni ključ poznajo vsi, privetnega pa le prejemnik. Kako bi to razložili s škatlami? Recimo, da ima Anita veliko pošte in si da izdelati lastno ključavnico, ki jo lahko vsi kupijo na pošti. Vsak, ki ji želi poslati sporočilo, mora kupiti njeno ključavnico in z njo zakleniti škatlo. Takoj ko škatlo zaklene tudi sam ne more več priti do sporočila. Edina, ki lahko škatlo odklene, je Anita.



Slika 7: asimetrična kriptografija

Tako, to je bil kratek uvod. Več bomo povedali v prihodnjih urah.

NEVIDNO ČRNILO

Starinska metoda skrivnega pisanja, popolnoma drugačna od vseh modernih metod z računalniki, je pisanje z nevidnim črnilom. Nevidno črnilo je takšna snov, ki na listu papirja ni vidno, dokler z nijim nekaj ne naredimo, torej dokler ne poteče kakšna izmed kemičnih reakcij. Že v starih časih so ta način veliko uporabljali, prav tako pa se ga poslužujejo vohuni tudi v današnjih modernih časih.

Najboljša nevidna črnila so narejena s posebnimi kemikalijami, ki jih lahko uporabljajo le kemiki v laboratorijih, saj ta črnila vsebujejo nevarne snovi. Mi bomo spoznali le varne in gotove metode kako narediti nevidno črnilo, uporabljali bomo nenevarne in obstojne reagente.

Vohuni redko pošiljajo svoja skrivna sporočila, napisana z nevidnim črnilom, na praznem, nepopisanem listu papirja, saj bi bilo zelo sumljivo, če bi kdo to sporočilo prestregel. Ponavadi je na papirju zapisano lažno vidno sporočilo, ki s skrivnim nima povezave. Skrivno sporočilo je zapisano med vrsticami lažnega sporočila, ob robovih ali pa celo na zadnji strani kakšne priložene »nedolžne« fotografije.
Eden izmed trikov, ki ga tudi uporabljajo je, da v določeni knijgi ali časopisnem članku z obkroževanjem ali podčrovanjem črk z nevidnim črnilom zapišejo skrivno sporočilo. Prejemnik lahko sedaj brez večjih težav prebere sporočilo, edino kar mora paziti je to, da črke bere po vrstnem redu.

Da bi sporočilo bilo še težje za odkriti za morebitnega napadalca, bi z nevidnim črnilom lahko zapisali tudi kodirano sporočilo. Tako bi imel napadalec več težav pri ugotavljanju sporočila – če bi slučajno odkril kako nevidno črnilo postane vidno, bi ga vseeno še moral dešifrirati.

Dijake razporedimo v 4 skupine. Vsaki skupini razdelimo po en učni list ter vse pripomočke, ki jih pri »poskusih« potrebujejo. Določimo vodje skupin in jim povemo, da bo morala po končanem delu skupina predstaviti svoje novo pridobljeno znanje ter »izdelke«. Opozorimo jih, da se držijo navodil in da naj na liste zapišejo tudi lažna sporočila, ki bi morebitne »napadalce« zmedla.

SKUPINA 1:

Črnila, ki se razvijejo na toploti

Potebujemo:

- 1 limono ali grenivko;

- cedilo;
- 2 kozarčka;
- 150 W žarnico (ali likalnik);
- mehak tanek čopič;
- mehak papir.

Za nevidno črnilo bi lahko uporabili sok katerekoli citronke, ali pa sok čebule. Mi bomo uporabili sok limone oziroma rumene grenivke, ki sta že v osnovi bolj svetlih barv. Vsi ti sokovi so organske snovi, ki porjavijo, če jih (»nežno«) segrejemo.

Najprej ožemite limono in sok precedite skozi cedilo, tako, da v soku ni grudastih delcev in koščic. S čopičem, ki mora biti popolnoma čist, zelo narahlo zapišemo sporočilo. Mehak čopič uporabljamo zato, ker bi lahko z vsemi drugimi pisali (recimo z nalivnim peresom) puščali sled, ali pa poškodovali vlakna papirja in bi zaradi takšnih napak sporočilo postalo vidno – oziroma, napadalec bi posumil, da se nekaj skriva v pismu. Prav zaradi vlaken papirja uporabljamo mehak papir, da se sok lepo vpije v vlakna in ne pušča površinskih sledi. Na kvalitetnem foto-papirju, bi se sok posušil na površini papirja in bi se sporočilo dalo prebrati že pri dnevni svetlobi.

Sedaj počakamo, da se napisano sporočilo posuši. Sporočilo, ki smo ga napisali, se bo razvilo na toploti. List s sporočilom počasi zapeljemo preko že nekaj časa prižgane žarnice.

Za razvoj sporočila nikoli ne uporabljajte ognja! Rezultat uporabe ognja bi bil le ožgan papir, ter velika nevarnost, da se nam skrivno sporočilo vžge. Če žarnice nimate na voljo, lahko papir raje nežno zlikate z likalnikom.

Sedaj previdno povlečemo sporočilo prek žarnice in pazimo, da si ne opečemo prstov. In sporočilo, sedaj zapisano z rjavimi črkami, je pred nami.

SKUPINA 2:

Črnilo, ki postane vijolično

Potebujemo:
- noževo konico fenolftaleina;
- pralni prašek;
- mehak tanek čopič;
- vato;
- 2 kozarčka;
- mehak papir.

Fenolftalein je bel prašek, ki je indikator za baze. To pomeni, da se obarva, če ga zmešamo z bazo. Fenolftalein je snov, ki jo čarovniki uporabljajo za trike, ko spreminjajo »vodo« v »vino«, saj se, ko reagira z bazo, obarva vijolično.

Čisti fenolftalein prodajajo v večjih drgerijah (je pa na žalost zelo drag). V Ameriki in še v nekaterih državah fenolftalein dajejo v vse odvajalne tablete, ki pa pri nas niso v prodaji, saj so po naših merilih prenevarne. Če bi dobili kakšne takšne tablete, jih lahko enostavno raztopite v alkoholu in fenolftaleinska raztopina za pisanje je pripravljena.

Mi bomo uporabili prašek fenolftaleina. Eno žličko praška popolnoma raztopimo v pol decilitra alkohola, pazimo, da je čim manj grudic. S čopičem narahlo zapišemo sporočilo in počakamo, da se posuši. Ko je črnilo posušeno, na listu ni videti nobenih sledi pisanja.

Sedaj želimo sporočilo prebrati. V malo vode raztopimo pralni prašek in v to raztopino pomočimo kos vate. Z vato potem nežno pritiskamo na list, na katerem je sporočilo. Paziti moramo, da ne mažemo z vato, saj bomo v tem primeru sporočilo razmazali.

Ko pritiskamo vato po celem listu, se nam vijolično obarvano sporočilo prikaže. Enostavno ga sedaj preberemo.

SKUPINA 3:

Črnilo, ki se prikaže, če ga posipamo s prahom

Potebujemo:
- mleko;
- navaden svinčnik;
- mehak tanek čopič;
- šilček;
- trd papir.

Eno izmed najbolj enostavnih in najboljših nevidnih črnil je, če za črnilo vzamemo kar navadno mleko. Čopič namočimo v mleko in z njim pišemo po trdem papirju. Ko sporočilo zapišemo, počakamo, da se mleko posuši.

Da se bo besedilo prikazalo nazaj, moramo ob list podrgniti kakršno koli temno substanco, recimo cigaretni pepel, grafitni prah, ki pade, ko šilimo svinčnik...
Mi ošilimo svinčnik in gledamo, da šilimo tako, da se špica lomi na čim manše prašne delce. Ko imamo ošiljeno dovolj, s prsti razmažemo prah po celem papirju in sporočilo smo razkrili.

SKUPINA 4:

Črnilo, ki postane vidno, ko list zmočimo

Potebujemo:
- ogledalo (ali kakšno drugo gladko stekleno površino;
- mehak navadni svinčnik;
- papir.

Obstaja kar nekaj kemijskih formul za sintetična črnila, ki se obarvajo, če list zmočimo. Mi si bomo pogledali tehniko, pri kateri ne rabiš nobenih kemikalij oziroma tehniko, pri kateri sploh ne potrebujemo črnila!

Namesto črnila bomo uporabili tako imenovano »vodno znamenje«, ki ga naredimo tako, da s pritiskanjem na papir uničimo vlakna v papirju. Ta poškodovana vlakna bomo opazili, ko bomo papir zmočili oziroma če bomo papir držali na zelo, zelo močni svetlobi.

»Vodna znamenja« uporabljajo na večini poštnih znamk in tudi na kvalitetnih papirjih, za potrditev pristnosti, kakovosti.

Pa izdelajmo naš »vodni znak«. Pomočimo list papirja v vodo. Moker papir položimo (napeto) preko gladke steklene površine (ogledalo). Čez moker list položimo suh list papirja, na katerega zapišemo naše skrivno sporočilo. Pisati moramo narahlo z mehkim svinčnikom, da ne bi po nesreči pretrgali zgornjega papirja. Ko je sporočilo zapisano, suh list odmakenemo in ga uničimo. Moker list umaknemo z ogledala in počakamo, da se posuši. Ko je list suh, se sporočila ne vidi.

Sedaj pa le zmočimo list in... sporočilo je vidno!

NENAVADNE METODE POŠILJANJA SKRIVNIH SPOROČIL

Nemogoče bi bilo opisati vse metode, ki so jih vohuni uporabljali. Veliko izmed teh metod je bilo nepraktičnih - recimo nekomu obrili glavo, mu vtetovirali sporočilo na glavo s pretvezo, da ga zdravijo za hudo boleznijo, ga pustili, da so mu zrasli lasje nazaj, nato pa ga poslali k svojim vojaškim zaveznikom in mu naročili, da pove: »Obrijte mi glavo. Sporočilo vam bo jasno.«. Ko so mu obrili glavo, so videli sporočilo in šli v napad.
Ena izmed nepraktičnih metod je bila tudi takšna, da so mačka napitali s sporočilom, ga poslali k »naslovniku«, ki je moral mačko ubiti, da se je lahko dokopal do sporočila.

Tik pred začetkom 2. svetovne vojne, so Nemci razvili in uporabljali fotografsko metodo – sporočilo so fotografirali, nato pa sliko tako pomanjšali, da ni bilo razvidno, da je to slika. Da bi bilo vse še bolj zvito, so naredili negativ slike in ga skrili v lažno sporočilo. To metodo je FBI razkrila leta 1941, ko so prestregli tako šifrirano sporočilo, ki ga je nosil nemški vohun. Ko so sliko povečali, naredili negativ, so dobili pravo skrivno sporočilo.

Metode, ki jih boste spoznali v teh urah se vam bodo morda zdele nenavadne, vendar so enostavne in jih boste res lahko uporabljali.

Dijake razporedimo v 5 skupin. Vsaki skupini razdelimo po en učni list ter vse pripomočke, ki jih pri šifriranju potrebujejo. Določimo vodje skupin in jim povemo, da bo morala po končanem delu skupina predstaviti svoje novo pridobljeno znanje ter »izdelke«. Opozorimo jih, da se držijo navodil.

SKUPINA 1:

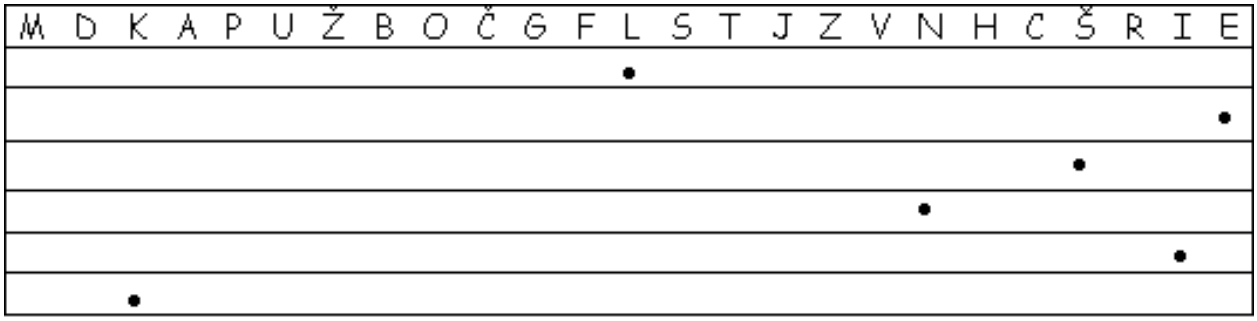
Točkovna koda

Potebujemo:
- pisala;
- škarje;
- črtasti papir.

Da bomo ta način šifriranja lahko uporabljali, si moramo mi in naši prijatelji izdelati trakec, na katerem je v poljubnem vrstnem redu zapisana celotna abeceda. Tule je primer takega traka:

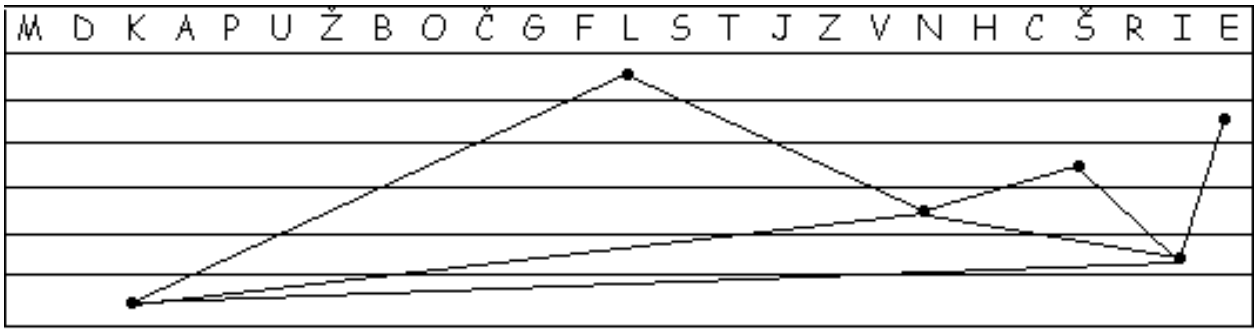
M	D	K	A	P	U	Ž	B	O	Č	G	F	L	S	T	J	Z	V	N	H	C	Š	R	I	E

Sedaj je edini stvari, ki ju še potrebujemo črtast list in svinčnik.
Da zapišemo besedo LEŠNIK, postavimo rob trakca z abecedo tik nad prvo črto na listu tako, da rob trakca in lista poravnamo. Sedaj v prvi vrsti naredimo piko pod črko L. V drugi vrsti naredimo piko tik pod črko E, v tretji pod Š in tako naprej. Vidimo, da vsaka pika natančno opisuje neko črko, vrste pa določajo vrstni red črk.
Če zapišemo LEŠNIK, zgleda naš črtast list takole (na vrhu imamo zapisan trakec):



Zapis s pikami lahko zlahka prebere vsak, ki ima šifrirni trakec. Ker pa bi bilo vsakemu napadalcu že na pogled jasno, da imajo pike nek pomen, lahko njihovo pomembnost malo zakrijemo s tem, da jih povežemo. Paziti moramo, da se povezavne črte ne sekajo, saj bi lahko njihovo presečišče kdo zamenjal za piko.

Če poljubno povežemo naše pike, sporočilo izgleda recimo takole:



Podobna različica te metode je, da namesto pikic delamo male luknjice. Luknjice so boljše, saj so manj vidne. Tako lahko na papir zapišemo lažno sporočilo, pod katerim luknjic skoraj ne bo opaziti. Tako tisti, ki bi prestregel naše sporočilo, verjetno sploh ne bi posumil, da je v sporočilu zapisano veliko več, kot lahko sam prebere.

Tako. Sedaj ste spoznali ta način šifriranja. Izdelajte dve sporočili – eno s pikicami, drugo z luknjicami in to metodo kasneje predstavite svojim sošolcem.

SKUPINA 2:

Kode z vozli

Potebujemo:
- dolgo vrvico;
- list;
- pisalo.

Da bomo ta način šifriranja lahko uporabljali, si moramo mi in naši prijatelji izdelati trakec, na katerem je v poljubnem vrstnem redu zapisana celotna abeceda. Paziti moramo, da so črke dovolj narazen. Tule je primer takega traka:

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

Sedaj je edina stvar, ki ju še potrebujemo vrvica.
Da zapišemo besedo LEŠNIK, poravnamo rob trakca z abecedo z začetkom vrvice. Sedaj naredimo vozelj tam, kjer je na trakcu črka L. Naprej nadaljujemo tako, da rob trakca poravnamo z vozljem. Nov vozelj naredimo tam, kjer se na listku nahaja črka E. Sedaj poravnamo trakec glede na vozelj, ki predstavlja E in naredimo nov vozelj tam, kjer je na traku črka Š. Postopek nadajljujemo in kot rezultat dobimo vrvico s šestimi vozlji.

Daljše sporočilo želimo zapisati, daljša je vrv. Prav zaradi dolžine vrvi verjetno nihče ne bi posumil, da je na vrvi skrito sporočilo.

Tisti, ki ima šifrirni trakec, enostavno prebere sporočilo, medtem ko imajo drugi z dešifriranjem veliko težav.

Metoda šifriranja z vozli je zelo stara metoda, ki so jo v preteklosti res veliko uporabljali.

Tako. Sedaj ste spoznali ta način šifriranja. Izdelajte sporočilo, ki bo šifrirano s kodo z vozli, in to metodo kasneje predstavite svojim sošolcem.

SKUPINA 3:

Koda z igralnimi kartami

Potebujemo:
- karte za tarok;
- svinčnik;
- radirko.

Nenavadno se zdi, da bi lahko set navadnih kart nosil skrivno sporočilo.Da lahko sporočilo zapišemo na karte moramo v rokah imeti karte za tarok ali pa kakšne druge karte, ki imajo na zadnji strani narisano kakšno podobo in lahko določiš kje je na zgornji strani zgoraj in kje spodaj.

Najprej vse karte zložimo tako, da so vse slike na zadnji strani enako obrnjene. S prijatelji se moramo vnaprej zmeniti v kakšnem vrstnem redu bomo zložili karte. Zmenimo se lahko recimo, da od vrha navzdol zlagamo najprej vse taroke od večje vrednosti k manjši, nato pa vse figure od večje vrednosti k manjši, najprej srce, nato kara, nato pik in nazadnje križ. Ko karte zložimo po vrstnem redu jih z eno roko močno stisnemo skupaj. Sporočilo sedaj zapišemo s svinčnikom na robove kupa kart. Paziti moramo, da karte res držimo tesno skupaj in pišemo z velikimi tiskanimi črkami tako, da nobena črta ni vodoravna ali horizontalna (pišemo postrani). Kot primer zapisa poglej naslednjo sliko:

Karte sedaj popolnoma premešaš, nekatere obrneš na glavo.

Tisti, ki pozna sistem zlaganja, bo brez težav prebral sporočilo. Če sporočilo zapišemo s svinčnikom, ga lahko prijatelj, ko ga prebere, izbriše z radirko in nam s svinčnikom napiše odgovor, premeša karte in nam jih pošlje nazaj.

Tako. Sedaj ste spoznali ta način šifriranja. Izdelajte sporočilo, ki bo zapisano na kartah, in to metodo kasneje predstavite svojim sošolcem.

SKUPINA 4:

Rdeče – modra koda

Potebujemo:
- rdečo barvico;
- rdeč celofan;
- modro barvico;
- papir.

V trgovinah z darili lahko skoraj povsod kupimo rdeč celofan. Uporabimo ga lahko za šifriranje sporočil, načrtov, ... A vendar – kako?

Postopek je zelo enostaven. Najprej na list papirja z rdečo barvico zapišemo lažno sporočilo. Na isti list z ostro ošpičeno modro barvico zelo rahlo zapišemo skrivno sporočilo. Paziti moramo, da pišemo res zelo rahlo in da je konica barvice vseskozi ostra. Naše skrivno sporočilo je na listu zelo težko opaziti, saj kričeče rdeče besedilo prav »sili« v oči.

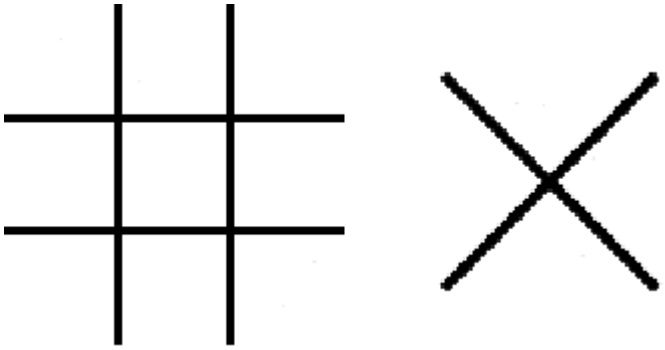
Da bi sporočilo lahko enostavno prebrali, moramo preko napisanega lista položiti rdeč celofan. Ko to storimo, rdeče (lažno) sporočilo izgine, skrivno modro sporočilo, pa se nam prikaže in ga z lahkoto preberemo.

Tako. Sedaj ste spoznali ta način šifriranja. Izdelajte sporočilo, ki bo šifrirano z rdeče-modro kodo in to metodo kasneje predstavite svojim sošolcem.

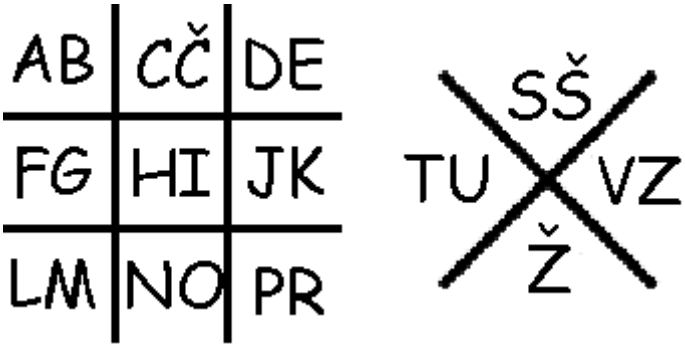
PIGPEN

Le kaj bi pomenilo takšno ime? V slovenščini bi se to glasilo »ograja za prašičke«, saj princip tega šifriranja temelji na tem, da uporabljamo neke vrste »tabelo«, v kateri so črke med sabo ločene z ograjicami, tako kot prašički v štalah. Drugo ime za takšno kodiranje je tudi Mansonovo kodiranje, saj ga je uporabljala družina Freemasonov že pred več kot sto leti. Ta način naj bi veliko uporabljali tudi med vojnami za pošiljanje skrivnih sporočil.

Pri tem načinu šifriranja moramo najprej narisati dve vzporednici in nato še dve vzporednici, ki sta na prvi dve pravokotni. Zraven narišemo velik X. Poglejmo si kar sliko:

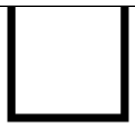


V prazne prostorčke zapišemo črke v poljubnem vrstnem redu, v vsak prazen prostor vpišemo po dve črki skupaj. Ker je v slovenski abecedi 25 črk, praznih prostorov pa imamo 13, bo v enem izmed prostorov zapisana le ena črka.
Mi si bomo pogledali primer, ko črke pišemo kar po vrsti.

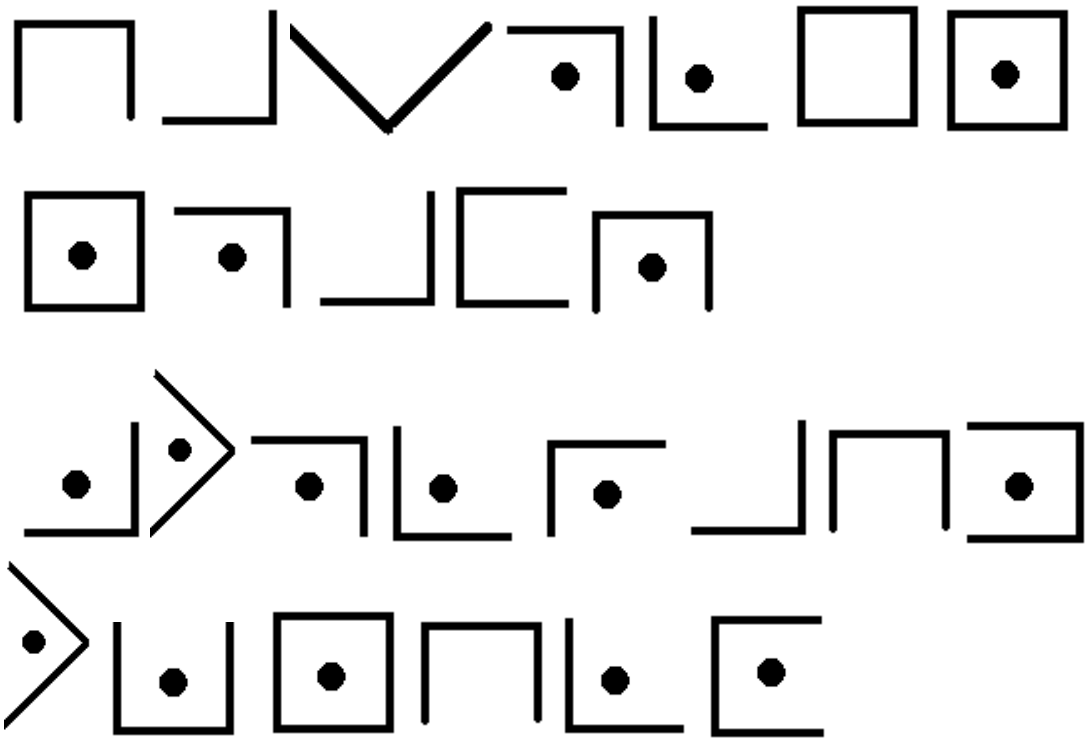


Vidimo, da so ograjice vsakega kvadratka različne. Ko bomo črko hoteli zašifrirati, bomo prerisali ograjico prostora, v katerem je zapisana. Če je črka, ki jo šifriramo prva v prostorčku, pustimo praznem proctor med ograjami, če pa je črka zapisana druga, pa v prazen proctor zapišemo piko. Šifrirajmo sedaj črki A in B:

Poglejmo si sedaj, kako zgleda celotna abeceda – da se prepričamo, da imamo za vsako črko drugačen znak.

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

Vidimo, da je vsaka črka predstavljena s svojim znakom. Sedaj je šifriranje in dešifriranje popolnoma enostavno. Ali znate prebrati spodnje besedilo?



Sedaj pa naj si dijaki v paru sestavijo svoje pigpene in si pošljejo nekaj sporočil.

ČISTO KLASIČNA KRIPTOGRAFIJA

Že pri prvi uri smo izvedeli, da nam bo izraz »čisto klasična kriptografija« pomenil način kodiranja, pri katerem za šifriranje in dešifriranje uporabimo isti ključ. Tak način šifriranja imenujemo tudi simetrična krpitografija.

1) Ena izmed najlažjih možnosti, kako skriti sporočilo je, da ga pišemo od desne proti levi in spuščamo presledke. (Pišemo »nazaj«.) Pri tem načinu skrivanja je problem, da bi napadalec lahko dokaj enostavno ugotovil, kako smo sporočilo skrili. Če kar pogledamo primer:

AŠURAMČEŠVURTEPEJADALAŠILSISA

Vsi ste takoj razbrali, da se sporočilo glasi:

A SI SLIŠALA, DA JE PETRU VŠEČ MARUŠA?

2) Druga možnost, ki pa je za napadalca težja za razbrati je obrnjeno pisanje abecede. Kaj pomeni, če rečemo, da bomo obrnjno pisali abecedo? To pomeni, da bomo namesto A pisali Ž, namesto B bomo pisali Z, namesto C pišemo V, itd. V tem primeru tisti, ki sporočilo prejme, le prepiše celotno sporočilo tako, da vsako črko zamenja z »obratno«. Zapišimo tabelo, ki jo rabimo za zamenjavo:

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

Recimo, da želimo prijatelju poslati sporočilo:

JUTRI OB OSMIH PRIDI POME

Z zamenjalno tabelo si pomagamo pri šifriranju. Vidimo, da moramo J zamenjati z N, U zamenjamo z Č, itd.
Šifrirano sporočilo se sedaj glasi:

NČDGOIZIFKOPHGOTOHIKŠ

Da bi napadalca še bolj zmedli lahko spustimo presledke, saj lahko, če sporočilo dešifriramo, presledke logično vstavimo sami. Napadalec pa se zmede, saj ne pozna dolžine besed. Če se vam ta zapis zdi nepregleden, se lahko tudi zmenite s prijatelji za sklope črk, ki jih boste pisali skupaj. Če za primer pogledamo sklope dolžine 3, se naše sporočilo glasi:

NČD GOI ZIF KOP HGO TOH IKŠ

3) Že prejšnja dva primera sta bila primera zamenjalnih tajnopisov. Zamenjalni tajnopis je tajnopis, ki ga dobimo tako, da črke zamenjamo z drugimi črkami. Ta način šifriranja so že velikokrat uporabljali v zgodovini. Če celotno abecedo zamaknemo za 3 mesta, ta način šifriranja imenujemo Cezarjevo šifriranje, saj ga je ogromno uporabljal sam Julij Cezar.

Kako pa naredimo premik za 3 mesta? V eno vrsto zapišemo celotno abecedo. Svinčnik postavimo na prvo črko (torej na A) in preštejemo naprej 3 mesta. Svinčnik imamo sedaj na črki Č, kar pomeni, da tik pod črko A v drugo vrsto zapišemo črko Č. Od Č naprej podpisujemo celotno abecedo – ko pridemo do črke Ž, nadaljujemo z A. Tako je pod črko A črka Č, pod B je D, itd.

Poglejmo si zamenjalno tabelo za Cezarjevo šifriranje:

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

Če bi na primer zašifrirali sporočilo:

SOVRAŽNE ČETE PRISPEJO V LONDON JUTRI ZJUTRAJ

Bi se to sporočilo glasilo:

USATČCRH FHZH ŠTLUŠHMS A OSRGSR MŽZTL BMŽZTČM

Oziroma, kot smo že povdarjali prej je boljše, da spuščamo presledke ali pa pišemo v sklope. Sporočilo potem zgleda tako:

USAT ČCRH FHZH ŠTLU ŠHMS AOSR GSRM ŽZTL BMŽZ TČM

Zamenjalni tajnopis se zdi dokaj varen, pa vendar to ni res. Za zamenjalni tajnopis, kjer zamikamo celotno abecedo, je le 25 možnih ključev. Tako napadalec ne bi porabil veliko časa da bi preiskusil vse in ugotovil, kateri je pravi.

4) Da bi bilo šifriranje še bolj zvito si lahko izmislimo skrivno geslo. Recimo, da smo si izbrali besedo LUNCA.

Postopek je podoben kot prej. Najprej v eno vrsto zapišemo celotno abecedo od A do Ž. Nato pod A podpišemo prvo črko gesla, v našem primeru je to L, pod B podpišemo drugo črko gesla, v našem primeru je to U, itd. Ko podpišemo celotno geslo, nadaljujemo s pisanjem abecede od A do Ž, pri pisanju pa spuščamo vse črke, ki se nahajajo v geslu. Zapišimo sedaj zamenjalno tabelo, v kateri smo uporabili geslo:

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

V primeru, da smo za geslo izbrali besedo, ki ima dve (ali več) enaki črki, prvo črko zapišemo, drugo pa spustimo. Tako bi če bi bilo geslo: ABRAHAM pod abecedo zapisali le ABRHM.

Če uporabimo zamenjalni tajnopis z uporabo gesla, bomo napadalcu povzročili kar nekaj preglavic, da se bo dokopal do sporočila.

Poglejmo si, kako bi s pomočjo zgornje tabele zapisali sporočilo:

PEPI IMA VELIKE NOGE

Šifrirano sporočilo se glasi (presledki so izpuščeni):

OBOFFJLVBIFHBKMDB

Kot smo videli, dešifriranje oziroma razbitje sporočila ni težko, če poznamo ključ.

Pojavi se nam vprašanje, kako pa bi lahko dešifrirali sporočilo, če bi bili mi tisti, ki smo sporočilo prestregli, pa ne vemo, kako so ga zakodirali (vemo pa, da je bil uporabljen nek način zamenjalnega zapisa). V tem primeru, da smo mi tisti, ki moramo dešifrirati sporočilo, nam v pomoč priskoči statistika slovenskih črk.

Tabela relativne frekvence črk in presledkov v slovenščini:

Presledek	E	A	I	O	N	R	S	L	J	T	V	D
173	89	84	74	73	57	44	43	39	37	37	33	30

K	M	P	U	Z	B	G	Č	H	Š	C	Ž	F
29	27	26	18	17	15	12	12	9	9	6	6	1

Večja je številka pod črko, večkrat se črka pojavlja v tekstih.
V primeru, da so v našem prestreženem skrivnem sporočilu presledki res presledki med besedami, nam pri ugotavljanju pomagajo še naslednji nasveti:

1) Na začetku so najpogostejše črke: N, S, K, T, J, L,
2) Najpogostejše končnice so: E, A, I, O, U, R, N,
3) V veliko pomoč ti bo, če boš ugotovil, kateri znaki zagotovo predstavljajo soglasnike in kateri samoglasnike,
4) V vsaki besedi je vsaj en samoglasnik ali samoglasniški R,
5) V vsaki besedi z dvema črkama je ena črka samoglasnik, druga pa soglanik,
6) Detektivska sreča ni nikoli odveč.

Kako bi se sedaj, ko smo zvedeli toliko zanimivih dejstev lotili dešifriranja?

Najprej moramo prešteti pogostnost vseh črk v našem besedilu. Pogostnost primerjamo s statističnimi podatki in upoštevajoč nasvete poskušamo ugotoviti, katera črka se slika v katero. Edina stvar, ki je v tem primeru nujna je, da je sporočilo, ki smo ga prestregli zelo dolgo. V krajših tekstih statistični podatki ne ustrezajo nujno frekvencam črk v sporočilu.

Poglejmo si dešifriranje kar na konkretnem primeru.

Recimo, da smo prejeli tajnopis:

BRVUHAČRVVRRUMTŽAHEVRKAHLČROAHBČMOHUHKŠHŠRBMSMŠTHČRTZ
ŠZTRBČZTŽRKHRVŠHČMAMOHBZZČAZJRŠTRJHTRERTRVRPKMRFUMLZČAZ
ŠVREMLMTFHŠHSŠTRKMSZUHKŠHČHŠZRVŠLZUDSMLHTČZKRBČZKTZEMCŠ
ZRUMJMTZUHASMČŠHRVČHČSHVHVRBČHFVHTRČMOHŽZEMLHČRUHKMŠE
RTRSMŽZVHEHLREMLARTŽZLZKMČZERUHEČZUZIRTZUŠZBČHZKMRVBRVU
HAČRVBČZŽRTHRFBČZTŽRKHOHSMZKMFHOTMLHTRVOHŽZŠHFHTBRVDUH
AČRVDŽZOTMSUHAČRVUDJUDJMŠERTRBRVUHAČRVSMBHUZŽZŠRUHTŽZČ
MUŽHBMFHUHKŠHVREMKFUMVRTLADOHKMŽHSMIRTZFLADORURČAMURC
ČRARVZGVRURUHAČRVZERURŽARSHČMTSRČZBZIRTRŽBRBHUZBHČZRVT
ZUKMSMBRVUHAČRVFHOTMLHTŠHČMAMOHZLVSRPŽHVHSSMIRTCMČHŠZL
HTMKSMFHKMTŠHFHČRFRFČMOVSMVZAZŠZRVEŽRČRFVHCZITSMVRURDB
ČREHDEHDEHDSHEHDEHDSMŽZVZERTZKMRVŽZPRČMTFUHAČRVZUŽBDV
HBŽAZČRBHUZSMIRTUHSPMVKAVŠZLMAVRČRFHPRŽVRUZOMTIRČRŽARUR
ADOZBŽZLHAOHSMUZAHTEMLVZZŽZURVSHČRBHUZURAŽARLMVHUMČZ

Želimo ga dešifrirati, to pomeni, da želimo najti ključ, s katerim se bomo dokopali do čistopisa. Naša prva naloga je, da preštejemo, kolikokrat se vsaka črka pojavi v našem tekstu.

Črka	Št.	Črka	Št.	Črka	Št.	Črka	Št.
R	97	U	43	Š	25	D	15
H	86	T	41	E	23	I	7
Z	65	A	32	K	22	P	5
M	61	B	27	L	19	J	5
V	47	Ž	26	F	17	C	4
Č	47	S	26	O	16	G	1

Črka N se v tajnopisu sploh ne pojavi.

Tabela relativne frekvence črk:

E	A	I	O	N	R	S	L	J	T	V	D
89	84	74	73	57	44	43	39	37	37	33	30

K	M	P	U	Z	B	G	Č	H	Š	C	Ž	F
29	27	2	1	17	15	12	1	9	9	6	6	1

		6	8				2					

Sedaj ugibamo kakšen bi lahko bil zamik. Najbolj pogosti črki sta E in A, zato sklepamo, da bi črki E in A lahko bili zamenjani z R ali H, saj sta ti dve črki najbolj pogosti in se nato zgodi kar velik preskok. Zapišimo obe tabeli, če bi bil se A slikal v H ali pa v R.

Tabela 1 (A→H):

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

Tabela 2 (A→R):

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

Sedaj pogledamo najmanj pogoste črke. Po statistiki je najmanj pogosto uporabljena črka slovenske abecede črka F, v našem primeru, bi se F lahko slikala v G ali N. Opazimo, da se v tabeli 1 F slika ravno v N, kot smo predpostavili. Posumimo, da smo morda našli pravo tabelo za dešifriranje. Pa poskusimo s tabelo 1. Sedaj delamo obraten postopek kot pri šifriranju. Če tabelo zaradi lažjega dela malce preoblikujemo (zamenjamo vrstici), sobimo novo zamenjalno tabelo za dešifriranje.

Dešifrirna tabela:

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

Ko to storimo, se nam prikaže tekst:

SINMARTINNIIMELPRAVNIČRADTIGRASTEGAMAČKAKISEJEKLATILOKOLISTOL
PIČAINKATEREGASOOTROCIKLICALIVILINIHČEIZMEDOTROKNIVEDELZAKAJK
LIČEJOMAČKATAKOINKDOMUJEDALTOČISTOČLOVEŠKOIMECELOMARJETKAI
NTATJANANISTAZNALITEGAPOVEDATIMAČEKVILIJEPONAVADIVEDRILPODOČ
ETOVIMAVTOMOBILOMKOSTAOČEINSINMARTINSTOPILAIZSTOLPIČAGAJEOČ
EZAGLEDALINGAPOKAZALSINUMARTINUPOGLEJMARTINMUCMUCEKVILISIN
MARTINJESAMOPOKIMALPOTEMPASEZAMAČKANIVEČZMENILDRUGAČEPAJE
BILOZDRUGIMITREMIŠTIRINOŽNIMIMARTINOVIMIPRIJATELJITOSOBILIPSISAM
OSATOINLOMČEJESINMARTINZAGLEDALKATEREGAODNJIHPANAJJEBILŠETAK
ODALEČJEZAČELKAZATIZIZTEGNJENOROKOINVPITIZNAŠOBLJENIMIUSTIVAU
VAUVAUJAVAUVAUJEPONOVILOČEINPOHITELZMARTINOMPSUNASPROTISAM
OJEBILMAJHENČRNKODERNITIZAHIPNIMOGELBITIPRIMIRUGOSPODARGAJEM
ORALVEDNOOPOMINJATISAMOMIRPRIDENAMESTO

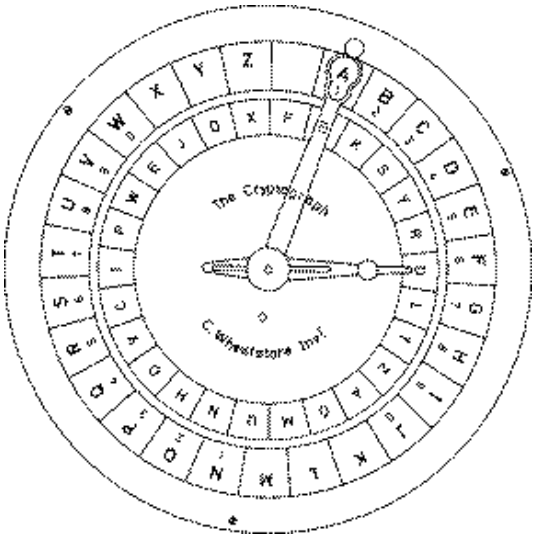
V tekstu sicer ni presledkov, a lahko sami brez problemov postavimo presledke in ločila. Dobimo:

SIN MARTIN NI IMEL PRAV NIČ RAD TIGRASTEGA MAČKA, KI SE JE KLATIL OKOLI STOLPIČA IN KATEREGA SO OTROCI KLICALI VILI. NIHČE IZMED OTROK NI VEDEL, ZAKAJ KLIČEJO MAČKA TAKO IN KDO MU JE DAL TO ČISTO ČLOVEŠKO IME. CELO MARJETKA IN TATJANA NISTA ZNALI TEGA POVEDATI. MAČEK VILI JE PO NAVADI VEDRIL POD OČETOVIM AVTOMOBILOM. KO STA OČE IN SIN MARTIN STOPILA IZ STOLPIČA, GA JE OČE ZAGLEDAL IN GA POKAZAL SINU MARTINU: POGLEJ, MARTIN, MUC, MUCEK VILI! SIN MARTIN JE SAMO POKIMAL, POTEM PA SE ZA MAČKA NI VEČ ZMENIL.
DRUGAČE PA JE BILO Z DRUGIMI TREMI ŠTIRINOŽNIMI MARTINOVIMI PRIJATELJI. TO SO BILI PSI SAMO, SATO IN LOM. ČE JE SIN MARTIN ZAGLEDAL KATEREGA OD NJIH, PA NAJ JE BIL ŠE TAKO DALEČ, JE ZAČEL KAZATI Z IZTEGNJENO ROKO IN VPITI Z NAŠOBLJENIMI USTI: VAU, VAU, VAU! JA, VAU, VAU, JE PONOVIL OČE IN POHITEL Z MARTINOM PSU NASPROTI. SAMO JE BIL MAJHEN ČRN KODER. NITI ZA HIP NI MOGEL BITI PRI MIRU. GOSPODAR GA JE MORALVEDNO OPOMINJATI: SAMO, MIR, PRIDE, NA MESTO!

(tekst: Smiljan Rozman, Sin Martin, Mladinjska knjiga, 1974)

Opazimo, da smo z malo detektivske sreče hitro prišli do čistopisa. Če nam to ne bi uspelo tako hitro, bi primerjali še pogostost ostalih črk.

KRIPTOGRAFSKI PRSTAN



Potebujemo:
- karton;
- pisalo;
- sponko za papir;
- škarje;
- ravnilo.

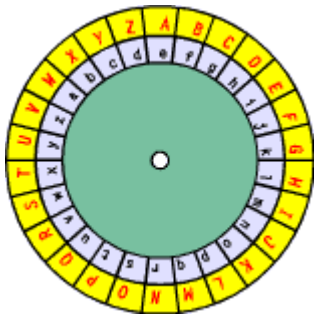
Za šifriranje z zamenjalnim zapisom, lahko uporabljamo tudi kriptografski prstan. Z njim lahko šifriramo le tako, da celotno abecedo zamaknemo za poljubno število mest. Jasno je torej, da lahko s tem prstanom šifriramo tudi tako, kot je šifriral Julij Cezar (za 3 mesta).

Najprej iz lepenke izrežemo en večji in en manjši krog (recimo r=4cm, R=5cm). V središčih obeh krogov naredimo luknjici. (Dijaki naj delajo samostojno ali v parih.)

Ker slovenska abeceda vsebuje 25 črk, moramo oba kroga razdeliti na 25 delov. To pomeni, da moramo kot 360^0 razdeliti na 25 delov, torej vsak del meri $14{,}4^0$. Na večji krog približno narišemo te stopinje in se potrudimo, da je krog razdeljen na 25 približno enakih delov. Ko imamo ta krog razdeljen na 25 delov,
Položimo najn manjši krog tako, da se središči krogov prekrivata. Črte, ki nam zaznamujejo dele večjega kroga povežemo s središčem večjega kroga in s tem razdelimo tudi manjši krog na 25 delov.

Celotno abecedo sedaj zapišemo na rob krogov tako, da vsako črko pišemo v svoj prostor. Sedaj moramo le povezati oba kroga s sponko za papir, ki jo damo čez središči krogov. In s tem je naš kriptografski prstan narejen. Ali je že jasno kako se z njim kodira?

Tule imamo sliko kriptografskega prstana z angleško abecedo:



Kolikšen premik imamo narejen na sliki? (4)

Recimo, da želimo naše sporočilo šifrirati po Cezarjevi metodi. Svinčnik položimo na črko A in preštejemo za 3 mesta naprej. Pridemo do črke Č, zato moramo spodnji krog zavrteti tako, da bo črka Č tik pod črko A. Sedaj smo s kriptografskim prstanom zelo hitro prišli do zamenjalne tabele, ki smo jo prejšnjo uro celo zapisali »na roko«.

Zdaj pa naj si dijaki sami izmislijo sporočilo ali pa izberejo poljuben odlomek iz kakšne knjige in ga s pomočjo kriptografskega prstana zašifrirajo. Zašifrirano sporočilo naj nato podajo sosedu, ki ga s pomočjo svojega kriptografskega prstana odšifrira.

MARY, QUEEN OF SCOTS

Kot smo pri prejšnjih urah že povedali, simetrična kriptografija ni zelo varna. Najbolj dramatičen prikaz tega, kaj se lahko zgodi, je zgodba Mary, kraljice Škotske.

Slika 1: Mary, Škotska kraljica

Mary je bila obtožena, grozila ji je smrt, njeno življenje pa je temeljilo na tem, ali bodo dešifrirali njena sporočila ali ne. Bitka za njeno življenje je potekala med Maryinimi kriptografi in razbijalci kod (imenujemo jih tudi kriptoanalisti) kraljice Elizabete, Mary je bila ena izmed najpomembnejših oseb 16. stoletja – bila je kraljica Škotske, kraljica Francije in je predstavljala grožnjo kraljici Elizabeti, kraljici Anglije. Kljub mogočni osebnosti, kakršna je Mary bila, je o njeni usodi odločal listek papirja... Pa si poglejmo njeno zgodbo.

Kralj Henrik VIII, kralj Škotske, je z napadom svoje armade na Anglijo, želel odvzeti krono kralju Jamesu V, kralju Anglije. Henrikove čete so bile poražene, odvzem krone ni uspel. Zaradi poraza je kralj Henrik VIII precej oslabel, tako fizično kot psihično. Dva tedna po izgubljeni bitki, se mu je rodila hči Mary, vendar ga tudi ta srečni dogodek ni mogel pozdraviti. Le teden po Maryinem rojstvu, v starosti 30 let, je kralj Henrik VIII umrl. Majcena Mary je tako postala kraljica Škotske. Devetega septembra 1543 so Mary kronali za kraljico. Ob njeni strani so bili trije ljudje, ki so v njenem imenu zaprisegli in prejeli krono. Ker je bila Mary tako majhna, si je Anglija lahko za nekaj časa odpočila od škotskih invazij. Angleži so želeli doseči spravo med deželama in so določili, da naj bi se Mary poročila z Edvardom, angleškim princem. Kot resno gesto je angleški kralj James V spustil nekaj čet, ki so jih zasegli ob škotskem zadnjem napadu.

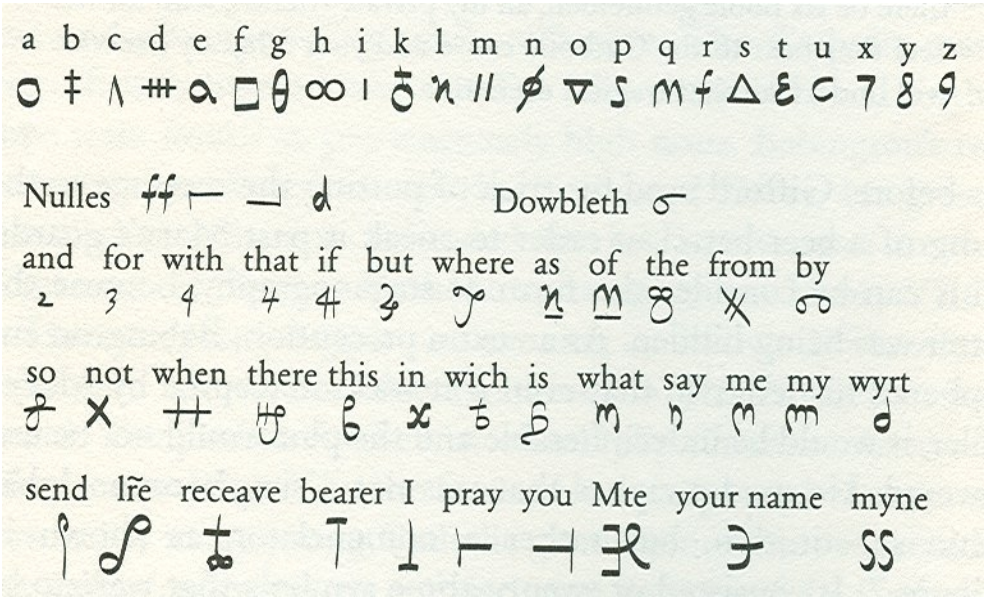
Kljub ponudbi je škotsko sodišče določilo drugače. Mary je bilo določeno, da se poroči s Francisom, princem Francije. Ker sta bili tako Škotska kot Francija katoliški državi, naj bi njuna združitev pomenila večjo moč. Čeprav sta bila Francis in Mary še otroka, je Francija obljubila Škotski pomoč ob morebitnih angleških napadih.

Angleži so po tem še povečali napade na Škotsko. Kljub škotski zvezi s Francijo, so Angleži močno napadali. Tudi ko je angleški kralj James V umrl, je njegov sim Edvard nadaljeval napade. Angleži so zmagovali, pustošili po Škotski, razmere so postale nevzdržne, zato so Mary v starosti 6 let prepeljali v Francijo. Tam je živela lepo, razkošno življenje, vzgojili so ji ljubezen do njenega bodočega ženina. Ko je bila Mary stara 16 let, sta se s Franciscom poročila. Po tem svečanem dogodku so pričakovali, da se bo Mary veličastno vrnila na Škotsko. Pa temu ni bilo tako. Francis je bil bolan, infekcija ušesa se je tako razbolela, da je že v letu po poroki umrl. Mary je bila stara 17 let in je že bila vdova. Od te točke naprej, je šlo njeno življenje samo še navzdol.

Mary se je spet poročila. V drugem zakonu je bila s svojim bratrancem. V tem zakonu se jima je rodil sin James VI, ki je bil edina svetla stran tega zakona. Njen mož je bil namreč barbar, nasilnež.

Leta 1567 so škotski protestantje postali nezadovoljni s svojo katoliško kraljico. Zato so Mary zaprli in jo prisilili, da se je odrekla kroni in jo prepustila sinu Jamesu VI, ki je bil takrat star 14 mesecev. Cilj te predaje krone je bil v tem, da je zastopstvo sina dobil Maryin polbrat (dokler James ne dopolni 18 let). Čez eno leto je Mary prebegnila iz zapora in zbrala vojsko 6000 mož in z njimi še zadnjič poskušala osvojiti nazaj krono. Ni ji uspelo. Razočarana Mary ni zbežala v Francijo, kakor bi predvidevali, pač pa v Anglijo, ker je upala, da ji bo sestrična, kraljica Elizabeta I. nudila zatočišče. Vendar se je Mary krepko zmotila. Elizabeta je Mary »ponudila« le zapor. Javni razlog za zaprtje je bil v povezavi s smrtjo njenega moža – njenega bratranca. Resnični razlog, da so Mary zaprli pa je bil v tem, da je Mary predstavljala grožnjo Elizabeti, saj so imeli katoliški angleži Mary za svojo pravo kraljico. Po vseh pravilih Mary ni imela pravice zahtevati krone, vendar katoliki Elizabete niso priznavali, saj je bila otrok iz drugega zakona kralja Henrya VII. Problem je bil v tem, da se je kralj od prve žene ločil in zato katoliki drugega zakona sploh niso priznavali. Veliko se je govorilo o Maryinem zaprtju, o njeni lepoti,govoru, sposobnostih... Pa vendar je po nekaj letih Mary utonila v pozabo.

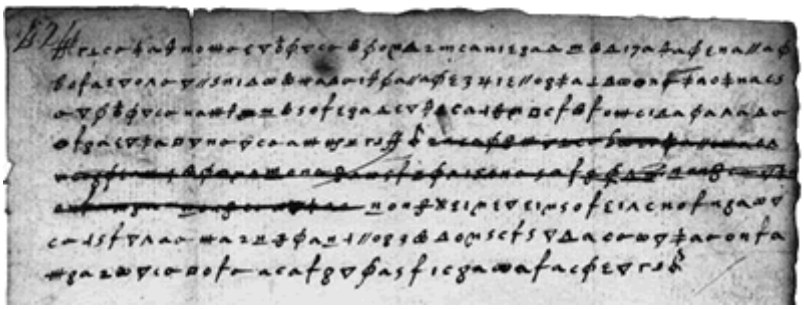
Leta 1586, po 18 letih v zaporu, je Mary izgubila vse privilegije. Upala je na združitev s sinom, vendar je sin ni maral, saj so ga vzgajali Maryini nasprotniki, ki so mu dejali, da je njegova mati ubila očeta, da bi se lahko poročila s svojim ljubimcem. Mary je bila izolirana od vseh, stike je imela le z ječarji. Zdelo se je, da je Mary izgubila vse upanje. Sklop okoliščin pa ji je omogočil, da je 6. januarja 1586 prejela pisma njenih občudovalcev, ljudi, ki so jo podpirali.Duhovnik Gilbert Gifford je bil katoliški anglež, ki je bil željan služiti Mary in ji je pretihotapil vsa pisma v njeno celico in iz nje. Gilfford je imel svoj način skrivanja teh pisem – šel je do lokalnega pivovarja in mu je le ta sporočilo skril v sod. Ko je sod prispel na dvor, so ga Maryine služabnice odprle, poiskale sporočilo in ga izročile Mary. Obraten postopek je veljej za pošiljanje sporočil nazaj.



Slika 2: Maryino šifriranje

Med vsem tem dogajanjem je v Londonu vrelo. Mary sicer ni vedela, a nekaj katoliških angležev je pripravljalo načrt, s katerim naj bi osvobodili kraljico Mary, usmrtili kraljico Elizabeto in organizirali upor. Vse te zadeve pa niso želeli začeti dokler jim Mary ne bi dala svojega blagoslova. Vse zgornje so najprej šifrirali na poseben način, nato pa to pismo poslali Mary. Za šifriranje niso uporabljali enostavnega monoabecednega šifriranja ampak kombinacijo šifriranja črk in besed, v sporočilo pa so pisali tudi prazne znake, to je znake brez pomena. Njihovo šifriranje je bilo sestavljeno iz 23 črk angleške abecede (manjkale so črke J, V in W), 35 simbolov, ki so predstavljali besede ter 4 prazne znake. Posebej so imeli določen tudi znak, ki je pomenil, da se črka, ki stoji za njim podvoji.

Za prenos teh pisem do Mary je na pomoč priskočil Gilfford, ki je to počel že prej. Ker je bil Gillford duhovnik, ni bilo čisto nič sumljivo, ko je venomer odhajal in prihajal. V tistem času pa je Anglija začela vršiti velik pritisk nad katoliki. Čeprav je bil Gillford Maryin sel že od začetka, je nekje vmes postal dvojni agent. Vsa pisma, ki jih je nesel Mary ali pa od Mary odnašal, je vmes nesel njenim nasprotnikom, da so pisma prepisali. Pisma, ki so bila velikega pomena, so bila zašifrirana. Da bi nasprotniki sploh spoznali vsebino pisma, so zaposlili Thomasa Phelipesa, ki je bil izredno dober v dešifriranju in kriptoanalizi nasploh. Res ni trajalo dolgo, ko je Phelipes uspel razkriti način šifriranja. Šifrirni ključ je našel še pred pismom z željo po blagoslovu. To pismo so takoj dešifrirali. Ko je Mary prejela pismo, so nasprotniki samo še čakali, kdaj bo Mary odgovorila. Mary je kmalu odgovorila, dala svoj blagoslov, ni pa vedela, da je s tem podpisala svojo smrtno obsodbo. Imeli so dovolj dokazov, da jo usmrtijo. Kljub temu, da so nasprotniki imeli dovolj dokazov za usmrtitev kraljice Mary, jim to ni bilo dovolj. Želeli so uničiti celotno zavezo, ki je načrtovala upor in usmrtitev kraljice Elizabete. Pheliepes je kot strokovnjak v kriptografiji ter kot človek, ki naj bi znal ponarejati katerokoli pisavo, ponaredil pismo, ki so ga nato izročili Mary. V pismu je Mary poziva, da izda imena vseh sodelujočih, pod pretvezo, da bodo lahko zdaj, v finalnih uricah pred upoorom, lažje kontaktirali med sabo, tako da bodo jasno vedeli, komu lahko zaupajo.



Slika 3: ponarejeno pismo

Mary je pasti nasedla ter v naslednjem pismu izdala imena vseh njenih zaveznikov. V treh dneh so ujeli vse njene zaveznike, tudi tiste, ki so se trudili bežati.

Dokazov je bilo več kot preveč, zato je kraljica Elizabeta ukazala usmrtiti kraljico Mary in vse njene privržence.

Kljub revmi in izmučenosti, je Mary na svojo usmrtitev prišla zravnao, ponosno. Njena zadnja misel pred giljotino je bila: »Moj konec je moj začetek.«.

VIGENERJEV TAJNOPIS

Problem zamenjalnih tajnopisov je, da se vsaka črka preslika v natančno določeno črko. Ta princip šifriranja je monoabeceden, zato se lahko napadalci dokaj hitro dokopljejo do naše skrivnosti. Najbolj drastičen prikaz zlomljivosti zamenjalnega tajnopisa je bila usmrtitev kraljice Mary.

Kriptografi so vedeli, da na njihovih ramenih leži dolžnost, da izumijo nov način kodiranja, ki bo precej težaven za dešifrirati. Nekje okrog leta 1460 je Leon Battista Alberti (rojen 1404) napisal esej o šifriranju, za katerega je verjel, da je popolnoma nov na področju kriptografije. To šifriranje ni bilo več monoabecedno! Alberti je predlagal, da bi za šifriranje uporabili dva ali več monobecednih šifriranj in ta šifriranja med sabo menjavali. S tem bi napadalca zmedli, saj ni nujno, da bi se ista črka preslikala v natančno določeno črko – lahko bi bila zamenjanja z več različnimi črkami.

Primer:

Original	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž
Menjava 1	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M
Menjava 2	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T

Poskusimo sedaj s pomočjo zgornje tabele zašifrirati besedo OKNO. Prvo črko besede zamenjamo pa Menjavi1 (M1), drugo po Menjavi2 (M2), tretjo po Menjavi1, itd. Vsako črko na lihem mestu torej šifriramo z Menjavo1, vsako črko na sodem mestu pa z Menjavo2.

Prva črka naše besede je O in ta se preslika po M1 v črko D. Druga čkrka K se po M2 preslika v G, tretja črka N gre v Č po M1, četrta črka, ki je O, pa se preslika po M2 v K. Beseda

OKNO

je zašifrirana v

DGČK.

Prvo kar opazimo je, da sta v besedi OKNO dve črki enaki, medtem ko se v šifrirani besedi nobena izmed črk ne ponovi, kljub temu pa črki D in K v šifrirani besedi predstavljata isto črko! In ta lastnost je bistvena pri zavajanju napadalca.

Največja prednost Albertijevega sistema je v tem, da se črke prvotnega sporočila ne preslikajo nujno v iste črke. Tako lahko imajo iste črke v šifriranem sporočilu popolnoma drugačen pomen.
Bleise de Vigenere, francoski diplomat, rojen leta 1523 je spoznal Albertijeve eseje v starosti 26 let. Takrat je bil Vigenere poslan na dveletno misijo v Rim, vendar se v eseje takrat ni poglobil, saj je bilo njegovo začetno ukvarjanje s kriptografijo bolj praktično in povezano z njegovo službo.

Šele v starosti 39 let je Vigenere prihranil dovolj denarja, da je opustil svojo kariero in se osredotočil na študij. Šele takrat je podrobno preučil Albertijeve eseje in jih spremenil v uporaben in močan način šifriranja, ki ga sedaj imenujamo po njem – Vigenerjev tajnopis.

Mogočnost Viegenerjevega tajnopisa je v tem, da ne uporablja le enega ključa, temveč menjava med 25 različnimi ključi.

Prvi korak za Vigenerjevo kodiranje je, da zapišemo tako imenovan Vigenerjev kvadrat:

Osnova	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž
M1	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A
M2	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B
M3	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C
M4	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č
M5	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D
M6	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E
M7	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F
M8	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G
M9	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H
M10	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I
M11	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J
M12	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K
M13	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L
M14	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M
M15	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N
M16	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O
M17	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P
M18	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R
M19	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S
M20	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š
M21	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T
M22	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U
M23	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V
M24	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z
M25	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž

V Vigenerjevem kadratu je v prvi vrsti zapisana celotna abeceda, ki ji sledi 25 monoabecednih ključev, vsak je za eno mesto premaknjen naprej od prejšnjega. M1 predstavlja zamik celotne abecede za eno mesto, M2 je premik abecede za 2 mesti, M3 predstavlja Cezarjevo kodiranje, ...

Vidimo, da se recimo črka A z vsakim ključem preslika v različno črko. Z M4 se sprelika v U, z M21 pa v D. Če bi uporabili le enega izmed monoabecednih ključev v Vigenerjevem kvadratu, bi to bil navaden zamenjalni, monoabecedni tajnopis.

Vigenerjev tajnopis temelji na tem, da pri šifriranju uporabljamo več vrstic Vigenerjevega kvadrata. Zašifrirali bi lahko recimo prvo črko po M4, drugo pa M21, tretjo po M13 in tako dalje. Če bi sedaj tako sporočilo poslali, bi moral prejemnik vedeti, v kakšnem vrstnem redu smo šifrirali. Poznati mora torej sistem in vrstni red izbora šifrirnih vrstic.

Če je bil izbor naključen, bomo imeli že veliko težav pri sporočanju načina šifriranja, zato si vedno pomagamo s ključno besedo – geslom. Pa si

izberimo, da bo naše geslo besedica KRALJ. Poskusimo sedaj zašifrirati besedilo:

POŠLJITE VSE ČETE V NAPAD

Najprej moramo naše geslo zapisati pod zapisano sporočilo. Geslo ponovno zapisujemo, dokler ne pridemo do konca sporočila. Kar poglejmo:

P	O	Š	L	J	I	T	E		V	S	E		Č	E	T	E		V		N	A	P	A	D
K	R	A	L	J	K	R	A		L	J	K		R	A	L	J		K		R	A	L	J	K

Zdaj kodiranje poteka povsem enostavno. Črko kodiramo po tistem ključu, katerega vrstica se začne s črko, ki je zapisana pod črko našega sporočila. Tako bomo prvo črko sporočila kodirali z vrstico, ki se začne z K, to je M11. Tako črko P zašifriramo v C. Drugo črko O šifriramo po vrstici, ki se začne z R, to je po M17, in s tem O zašifriramo v G. Tretjo črko, to je Š, šifriramo po M25, tako Š kar ostane Š. Četrto črko L šifriramo po M12 in postane Ž, peto črko J pa po M10. J postane T. Postopek nadaljujemo.

Pomagamo si z Vigenerjevim kvadratom, kjer si označimo vrstice, ki se začenjajo s črkami gesla.

Osnova	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž
M1	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A
M2	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B
M3	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C
M4	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č
M5	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D
M6	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E
M7	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F
M8	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G
M9	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H
M10	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I
M11	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J
M12	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K
M13	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L
M14	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M
M15	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N
M16	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O
M17	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P
M18	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R
M19	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S
M20	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š
M21	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T
M22	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U
M23	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V
M24	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z
M25	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž

Sporočilo

POŠLJITE VSE ČETE V NAPAD

se sedaj glasi

CGŠŽTTLEIČPTEGOHFAČJO.

Znova smo pri šifriranju spustili presledke.
Ko naslovnik prejmo naše sporočilo, mora le poznati geslo, pa lahko sporočilo zelo hitro prebere. Če pa pride sporočilo v napačne roke, pa je zelo verjetno, da tudi po daljšem času ukvarjanja s sporočilom ne bo imel niti najmanjše ideje, kaj v sporočilu piše.

Dejstvo je, da je sporočilo kratko in da obstaja ogromno možnih ključev – nasprotnik nikakor ne more poskustiti z vsemi besedami, ki so v slovarju, nikakor ne more razbrati našega sporočila. Edina možnost, da ga dešifrirajo je, da se dokopljejo do gesla (ali ga komu ukradejo ali pa koga prisilijo, da izda geslo).

Poliabeceden Vigenerjev tajnopis je bil dolgo časa najboljša možnost, da si skrivnem sporočilu zagotovil varen prenos. Uporabljali so ga za prenos pomembnih poslovnih sporočil, ki so jih prenašali po telefonih, saj tudi če je kdo prestregel sporočilo si s črkami, ki so jih govorili ni mogel prav nič pomagati. Napadalci so bili pred Vigenerjevim tajnopisom nemočni.

Dolgo časa so imeli Vigenerjev tajnopis za nezlomljiv in je ta tajnopis zaradi tega dobil ime »la chiffre indechiffrable« - ključ, ki se ne da razbiti.

G. BABAGE IN RAZBITJE VIEGENERJEVEGA TAJNOPISA

Najpomembnejši mož za kriptografijo 19. stoletja je bil Charles Babbage, ekscentričen anglež, ki je bil znan po veliko izumih – precej tudi glede izumov v zvezi z računalniki.

Charles Babbage se je rodil leta 1791 kot sin Benjamina Babbagea, bogatega londonskega bankirja. Charles Babbage se je brez očetovega privoljenja poročil in s tem izgubil pravico do družinskega denarja. Kljub temu je imel Charles dovolj denarja, da je bil popolnoma finančno neodvisen. Živel je življenje nadobudnega študenta, svoj nos je vtaknil v skoraj vsako stvar, ki je šla mimo njega. V tem zanimanju je izumil veliko stvari – ti vključujejo merilec hitrosti in »preganjalec krav«, to je takšna naprava, ki so jo lokomotive pritrdile spredaj in je lokomtiva s tem lahko varno spravila živino s tračnic.

Če govorimo o znanstvenih dosežkih, je bil Charles Babbage prvi, ki je povezal širino drevesa in vreme v letu, ter prvi, ki je s proučevanjem starih dreves določil podnebne razmere v preteklosti. Zanimalo ga je skorajda vse – tudi statistika in tu je Charles izumil smrtnostne tabele, ki jih kot osnovno zadevo še vedno ogromno uporabljajo.

Preobrat v Babbageovi karieri je nastopil leta 1821, torej ko je bil star 30 let. Takrat sta z astronomom Johnom Herschelom preučevala matematične tabele, ki so jih uporabljali za osnovne izračune v astronomiji, strojništvu in navigaciji. Charles in John sta bila šokirana nad številom napak, ki sta jih našla v tabelah. V eni izmed tabel, v tabeli za navtične izračune, sta našla več kot tisoč napak! Vedelo se je, da se je veliko nesreč, brodolomov in strojnih katastrof zgodilo prav zaradi napak v tabelah.

Vse tabele so bile preračunane ročno oziroma »peš«. Vse napake so bile le plod človeške zmotljivosti. Babbage je nekoč izjavil, da želi, da bi vse tabele zgorele ob udarcu strele. Babbage je dobil idejo, da bi izumil stroj, ki bi znal računati in bi napravil manj napak kot človek. Tako je leta 1823 naredil načrt za izdelavo »Difference Engin No. 1«, čudovito računalo, sestavljeno iz 25000 majhnih delčkov. Načrt je podprla vlada in Babbagea podprla z vladnim denarjem. Pa vendar je bil Charles Babbage dober izumitelj, a slab v izvedbi izumov. Tako je po desetih letih ukvarjanja z »Difference Engin-om No. 1« opustil ta projekt. Kljub opustitvi projekta, pa je v vmesnem času naredil nov načrt, za novo računalo, ki ga je poimenoval kar »Difference Engine No. 2«.
Ko je Babbage opustil projekt in se lotil novega, mu vlada ni želela dati nobenega denarja več, saj je že za prvi projekt porabil toliko denarja, da bi z njim lahko naredil kar nekaj bojnih ladij. Zaradi pomanjkanja denarja Babbageu ni uspelo sestaviti tudi drugega stroja. Šele stoletje kasneje, med Drugo svetovno vojno, so zgradili prvo elektronsko verzijo

Babbageovega računala. Tako je Babbage veliko prispeval k začetku moderne tehnologije.

V svojem življenju pa je Babbage pustil ogromen pečat tudi kriptografiji, predvsem v razbijanju sporočil. Charles Babbage je razbil Vigenerjev tajnopis, za katerega so do tedaj mislili, da se ga ne da razbiti. Babbage se je že kot majhen deček zanimal za skrivna sporočila, velikokrat se prav zaradi tega padel v težave. Starejši fantje so napisali skrivna sporočila, Babbage pa je sporočilo takoj, ko se je dokopal do nekaj besed, dešifrilal. Prav zaradi njegovega hitrega dešifriranja so ga starejši fantje večkrat pretepli. Niso razumeli, da je bila njihova neumnost, neznanje in nespretnost kriva temu, da je Charles tako hitro dešifriral. Kljub vsem prejetim brcam in udarcem, pa Babbage ni izgubil zanimanja za razbijanje tajnopisov. Kljub temu, da je večina ljudi že obupala nad razbitjem Vigenerjevega tajnopisa, Babbage ni izgubil zanimanja. Vseskozi ga je navduševala izmenjava pisem z Johnom Hallom Brookom, pisala sta si o problemih razbitja ter o Vigenerjevem tajnopisu nasploh.

Leta 1854 je Thwaites, zobozdravnik iz Bristola trdil, da je odkril nov način kodiranja, ki pa je bil identičen Vigenerjevemu tajnopisu. Thwaitsov članek je bil objavljen v neki reviji, v katero je tudi Babbage poslal pismo in objasnil situacijo. Thwaites se kljub Babbagevemu pismu ni opravičil, ne kesal, ampak Babbagea izzval, če zna razbiti »njegov« tajnopis. Ali se je dal ta tajnopis razbiti ali ne, je bilo popolnoma vseeno v razpravi ali je ta tajnopis nov ali ne. Kljub temu pa je celoten potek dogodkov Babbagea izzval, spodbudil k iskanju principa, kako razbiti Vigenerjev tajnopis. In Babbageu je uspelo! Razbil je Thwaitesovo nalogo in s tem tudi ugotovil princip razbijanja Vigenerjevega tajnopisa.

Pri razbijanju Vigenerjevega tajnopisa nam statistika črk ne pomaga, saj se iste črke ne zakodirajo v različne in zato lahko tudi iste črke v tajnopisu predstavljajo različne črke v čistopisu (prvotnem sporočilu). Problem je v poliabecednem šifriranju.

Če bi imeli za geslo besedo KRALJ, se lahko recimo črka E slika v P, V, E, R ali O (glej Vigenerjev kvadrat):

Osnova	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž
M1	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A
M2	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B
M3	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C
M4	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č
M5	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D
M6	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E
M7	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F
M8	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G
M9	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H
M10	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I
M11	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J
M12	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K
M13	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L
M14	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M
M15	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N
M16	P	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O
M17	R	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P
M18	S	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R
M19	Š	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S
M20	T	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š
M21	U	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T
M22	V	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U
M23	Z	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V
M24	Ž	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z
M25	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž

Podobno kot črke se tudi celotne besede slikajo v različne sklope. Besedica DA se lahko preslika v OR, UA, DL ali PJ, odvisno je seveda od pozicije, na katerih te črke stojijo. Ravno te stvari povzročajo največje težave pri razbijanju tajnopisa. V slovenščini pride do še večjih težav, saj nimamo nobene besede dolžine dve ali tri, ki bi se non-stop ponavljala. V angleščini je taka besedica THE. In prav ta besedica je ključnega pomena.

Razbitje Vigenerjevega tajnopisa si bomo pogledali na angleškem tekstu, kjer si bomo precej pomagali z besedivo THE.

Ker bomo imeli sedaj šifriran angleški tekst, moramo zapisati nov Vigenerjev kvadrat:

	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
M1	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	A
M2	C	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
M3	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
M4	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	D
M5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
M6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
M7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
M8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
M9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
M10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
M11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
M13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
M14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
M15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
M16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
M17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
M18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
M19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
M20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
M21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
M22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
M23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
M24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
M25	Z	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
M26	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

Ker bomo delali z angleškim tekstom, si izberimo tudi angleško geslo namesto KRALJ bomo sedaj uporabljali KING, kar je angleški prevod besedice kralj.

Poglejmo si najprej šifriranje angleškega stavka (s pomočjo zgornjega kvadrata):

Čistopis	T	H	E	S	U	N	A	N	D	T	H	E	M	A	N	O	N	T	H	E	M	O	O	N
Geslo	k	i	n	g	k	i	n	g	k	i	n	g	k	i	n	g	k	i	n	g	k	i	n	g
Tajnopis	D	P	R	Y	E	V	N	T	N	B	U	K	W	I	A	O	X	B	U	K	W	W	B	T

Vidimo, da se besedica THE zašifrira enkrat v DPR, dvakrat pa v BUK. Razlog v ponovitvi je v tem, da je kjučna beseda dolžine 4, besedici THE, ki se zašifrirata isto, pa sta 8 polj narazen. Število 8, pa je deljivo s 4. (Pod THE imamo obakrat zapisano ing.)

Ponovitve sklopov črk, ki temeljijo predvsem na besedici THE, je glavni ključ pri dešifriranju Vigenerjevega tajnopisa. Pa poskusimo dešifrirati naslednji tekst:

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

Videli smo, da se besedica THE kljub ključni besedi kar nekajkrat zašifrira v isti sklop črk.

Iščemo zaporedja črk, ki se ponavljajo. Recimo sklop črk E-F-I-Q se pojavi v prvi vrsti tajnopisa in se znova ponovi po 95-tih črkah. Vemo, da bi bilo dešifriranje enostavno, če bi poznali ključno besedo. Naš cilj je najprej ugotoviti ključno besedo, s katero je bil tekst zašifriran.

Poglejmo si še en sklop črk, ki se ponovi W-C-X-Y-M. Ta sklop se znova ponovi po 20-črkah. Tako vemo, da je dolžina ključa število, ki deli 20, torej 1, 2, 4, 5, 10 ali pa 20.

Poiščemo še več sklopov črk, ki se ponavljajo in zapišemo tabelo. V to tabelo vpišemo možne dolžine ključev, zavržemo pa možnost, da bi bil ključ dolžine 1, saj bi imeli potem opravka z navadnim monoabecednim kodiranjem.

Pa zapišimo tabelo:

sklop	ponovitev	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
E-F-I-Q	95				✓														✓	
P-S-D-L-P	5				✓															
W-C-X-Y-M	20	✓		✓	✓					✓										✓
E-T-R-L	120	✓	✓	✓	✓	✓		✓		✓		✓			✓					✓

Opazimo, da je edina skupna možnost za dolžino ključa število 5. Ko to ugotovimo, moramo vse črke tajnopisa porazdeliti v 5 skupin (ker ima ključna beseda 5 črk):

- V prvo skupino damo 1., 6., 11., ... črko (črke na 5n+1 mestu, n=aravno število ali nič).
- V drugo skupino damo 2., 7., 12., ... črko (črke na 5n+2 mestu, n=naravno število ali nič).
- V tretjo skupino damo 3., 8., 13., ... črko (črke na 5n+3 mestu, n=naravno število ali nič).
- V četrto skupino damo 4., 9., 14., ... črko (črke na 5n+4 mestu, n=naravno število ali nič).
- V peto skupino damo 5., 10., 15., ... črko (črke na 5n mestu, n=naravno število).

Sedaj nam črke v posameznih skupinah predstavljajo enostavno monoabecedno kodiranje, ki ga rešimo s pomočjo statistike angleških črk (podobno kot smo prej to storili s slovenskimi črkami). Tega sedaj ne bomo počeli, saj je bil smisel vsega tega pokazati način, s katerim se da vigenerjev tajnopis dešifrirati. Z zgornjim smo videli, da Vigenerjev način kodiranja ni nezlomljiv, še več – precej hitro ga lahko rešimo.

S pomočjo statistike bi ugotovili, da je prva skupina črk zašifrirana z vrstico Vigenerjevega kvadrata, ki se začne s črko E, druga z vrstico, ki se začne s črko M, tretja z I, četrta z L, peta je zakodirana z vrstico, ki se začne z Y. Ključno besedo sedaj dobimo tako, da preberemo črke eno za drugo in dobimo, da je geslo, s katerim je bil čistopis zakodiran EMILY.

Če s pomočjo tega gesla sedaj dešifriramo tajnopis, se čistopis glasi:

Sit thee down, and have no shame,
Cheek by jowl, and knee by knee:
What care I for any name?
What for order or degree?

Let me screw thee up a peg:
Let me loose thy tounge with wine:
Callest thou that thing a leg?
Which is thinnest? Thine or mine?

Thou shalt not be saved by works:
Thou hast been a sinner too:
Ruined trunks on withered forks,
Empty scarecrows, I and you!
Fill the cup, and fill the can:
Have a rouse before the morn:
Every moment dies a man,
Every moment one is born.

Videli smo, da je bila zašifriran tekst pesmica. Napisal jo je Arthur, Lord Tennyson, naslov pesmice pa je »The Vision of Sin«.

RSA

S to uro zapuščamo območje enostavno zlomljivih, zgodovinskih tajnopisov. Sedaj bo prej nepojmlivo postalo resnično. Kodirajne RSA se imenuje po svojih izumiteljih **R**ivest-u, **S**hamir-ju in **A**delman-u.

RSA kodiranje je asimetrično kodiranje, to pomeni, da imamo dva ključa – privatni in javni ključ. Javni ključ je ključ, ki je dostopen vsem, ponavadi ga celo objavijo na internetu, medtem ko ima privatni ključ v lasti samo ena oseba. Da bi nam bil princip RSA čim bolj jasen ga bomo spoznali na podoben način, kot so njegovi izumitelji prišli do ideje o novem načinu kodiranja.

1. KORAK: Ideja o potenciranju ostankov.

V monoabecednem kodiranju smo z uporabo tabel nezavedno uporabljali tudi seštevanje ostankov po modulu 25. Kako?
Najprej moramo črkam slovenske abecede prirediti številko – to je kar število mesta, na katerem črka stoji.

	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž
Št.	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24

Poglejmo si kar Cezarjevo kodiranje – to je zamik za 3 mesta. Po postopku, ki smo ga uporabljali prej, bi postavili svinčnik na črko A in prešteli 3 naprej. Tako bi prišli na črko Č. Pod črko A bi tako zapisali črko Č, nato pa nadaljevali s podpisovanjem črk, ki sledijo črki Č.

	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž
+3	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž	A	B	C

Ker ima slovenska abeceda 25 črk, bomo vse gledali po modulu 25. Če črki pripada število x, moramo, ko kodiramo gledati, čemu je enako $x+3$ po modulu 25. Rezultat, ki ga dobimo je neko število med 0 in 24, za katerega pa vemo, katero črko predstavlja.
Poglejmo recimo črko A. Črki A pripada število 1. Če prištejemo število 3, dobimo 4, kar pa je kongurentno 4 po modulu 25. Črki Z pripada število 23. Če temu prištejemo 3 dobimo 26, kar pa je enako 1 po modulu 25.

	A	B	C	Č	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	Š	T	U	V	Z	Ž
Št	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
+3	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27
mod	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	0	1	2

Ker je ta ideja dobra, so razmišljali, kaj vse bi se še dalo početi z moduli. Prišli so na idejo, da bi uporabili latsnost potenciranja pri modulih, torej, da je če je

$$a \equiv b \pmod{c}$$, potem je $a^n \equiv b^n \pmod{c}$.

Kaj bi se zgodilo, če bi uporabili eksponent 3?

$$A^3 = 0^3 \equiv 0 \pmod{25} \qquad A$$
$$B^3 = 1^3 \equiv 1 \pmod{25} \qquad B$$
$$C^3 = 2^3 \equiv 8 \pmod{25} \qquad H$$
$$\check{C}^3 = 3^3 = 27 \equiv 2 \pmod{25} \qquad C$$
$$D^3 = 4^3 = 64 \equiv 14 \pmod{25} \qquad N$$
$$E^3 = 5^3 = 125 \equiv 0 \pmod{25} \qquad A$$

M

Vidimo, da se različne črke s takšnim šifriranjem lahko zakodirajo v iste črke, kar smo videli da je bistvena težava za napadalce, ki hočejo odšifrirati naše sporočilo. Rivest, Adelman in Shamir so morali sedaj odgovoriti na naslednji dve vprašanji:

1) Kako izbrati eksponent, da zagotovljeno nedovoumno kodiranje in pravilno odkodiranje?
2) Glede na izbor kodirnega eksponenta, kakšen mora biti odkodirni eksponent, da bomo dobili res nedvoumno pravilnen čistopis?

Tukaj so se poskušali spomniti vseh izrekov, ki vključujejo potenciranje in module, in jih v matematiki poznamo.

2. KORAK: Uporaba Eulerjevega izreka.

Na zgornje vprašanje so hitro našli odgovor. Eden izmed glavnih izrekov Teorije števil, ene najstarejših vej matematike, je Eulerjev izrek. Ta pravi: Naj bo *p* praštevilo in *a* poljubno število, različno od *p*. Potem velja:

$$a^{p-1} \equiv 1 \pmod{p}.$$

Poglejmo si primer, ko je p=5:

$$2^4 = 16 \equiv 1 \pmod{5},$$
$$3^4 = 81 \equiv 1 \pmod{5},$$
$$4^4 = 256 \equiv 1 \pmod{5},$$
$$6^4 = 1296 \equiv 1 \pmod{5},$$

M

Za uporabo tega izreka pri RSA kodiranju, bomo uporabili posplošitev (kasneje bomo razložili zakaj):

$$a^{(p-1)(q-1)} \equiv 1 \pmod{p \cdot q}.$$

Poglejmo si primer, ko je p=3 in q=5. Potem je $a^8 \equiv 1 \pmod{15}$, za vsak a, ki nima nobenih skupnih deliteljev s $p \cdot q$. Torej je največji skupni delitelj števil a in $p \cdot q$ enak 1.
Vidimo, da je:

$$2^8 = 256 \equiv 1 \pmod{15},$$
$$4^8 = 65536 \equiv 1 \pmod{15},$$
$$7^8 = 5764801 \equiv 1 \pmod{15},$$

M

3. KORAK: Kako nam Eulerjev izrek omogoča izdelavo novega načina kodiranja.

Sedaj je konstrukcija novega načina kodiranja dokaj enostavna. Poglejmo.

Modul *m*, po katerem bomo gledali ostanke, mora biti večji od števila uporabljenih črk. Število *m* mora biti produkt dveh praštevil. Recimo, da izberemo

$$m=33=3\cdot 11.$$

Po Eulerjevem izreku je torej

$$a^{20} = 1 \pmod{33}$$

in zato velja tudi, da je

$$a^{21} \equiv a \pmod{33}.$$

In to je tisto, kar so kriptografi želeli! Predstavljajte si, da imamo neko število *a* (ki predstavlja neko črko), in ga nato potenciramo na 21. Pri tem dobimo kot rezultat tega potenciranja originalno število *a*, samo v primeru, da zadevo gledamo po modulu 33.
Če bi lahko ta princip razdelili na dve fazi – kodiranje in odkodiranje, bi bili na konju. Pa vendar – ali lahko ti dve fazi dobimo?

Seveda lahko. Saj poznamo pravilo potenciranja potenc – če potenco potenciramo, osnovo prepišemo, eksponenta pa zmnožimo:

$$a^{m\cdot n} = (a^m)^n.$$

V našem primeru je torej

$$a^{21} = (a^3)^7.$$

Tako bi lahko izbrali, da bo šifrirni ključ enak 3 in bi tako vsako črko kodirali tako, da bi uporabili eksponent 3:

$$C \equiv P^3 \pmod{33}.$$

Da bi zadevo dešifrirali, uporabimo dešifrirni ključ, to je 7 in se vse skupaj odkodira:

$$C^7 \equiv (P^3)^7 \pmod{33}$$

$$C^7 \equiv P^{21} \pmod{33}$$

$$C^7 \equiv P \pmod{33}.$$

Odlično! Sedaj smo prišli tako daleč, da že lahko opišemo kodirno in dekodirno funkcijo RSA-ja.

Pošiljatelj zakodira čistopis P tako, da uporabi javni ključ (e,m) takole:

$$C \equiv P^e \pmod{m}.$$

Prejemnik dešifrira tajnopis C z uporabo svojega privatnega ključa (d,m) na sledeč način:

$$P \equiv C^d \pmod{m}.$$

Prejemnik na ta način iz tajnopisa enostavno pride do čistopisa z uporabo svojega privatnega ključa, kar pomeni, da lahko sporočilo prebere samo on, ki ima v lasti ta ključ. In to je ravno tisto, kar smo želeli dobiti. Pa vendar – ali bi zaupali kodiranju z *m*=33 za plačilo s kreditno kartico prek interneta? Podobno kot Cezarjev tajnopis je tudi tu problem, da zadeva

sicer dela, pa vendar je vse to daleč od tega, da bi bil prenos varen (za zdaj).

Recimo, da želimo po e-pošti poslati našo osebno davčno napoved našemu finančnemu svetovalcu. V tem primeru najprej poiščem javni ključ (e=3, m=33) in z njim zakodiram mojo napoved. Ta javni ključ je zadostna informacija za nepridiprave, ki želijo vpogled v našo napoved.

Pa poglejmo zakaj: Nepridiprav ve, da je $m=33=11\cdot 3=p\cdot q$,
tako da s tem pozna tudi kodirno enačbo

$$a^{21} \equiv a \pmod{33}.$$

Zdaj brez problemov zračuna eksponent:

$$21=(p-1)(q-1)+1=(11-1)(3-1)+1=10\cdot 2+1.$$

Ker je $21=e\cdot d$ in ker nepridiprav ve, da je e=3, ve, da je dešifrirni ključ enak d=7. Tako lahko nepridiprav enostavno pride do naših podatkov in uživa v branju naše napovedi. Ne glede na to, kdo je ta, ki napada naš tajnopis, ali je to FBI, CIA ali pa samo naš sosed, želimo mi pred vsemi te podatke skriti – ostati morajo le med nami in našim finančnim svetovalcem.

Sklep: Postopek dela, pa vendar je daleč od tega, da bi bil varen. Zato pojdimo naprej in poglejmo, kaj je treba narediti, da je RSA varen način prenosa podatkov.

4. KORAK: RSA: Uporaba »enosmernih« funkcij naredi RSA varen

Razlog za varnost je v protislovju s tem kar smo do sedaj povedali: »Kljub temu, da vsi na svetu poznajo modul m in kodirni ključ e, nihče ne more uganiti dešifrirnega ključa d.«

Ta skoraj neverjetna trditev je resnična zaradi uporabe tako imenovanih »enosmernih« funkcij: »Kljub temu, da je množenje dveh poljubno velikih števil enostavno narejeno, je nasprotje temu – iskanje faktorjev poljubno velikega števila nemogoče.«

To pomeni, da vsek računalnik zelo hitro izračuna, da je

14661447539859647450758235565692138592940747688613829394033737162285790173007438 3
*
75927691025434806960037534144529320936577608016494583610079969972686437092104055 1

=

11132098587920845829411563690317448763481537837636606896195796281815330141176469 48
37737625838893687610402628112788959622813543185395045279971949456605272989305033

Če imamo podan zgornje število (produkt), je nemogoče odkriti, kateri števili sta bili zmnoženi. To je enostaven primer »enosmerne« funkcije, ki prikaže, zakaj je RSA varen. Potencilna nevarnost: če bo kdo odkril algoritem za ugotavljanje faktorjev ogromnih števil, bo RSA zlomljen, ne bo več varen.

Kljub temu pa noben matematik doslej še ni uspel rešiti ta stoletja star problem. Če bi združili moči super računalnikov (recimo močne računalnike FBI in NSA), bi lahko faktorizirali 120-mestna števila. Zatorej, da bi zagotovili popolno varnost RSA-ja, moramo izbrati dovolj velik ključ (to je dovolj velik modul *m*). Sedaj za varno kodiranje z RSA uporabljajo vsaj 200-mestna števila. Tako zagotovijo popolno varnost.

5. KORAK: Zagotovitev pravilnega dešifrirnega procesa.

Kodiranje ima smisel le v primeru, če imamo zagotovljeno varno in nedvoumno dekodiranje – torej da kot rezultat dešifriranja res dobimo pravi čistopis. Matematika je znanost, ki nam bo pomagala doseči cilj. V tem, to je v zadnjem koraku, bomo naredili matematičen dokaz, da je dešifrirna funkcija za RSA nedvoumna.

Začnimo že z zgoraj omenjenim Eulerjevim izrekom:

$$a^{(p-1)(q-1)} \equiv 1 \pmod{p \cdot q}, \quad (1)$$

kjer je *a* celo število, ki nima nobenega skupnega delitelja s $p \cdot q$ (razen 1). Sledi

$$a^{(p-1)(q-1)+1} \equiv a^{e \cdot d} \equiv a \pmod{p \cdot q}. \quad (2)$$

Pomembno: RSA dela pravilno le v primeru, če iz $a^{e \cdot d}$ dobimo *a* za VSAK *a*, saj bo le v tem primeru prejemnik dobil dešifrirano pravilno črko čistopisa. Pa vendar Eulerjev izrek ne velja za vse *a*-je – ne velja za tiste *a*, ki imajo kakšne skupne delitelje s $p \cdot q$. Zato moramo pokazati, da enačba (2) velja tudi v primeru, če ima število *a* s številom $p \cdot q$ kakšne skupne delitelje.
Pa dokažimo zgornje: Naj bo število *a* večkratnik števila *p* ali pa večkratnik števila *q*. Če bi bil *a* večkratnik števila $p \cdot q$, bi bil najmanj velikosti $p \cdot q$, kar pa pri RSA ni možno. Zato lahko brez škode za splošnost predpostavimo, da je *a* večkratnik števila *p*. To lahko zapišemo kot:

$$a \equiv 0 \pmod{p}. \quad (3)$$

Zato je za vsako potenco števila *a*:

$$a^{e \cdot d} \equiv 0 \pmod{p}. \quad (4)$$

Odštejmo sedaj enačbo (3) od enačbe (4). Dobimo:

$$a^{e \cdot d} - a \equiv 0 \pmod{p} \quad (5)$$

za vsako pozitivno celo število *a.*

S tem smo že skoraj prišli do naše željene enačbe (2), razlika je le v tem, da gledamo sedaj po modulu *p*, želeli pa bi gledati po modulu $p \cdot q$. Sedaj preoblikujmo sedaj enačbo (5).

Ker je *a* večkratnik števila *p*, ne more biti večkratnik števila *q*, saj je *q* praštevilo. Torej *a* in *q* nimata skupnih deliteljev. Sedaj uporabimo Eulerjev izrek z uporabo modula *p* (ta poseben primer se imenuje Mali Fermajev izrek). Zapišemo lahko:

$$a^{q-1} \equiv 1 \pmod{q}.$$

Potencirajmo to enačbo na potenco *p-1*. Dobimo:

$$\left(a^{(q-1)}\right)^{p-1} \equiv 1 \pmod{q}.$$

Enačbo sedaj pomnožimo z *a*:

$$a^{(q-1)(p-1)+1} \equiv a \pmod{q}.$$

To pa je tisto, kar smo potrebovali, saj so bili ključi izbrani tako, da je

$$e \cdot d = (p-1)(q-1)+1.$$

Tako smo pokazali, da je

$$a^{e \cdot d} \equiv a \pmod{q} \quad (6)$$

za vsak *a*.

Preostane nam le še, da logično združimo enačbe (2),(5) in (6). Enačba (5) nam pove, da *p* deli $a^{e \cdot d}$*-a.* Podobno nam enačba (6) pove, da tudi *q* deli $a^{e \cdot d}$*-a*.

Ker sta *p* in *q* različni praštevili, ki delita isto število, mora tudi njun produkt *p*·*q* deliti $a^{e \cdot d}$*-a..* To lahko zapišemo kot

$$a^{e \cdot d} - a \equiv 0 \pmod{p \cdot q}$$

oziroma

$$a^{e \cdot d} \equiv a \pmod{p \cdot q}.$$

S tem smo doakzali enačbo (2), torej smo pokazali, da je nedvoumno dekodiranje pri RSA-ju zagotovljeno.

RSA-digitalni podpis

Prejšnjo uro smo spoznali kako RSA kriptosistem deluje, kako ga lahko uporabimo, da naše skrite informacije ostanejo skrite. Kako bi sedaj z RSA zagotovili avtentičnost? Če plačujemo prek Klika, moramo ob logiranju na internetno stran vnesti skrivno geslo. Uporabniško ime in geslo nas pri prijavi na računalnik identificira kot uporabnika, za katerega računalnik pričakuje, da smo. Podobno, če pošiljamo po e-pošti pomembne dokumente, bi morda želeli zagotoviti prejemniku, da smo res mi poslali to sporočilo, torej bi radi zagotovili avtentičnost sporočila. Tako so vsa pomembna sporočila podpisana tako, da zagotavljajo avtentičnost pošiljatelja. Takemu podpisu pravimo digitalni podpis.

Pri tej ideji o podpisovanju dokumentov z digitalnim podpisom lahko enostavno uporabimo RSA način kodiranja. Kako deluje digitalni podpis? Enostavno, če smo razumeli princip, kako RSA deluje.

Na internetu objavimo naš javni kluč (e,m). Dostop do tega ključa ima vsak. Vsako sporočilo P nato zakodiramo z našim privatnim ključem (d,m).

$$S \equiv P^d \pmod{m}.$$

Prejemnik, ki naše sporočilo dobi, sedaj odklene z javno znanim ključem (e,m).

$$P \equiv S^e \pmod{m}.$$

Ker ključ (d,m) poznam le jaz, mu tega sporočila ni mogel poslati nihče drug, kot jaz osebno. Tako je lahko pošiljatelj prepričan o avtentičnosti sporočila.

Poglejmo si še primer, ko želi Ana poslati Borisu zašifrirano sporočilo, zraven ga pa želi tudi podpisati. Kaj naj stori? Recimo, da je P čistopis, ki ga želi Ana zakodirati, podpisati in poslati Borisu. Najprej Ana zakodira sporočilo P z Borisovim javnim ključem e_B:

$$C \equiv P^{e_B} \pmod{m}.$$

Nato Ana podpiše to sporočilo s svojim privatnim ključem d_A:

$$S \equiv C^{d_A} \pmod{m}.$$

To sporočilo S Ana nato pošlje Borisu. Ko Boris prejme sporočilo mora storiti najprej preveriti, da mu je to sporočilo res polala Ana. To preveri tako, da na sporočilu uporabi Anin javni ključ e_A:

$$S^{e_A} \equiv \left(C^{d_A}\right)^{e_A} \pmod{m} \equiv C \pmod{m}.$$

Nato, ko je preveril avtentičnost sporočila, odkodira sporočilo s svojim privatnim ključem d_B:

$$C^{d_B} \equiv \left(P^{e_B}\right)^{d_B} \pmod{m} \equiv P \pmod{m}.$$

Če sta Ana in Boris izbrala svoje ključe dovolj velike, imata oba dve zagotovitvi – da je zagotovo Ana tista, ki je poslala sporočilo in da nihče, razen Borisa, ne more prebrati sporočila.

LITERATURA

Knjigi:

- Martin Gardner: CODES, CHIPERS AND SECRET WRITING, Dover Publications, Inc., New York
- Simon Singh: THE CODE BOOK- HOW TO MAKE IT, BREAK IT, HACK IT, CRACK IT, Delacorte Press, 2003

Internetne povezave:

Zgodovina: http://www.saintanns.k12.ny.us/depart/math/Gena/ccw.html

Enigma: http://www.ugrad.cs.jhu.edu/~russell/classes/enigma/

Navajo: http://www.history.navy.mil/faqs/faq61-2.htm
http://bingaman.senate.gov/code_talkers/

Zimmerman: http://www.lib.byu.edu/~rdh/wwi/1917/zimmerman.html

Nevidno črnilo:
http://www.iit.edu/~smile/ch9602.html
http://starryskies.com/articles/dln/6-01/invisible.html
http://www.inmotion-pcs.com/amass/theboss/invisink.htm

Vigener: http://www.trincoll.edu/depts/cpsc/cryptography/vigenere.html
http://mathematica.ludibunda.ch/crypto3.html

Ceasar: http://www.trincoll.edu/depts/cpsc/cryptography/caesar.html
http://www.trincoll.edu/depts/cpsc/cryptography/substitution.html

Rsa: http://www.trincoll.edu/depts/cpsc/cryptography/rsa.html
http://www.antilles.k12.vi.us/math/cryptotut/rsa1.htm

Klasika: http://williamstallings.com/Extras/Security-Notes/lectures/classical.html
http://www.ciphersbyritter.com/LEARNING.HTM
http://www.murky.org/cryptography/classical/jefferson.shtml
http://www3.brinkster.com/Redline/crypt.asp
http://mathematica.ludibunda.ch/crypto.html
http://library.thinkquest.org/27158/concept1_1.html
http://nrich.maths.org/public/viewer.php?
obj_id=2197&part=index&refpage=freesearch.php
http://www.simonsingh.net/file/633.doc

Mary: http://www.marie-stuart.co.uk/