Šifrovaná komunikácia

Vladimír Boža

Obsah

0. Úvod

Výmenu informácií medzi dvoma alebo viacerými jedincami nazývame komunikácia. Je to jedna z vecí, bez ktorej by ľudstvo nemohlo existovať. To je hlavný dôvod, prečo ma táto téma zaujala.

Komunikácia môže prebiehať rôznymi spôsobmi. Prenos informácií sa dá rozdeliť na priamy a nepriamy. Priamym spôsobom rozumieme taký spôsob, keď sú dotyční jedinci v priamom kontakte, čiže napr. reč, posunky. Pri nepriamom spôsobe sú naopak dotyční jedinci od seba vzdialení, touto formou komunikácie je napr. listová pošta, telefón. Kým priama komunikácia väčšinou vyžaduje len prítomnosť komunikujúcich jedincov, nepriama komunikácia vyžaduje aj rôzne ďalšie prostriedky, pričom konštrukcia niektorých z nich môže vyžadovať vysoké technické znalosti. Preto je táto forma komunikácie podľa mňa oveľa zaujímavejšia.

Avšak nepriama komunikácia má jednu značnú nevýhodu. Je nemožné zaručiť, aby sa k prenášanej správe nedostal niekto nevhodný. Preto bolo nutné zaviesť šifrovanú komunikáciu. S tým súvisel aj vznik dvoch vedných odborov, ktorými sú:
kryptografia – veda, ktorá sa zaoberá tvorbou šifier
kryptoanalýza – veda, ktorá sa zaoberá lúštením - prelamovaním šifier
Obidve vedy sú zahrnuté vo vednom odbore zvanom kryptológia.

Mojím cieľom je prejsť historickým vývojom šifier a šifrovacích systémov a poukázať na situácie, kedy prelomenie/neprelomenie šifry zmenilo osudy niektorých ľudí. Taktiež, hlavne pri najmodernejších šifrách, chcem ukázať využitie matematiky v praxi.

1. Šifrovanie pred vynálezom rádiovej komunikácie

Aj v dobách dávno minulých bolo nutné prenášať správy tak, aby ich mohli prečítať len povolané osoby. Dôležité to bolo hlavne v stave vojny, kedy získaná informácia mohla znamenať aj víťazstvo nad nepriateľom. Na zašifrovanie textu sa zvyčajne používali dva postupy, a to:

Transpozícia znamená zamenenie poradia písmen podľa určitého postupu. Je to vlastne prešmyčka. Dá sa napríklad aplikovať tak, že sa vezme nejaký pruh látky (prípadne opasok) a namotá sa okolo tyče so správnym priemerom. Potom sa naň napíše správa. Po odmotaní opasku dostaneme nič nehovoriacu postupnosť písmen. V histórii sa tento postup použil napríklad v Grécko-Perzskej vojne. V roku 404 p. n. l. dorazil k spartskému kráľovi ťažko ranený posol, ktorý ako jediný prežil cestu z Perzie. Podal kráľovi svoj opasok. Kráľ použil tyč správneho priemeru a z odkazu sa dozvedel, že sa perzský kráľ chystá na neho zaútočiť. Vďaka tejto správe mohol pripraviť obranu a útok odraziť.

Substitúcia znamená nahradenie určitého písmená iným znakom podľa vopred určeného postupu, napr. miesto znakov klasickej abecedy použijeme iné znaky. Najznámejší používateľ tohto typu šifry je rímsky cisár Julius Caesar. Používal posun v abecede o 3 znaky (miesto A písal D, miesto B písal E, ..., miesto Z písal C). Preto sa tento typ šifry nazýva Caesarova šifra.
Typická substitučná šifra je obvykle ťažko prelomiteľná bez ďalších znalostí, pretože sa nemusí obmedziť len na posun znakov v abecede, ale môže miesto znakov používať ľubovoľné symboly. Tým sa zväčšuje počet možnosti nutný na odskúšanie na viac než 400 000 000 000 000 000 000 000 000.

S vývojom šifier sa samozrejme vyvíjali aj postupy používané pri ich prelamovaní. Kryptoanalýza sa vyvíjala najmä v islamských krajinách. Arabskí učenci si všimli, že nie každé písmeno sa v texte vyskytuje rovnaký počet krát. V deviatom storočí Abú al-Kindí zistil, že toto je možné využiť pri prelamovaní substitučných šifier.

Kým v arabských krajinách v 9.-12. storočí prebiehalo obdobie prudkého rozvoja vzdelanosti, Európa uviazla v temnote. Arabi mali už rozvinutú kryptoanalýzu, v Európe bola len kryptografia na začiatku svojho rozmachu. Najskôr sa používala iba v kláštoroch. Prvú európsku knihu o kryptografii napísal v 13. storočí anglický františkán a polyhistor Roger Bacon. Opisuje sedem metód ako uchovávať tajomstvo správ. V 14. storočí sa už kryptografia používala bežne. Začal aj rozvoj kryptoanalýzy. Nie je známe, či v Európe sa kryptoanalýza rozvinula nezávisle od arabských objavov, alebo bola prenesená z arabského sveta. Vďaka tomu boli vedci, ktorí sa zaoberali kryptografiou, nútení vymýšľať dokonalejšie šifry. Zvyčajne však aj tieto vylepšené šifry boli ľahko rozlúštiteľné.

Najzdrvujúcejšie sa prevaha kryptoanalytikov nad kryptografmi prejavila v prípade štótskej kráľovnej Márie Stuartovej. Bola väznená Alžbetou I. a so svojimi spolubojovníkmi komunikovala pomocou šifrovaných správ, ktoré využívali substitučnú šifru. Tieto správy však boli zadržané a rozlúštené. Ich obsah, ktorý hovoril o pláne zvrhnúť Alžbetu, jasne podpísal rozsudok smrti pre Máriu. Je to typický príklad toho, že slabé šifrovanie je horšie ako žiadne. Mária a jej spolubojovníci naivne verili tomu, že nikto iný nečíta ich komunikáciu. Dali tak nepriateľom do rúk veľmi citlivé informácie.

Túto situáciu zmenil až Blaise de Vigenére, francúzsky diplomat narodený v roku 1523. Princíp jeho novej šifry je pomerne jednoduchý. Správa sa šifruje pomocou kľúča. Napríklad, keď máme kľúč ABC, tak sa každé tretie písmeno v správe posúva o jeden znak, ich susedia sa posúvajú o dva znaky a ostatné písmená o tri znaky. V praxi to vyzerá takto:

Kľúč:	ABCABCABCAB
Správa:	CHODTEDOMOV
Zašifrovaná správa:	DJREVHEQPPX

Tento systém bol spočiatku odolný voči kryptoanalýze využívajúcej frekvenciu jednotlivých písmen v jazyku. Postupom času však aj táto šifra bola prelomená. Pri lúštení sa využívalo v podstate to isté, čo pri bežnej substitučnej šifre. Odlišnosť bola v nutnosti zistiť komplikovaným spôsobom dĺžku kľúča. Potom sa už šifra zmenila na niekoľko Caesarovych šifier, ktorých postup riešenia bol známy.

2. Šifrovanie koncom 19. storočia a počas 1. svetovej vojny

Po rozlúštení Vigenérovej šifry bolo nutné vymyslieť novú, ktorá by uspokojila vojenské potreby a hlavne umožnila bezpečné využívanie telegrafu. Zvýšenie záujmu o kryptografiu spôsobil aj vynález rádiovej komunikácie. Tento vynález mal jednu obrovskú výhodu – nebolo nutné mať elektrické vedenie medzi odosielateľom a príjemcom. Avšak s tým bola spojená aj obrovská nevýhoda. Správu mohol zachytiť nielen príjemca, ale úplne hocikto. Preto vo vojenskej sfére bolo spoľahlivé šifrovanie nutnosťou.

Do popredia sa táto činnosť dostala hlavne počas 1. svetovej vojny. Je zjavné, že rozlúštenie nepriateľskej šifry prináša obrovskú taktickú výhodu. Väčšina šifier používaných počas 1. svetovej vojny bola rozlúštená. Jednou z najznámejších je nemecká šifra ADFGVX. Bola zavedená 5. marca 1918, krátko pred veľkou nemeckou ofenzívou, ktorá začala 21. marca. Táto šifra využíva substitúciu a následnú transpozíciu. Najprv je potrebné vyplniť mriežku veľkosti 6x6 pomocou písmen A až Z a číslic 0 až 9. Každý riadok a stĺpec je identifikovaný pomocou písmen A, D, F, G, V, X. Príjemca aj odosielateľ sa musia dohodnúť na rovnakej mriežke. Povedzme, že je vyplnená napr. takto:

	A	**D**	**F**	**G**	**V**	**X**
A	8	p	3	d	1	n
D	l	t	4	o	a	h
F	7	k	b	c	5	z
G	j	u	6	w	g	m
V	x	s	v	i	r	2
X	9	e	y	0	f	q

V prvej časti šifrovania sa každé písmeno nahradí pomocou písmen označujúcich jeho riadok a stĺpec. Napríklad p sa nahradí ako AD, o sa nahradí ako DG. Vcelku to vyzerá takto:

Správa: a t t a c k a t 1 0 p m

Zašifrovaný text: DVDDDDDVFGFDDVDDAVXGADGX

Potom nasleduje transpozícia zašifrovaného textu. Najprv sa príjemca a odosielateľ musia dohodnúť na kľúčovom slove – v našom prípade nech je to MARK. A transpozícia sa robí takto:
Kľúčové slovo napíšeme do horného riadku mriežky. Text z prvej časti píšeme postupne do mriežky po riadkoch. Potom stĺpce usporiadame tak, aby znaky kľúčového slova boli v abecednom poradí. A konečný zašifrovaný text získame postupným čítaním vzniknutej mriežky po stĺpcoch.

M	**A**	**R**	**K**
D	V	D	D
D	D	D	V
F	G	F	D
D	V	D	D
A	V	X	G
A	D	G	X

A	**K**	**M**	**R**
V	D	D	D
D	V	D	D
G	D	F	F
V	D	D	D
V	G	A	X
D	X	A	G

A dostávame výsledný text:
VDGVVDDVDDGXDDFDAADDFDXG

Znaky A, D, F, G, V, X sa použili preto, lebo sa v Morseovej abecede od seba výrazne líšia a znižuje sa tým riziko chyby pri prenose.

Keďže šifra bola vcelku komplikovaná, nemecké velenie ju považovalo za bezpečnú. Počas nemeckej ofenzívy sa nemecké delostrelectvo dostalo nebezpečne blízko Paríža, preto jediná nádej Dohody spočívala v rozlúštení šifry ADFGVX. Nakoniec ju 2. júna prelomil francúzsky kryptoanalytik Georges Painvin. A tak vďaka tomu mohli vojaci Dohody posilniť miesto pripravovaného nemeckého útoku a odraziť ho.

Ďalším príkladom naivného použitia šifry bol plán nemeckého ministra zahraničných veci Arthura Zimmermanna. Nemecko potrebovalo zahájiť neobmedzenú ponorkovú vojnu, vďaka ktorej by prinútilo kapitulovať Veľkú Britániu. Avšak toto by s najväčšou pravdepodobnosťou znamenalo vstup USA do vojny. Preto Zimmermann poslal veľvyslancovi Nemecka v Mexiku šifrovaný telegram. V ňom sľuboval Mexiku

nemeckú podporu, ak Mexiko napadne USA. Spoliehal sa na to, že túto správu ani USA, ani Británia nedostane do rúk. Avšak Británia ju rozlúštila. No neinformovala o tom USA okamžite. Z jednoduchého dôvodu – nechceli, aby sa Nemci dozvedeli, že ich šifra bola prelomená a nahradili ju silnejšou. A tak chceli počkať na začiatok ponorkovej vojny a následný predpokladaný vstup USA do vojny. Avšak USA do vojny nevstúpili. A tak neostávalo nič iné ako zverejniť telegram. Ale podarilo sa to urobiť tak, aby si Nemci mysleli, že telegram bol zadržaný v Mexiku.

V tomto období bola vynájdená konečne aj skutočne neprelomiteľná šifra. Slabina Vigenérovej šifry spočívala v tom, že sa jej kľúč používal stále periodicky dookola. Avšak keby bol kľúč taký dlhý ako celý text, periodickosť by sa odstránila. Jediný problém tejto šifry je v komplikovanej distribúcii kľúča. Preto sa táto šifra neujala v oblastiach, kde sa požaduje hromadné nasadenie, napríklad v armáde. Využíva sa však napríklad na horúcej linke, ktorá spája prezidentov USA a Ruska.

4. Šifrovanie počas druhej svetovej vojny

4.1. Enigma

Nové potreby rýchlej šifrovanej komunikácie nútili kryptografov k použitiu najnovších technických vymožeností. Začal sa vývoj rôznych šifrovacích prístrojov. Najznámejším z nich je Enigma, používaná Nemeckom v druhej svetovej vojne. Jej vynálezcom bol Arthur Scherbius.

Prístroj sa skladá z troch častí. Prvá z nich je klávesnica, druhá je šifrovacia jednotka a tretia je signálna doska, na ktorej sa zobrazuje zašifrovaný text. Na obrázkoch v prílohe vidíme základný princíp jeho fungovania. Základnou časťou prístroja je tzv. scrambler, gumový kotúč popretkávaný vodivými drôtmi. Do kotúča vstupuje vedenie z klávesnice na 26 miestach a potom z nej vychádza tiež na 26 miestach, pričom vnútri sa drôty rôzne prehýbajú a menia. Dôležité však je, že po zašifrovaní každého písmena sa scrambler otočí o 1 pozíciu. To značí, že keď stlačíme napríklad A dvakrát po sebe, tak nedostaneme do isté písmeno. Avšak v Enigme nie je len jeden takýto kotúč, ale rovno 3 za sebou. Pričom tie ďalšie sa otáčajú až vtedy, keď sa predchádzajúci otočí raz dookola. V Enigme sa nachádza ešte za sústavou scramblerov tzv. reflektor. Táto súčasť Enigmy je statická a vždy zostáva na svojom mieste V podstate len otočí elektrický signál a pošle ho znovu cez sústavu scramblerov. Avšak jeho význam v Enigme je veľmi dôležitý.

Keď chceme napr. zašifrovať slovo „UTOK“, tak nastavíme Enigmu do patričnej počiatočnej pozície (určená počiatočnými nastaveniami scramblerov) a zadáme na klávesnici „UTOK“. Z Enigmy dostaneme výstup, napr. „AYUP“. A keď Enigmu nastavíme znovu do rovnakej počiatočnej pozície a zadáme na klávesnici „AYUP“, tak dostaneme ako výstup pôvodné slovo „UTOK“. Čiže operácie šifrovania a dešifrovania sú zrkadlové. To v praxi zjednodušuje používanie prístroja. Ale to ešte nie je všetko. Zatiaľ má Enigma 26.26.26=17576 počiatočných nastavení. To je celkom málo. Preto je v Enigme ešte aj tzv. prepojovacia doska. Je to vlastne miesto, kde sa zapojením prepojovacieho kábla vymenia dve písmena pri prechode medzi klávesnicou a scramblerom a medzi scramblerom a signálnou doskou. Je možné

urobiť až 6 takýchto prehodení, čo zvyšuje počet možností počiatočného nastavenia Enigmy na vyše 10 000 000 000 000 000.

4.2. Boj s Enigmou

Po zavedení Enigmy do nemeckej armády začali byť britskí a francúzski kryptoanalytici bezradní. Avšak poľskí kryptoanalytici pod tlakom vojenskej hrozby z Nemecka boli nutení Enigmu prelomiť a podarilo sa im to. Využili pritom jednu slabú vec v systéme. Pre každý deň sa používalo samostatné nastavanie Enigmy (nastavenia scramblerov a prepojovacej dosky), tzv. denný kľúč. A na začiatku každej správy sa pomocou denného kľúča zašifrovalo nastavenie scramblerov pre danú správu. Avšak toto sa napísalo vždy dvakrát, aby sa predišlo preklepu. Toto oslabenie Poliaci (na čele s matematikom Marianom Rejewskim) využili a boli schopní čítať nemecké správy.

Avšak pár dni pred začiatkom druhej svetovej vojny Nemci Enigmu vylepšili a Poliaci nemali dostatok prostriedkov na boj s novou verziou. Ale stihli predať cenné informácie do Veľkej Británie. Tam začali vo veľkom dešifrovať nemecké správy. V praxi mali Briti všetky informácie o pohybe nemeckých jednotiek. To im umožnilo dosiahnuť oveľa ľahšie prevahu na mori a vo vzduchu, keďže Nemci stratili dôležitý moment prekvapenia.

5. Problém výmeny kľúčov

V dobe rozvoja počítačov už nebol problém zostaviť dostatočne silnú šifru postavenú na zložitých matematických operáciách, ktorá bola dostupnými prostriedkami neprelomiteľná. Ale zostával tu vždy ešte jeden problém. Tým bola distribúcia kľúča. Väčšina šifier sa skladá z algoritmu, ktorý mení správu pomocou kľúča na zašifrovaný text. A následne pomocou toho istého kľúča je algoritmus schopný premeniť zašifrovaný text na pôvodný. Samozrejme, nedá sa spoliehať na utajenie algoritmu. Preto je nutné utajenie kľúča. Na tom sa musia komunikujúce strany dohodnúť. To však môže byť nepohodlné, prípadne časovo, alebo finančne náročné. Preto sa rôzni vedci snažili nájsť spôsob, ktorým by sa mohli komunikujúce strany dohodnúť na kľúči bez toho, aby bolo nutné osobné stretnutie (resp. použitie spoľahlivo utajeného komunikačného kanála).

To, že sa to dá teoreticky dosiahnuť, si môžeme ukázať jednoduchým myšlienkovým experimentom. Prestavme si, že Alica chce poslať Bobovi niečo tajné. Zoberie balíček a dá na neho svoj zámok a pošle ju Bobovi. Bob pridá na balíček svoj zámok a pošle späť Alici. Alici odstráni svoj zámok a pošle Bobovi. A Bob len odstráni svoj zámok a má obsah balíčku k dispozícii. Pričom ktokoľvek, kto balíček odchytí nemá šancu dostať jeho obsah, lebo je zamknutý.

Avšak toto je v reči šifier nepoužiteľné. Je prakticky nemožné zostaviť šifru, pri ktorej by tento systém fungoval a zároveň bol bezpečný.

5.1 Diffie-Hellmannov algoritmus

Preto sa hľadali iné riešenia. Dôležitými sa stali hlavne poznatky v teórii čísel, hlavne týkajúce sa modulárnej aritmetiky. V tejto aritmetike sa nepoužíva celý rozsah celých čísel, ale iba čísla z istého rozsahu. Ak sa pri niektorej operácii tento rozsah prekročí, začína sa znovu od nuly. Čiže napr.:
*2 + 3 = 5 (mod 7) 1 + 6 = 0 (mod 7) 4*4=2 (mod 7)*

mod 7 vyjadruje daný rozsah. V tomto prípade používame rozsah od 0 do 6. Dá sa tomu rozumieť aj tak, že *(mod N)* je vlastne zvyšok po delení *N*.

V tejto aritmetike sú hlavne dôležité operácie, ku ktorým nepoznáme operáciu inverznú (inverzná operácia k sčítaniu je odčítanie, k násobeniu delenie, k umocňovaniu odmocňovanie, ...). A práve umocňovanie je operácia, na ktorej je založený Diffie-Hellmannov algoritmus (pomenovaný je po jeho stvoriteľoch Whitfildovi Diffiem a Martinovi Hellmannovi).

Algoritmus pracuje takto (komunikujúce strany označme ako Alicu a Boba):

1. Alica a Bob sa dohodnú na číslach *Y, P* (pričom $Y < P$ a *Y,P* sú nesúdeliteľné). Toto môžu vykonať aj verejne. V praktickom použití sú tieto čísla minimálne veľkosti 2^{128}.
2. Alica si vymyslí číslo *A* a uchová ho v tajnosti. Takisto Bob si vymyslí číslo *B*.
3. Alica vypočíta číslo $\alpha = Y^A \ (mod\ P)$, Bob vypočíta $\beta = Y^B \ (mod\ P)$
4. Alica a Bob si vymenia čísla α, β. Opäť to môžu uskutočniť verejne.
5. Alica vypočíta $k = \beta^A \ (mod\ P)$, Bob vypočíta $k = \alpha^B \ (mod\ P)$
6. Obaja dostanú rovnaké číslo. V skutočnosti $k = Y^{A.B} \ (mod\ P)$ – toto sa dá aj matematicky dokázať, ale nepovažujem to za potrebné.

Prakticky sa Alica a Bob dohodli na spoločnom čísle, ktoré môžu použiť ako kľúč. Tento spôsob výmeny kľúča je absolútne bezpečný. Hocikto, kto chce získať kľúč má k dispozícii čísla *Y, P,* α, β, ale nemôže z nich zrekonštruovať *k* v dostatočne rýchlom čase. O riešenie tohto problému s názvom „problém diskrétneho logaritmu“ sa pokúšajú poprední svetoví matematici a zatiaľ bez úspechu.

Ešte môže byť na mieste otázka ako rýchlo umocňovať tak veľké čísla. Tu je riešenie veľmi jednoduché. V klasickej matematike môžeme napr. napísať:
$3^{10} = 3^8 \ . \ 3^2$
A to môžeme urobiť aj v modulárnej aritmetike:
$3^{10} = 3^8 \ . \ 3^2 \ (mod\ N)$

Takže keď robíme operáciu $Y^A \ (mod\ N)$, rozložíme číslo A na súčet mocnín čísla 2. A potom postupne vypočítame $Y^2 \ (mod\ N)$, $Y^4 \ (mod\ N)$, $Y^8 \ (mod\ N)$, $Y^{16} \ (mod\ N)$, ...a z toho dopočítame $Y^A \ (mod\ N)$ a vykonáme pritom oveľa menej operácia ako keby sme len čisto násobili *A*-krát číslo *Y* samým sebou.

V praxi sa tento systém veľmi neujal z jednoduchého dôvodu. Na dohodnutie kľúča je nutné poslať príliš veľa správ, čo môže spôsobovať problémy.

5.2 Kryptografia s verejným kľúčom

Ďalšou myšlienkou riešiacou problém výmeny kľúčov, bola práve kryptografia s verejným kľúčom. Princíp spočíva v tom, že na zašifrovanie sa používa iný kľúč ako na odšifrovanie. Takže každý, kto chce prijímať správy potrebuje mať dvojicu kľúčov. Jeden verejný, ktorým sa budú správy preňho zašifrovávať a druhý súkromný, pomocou ktorého sa budú správy dešifrovať. Dôležité je, aby sa z verejného kľúča nedal získať kľuč súkromný. Táto kryptografia má hneď aj svoju nevýhodu. Pokiaľ bude chcieť útočník čítať správy pre nejakú osobu, stačí, že jej verejný kľúč nahradí svojím a môže čítať dané správy. Preto je dôležité, aby bol verejný kľúč overený niekým dôverihodným, napríklad tzv. „certifikačnou autoritou“.

Šifry, ktoré používajú iný kľúč na šifrovanie a iný na dešifrovanie, sa nazývajú asymetrické (obdobne šifry, ktoré používajú na šifrovanie a dešifrovanie rovnaký kľúč, majú názov symetrické). Myšlienka asymetrickej šifry bola formulovaná v roku 1975 Whitfieldom Diffiem, ale až v roku 1977 Ronald Rivest prišiel na to, ako ju realizovať. Vytvoril šifru RSA (pomenovanú po ňom a po jeho spolupracovníkoch Adim Shamirovi a Leonardovi Adlemanovi).

Táto šifra využíva Eulerovu vetu, ktorá hovorí:

$a^{k \cdot \varphi(N)+1} = a \ (mod\ N)$

Pričom *a, N, k* sú ľubovoľné prirodzené čísla, $\varphi(N)$ je počet čísel menších ako *N*, ktoré sú nesúdeliteľné s *N*.

Z tohto sa môžeme dostať k tomu, že by malo platiť(*e* – verejný kľúč, *d* – súkromný kľúč):

$e \cdot d = k \cdot \varphi(N) + 1$

Čo značí:

$e \cdot d = 1 \pmod{\varphi(N)}$

A ešte vieme, že ak $N = p.\ q$ (kde *p, q* sú rôzne prvočísla), tak potom:

$\varphi(N) = (p-1)(q-1)$

Z tohto sa dá vyvodiť princíp šifry RSA. Opäť komunikujúce strany označíme ako Alica a Bob (Bob posiela správu Alici):

1. Bob vygeneruje dve dostatočne veľké prvočísla *p, q*. Reálne sa používajú čísla minimálne veľkosti 2^{512}.
2. Vypočíta $N = pq$. A vygeneruje číslo *e*
   (*e* by malo byť nesúdeliteľné s $(p-1)(q-1)$)
3. Vypočíta si svoj súkromný kľuč *d*. Pričom platí $d \cdot e = 1 \pmod{(p-1)(q-1)}$
4. Dvojicu *N, e* zverejní ako svoj verejný kľúč.
5. Alica chce poslať Bobovi správu *M* (správa môže byť aj číslo). Zašifruje ju ako $c = M^e \pmod{N}$ a pošle Bobovi *c*.
6. Bob správu rozšifruje a dostane $M = c^d \pmod{N}$

Ako sa dá všimnúť, celá bezpečnosť šifry RSA stojí na neschopnosti rozložiť číslo *N* na prvočísla v dostatočne rýchlom čase. Pri dnešných znalostiach stále nevieme dostatočne rýchlo faktorizovať (rozkladať číslo na prvočísla) veľké čísla, takže RSA je zatiaľ bezpečná.

6. Asymetrické šifrovanie v praxi

Spočiatku mali asymetrické šifry jeden zásadný problém – rýchlosť. Na vtedajších počítačoch neboli schopné dostatočne rýchlo pracovať. Postupom času sa situácia zlepšovala, ale stále bolo nepohodlné pomocou asymetrickej šifry šifrovať celý dokument. Preto sa dokument šifroval pomocou rýchlejšej symetrickej šifry a kľúč k symetrickej šifre sa zašifroval pomocou asymetrickej šifry. Takto pracuje aj program PGP (Pretty good privacy – v preklade Celkom dobré súkromie), ktorý je voľne prístupný na internete.

6.1. Ochrana súkromia vs. štátny odposluch

V dobe, keď sa používala listová a telefonická komunikácia, bol odposluch komunikácie pomerne časovo a finančne náročný, ale bol možný. So zavedením internetovej komunikácie sa značne zjednodušil, lebo odposluch mohli vykonávať počítače na to pripravené. Všetko štátnym inštitúciám skomplikovala dostupnosť šifrovacích produktov typu PGP, ktoré mohli odpočúvanie úplne znemožniť. To vyvolalo dlhotrvajúcu debatu medzi politikmi, sudcami, bojovníkmi za ľudské práva a ďalšími. Rozdelili sa na dva tábory. Jeden hovoril, že šifrovanie je hrozba pre spoločnosť, lebo umožňuje zločincom bezpečne komunikovať. Druhá strana argumentovala, že obmedzenie kryptografie obmedzuje slobodu jedinca, čo je základný prvok demokracie. V USA boli snahy obmedziť kryptografiu pomocou zákonov, ale nakoniec tieto zákony neboli schválené. Ale platia tam zákony, ktoré stavajú vývoz šifier z USA do úrovne vývozu zbraní. Pri vyvážaných šifrách je obmedzená veľkosť kľúča a vďaka tomu sú šifry prelomiteľné metódou vyskúšania všetkých možných kľúčov. Na Slovensku zatiaľ žiadny zákon o kryptografii nemáme.

6.2. Digitálny podpis

Okrem toho, že komunikácia internetom je rýchlejšia a pohodlnejšia ako komunikácia listovou poštou, má aj jednu nevýhodu a tou je nemožnosť jednoduchého podpisu, teda zaručenia, že správu poslal skutočne odosielateľ. A navyše je nemožné zaručiť, že správa nebola cestou pozmenená. Samozrejme aj pri listovej pošte sa dajú

falšovať podpisy a meniť obsah správ, ale pri internetovej komunikácii je to oveľa jednoduchšie. Preto bolo nutné zaviesť jednoduchý systém, ktorý zaručí jednoznačnú identifikáciu odosielateľa. Stačilo na to použiť šifru RSA, avšak trochu ináč ako pri zašifrovaní správy. Predstavme si, že Bob chce poslať správu Alici a chce sa pod ňu podpísať. Použije opäť RSA vytvorí dvojicu kľúčov – verejný a súkromný. Verejný zverejní, čiže sa ho dozvie aj Alica. A teraz svoju správu zašifruje pomocou svojho súkromného kľúča a túto zašifrovanú verziu pripojí k správe. Alica má možnosť pomocou verejného kľúča odšifrovať zašifrovanú časť a porovnať s pôvodnou správou. Ak sa zhodujú tak správa prišla v nezmenenej podobe od Boba.

Toto má ale jeden technický nedostatok. Vyššie sme spomínali, že RSA je príliš pomalé na šifrovanie celých dokumentov. Samozrejme podobne to aj pri digitálnom podpise. Preto sa nešifruje celý dokument, ale iba tzv. hash (čítaj „heš“) dokumentu.

6.2.1 Čo je to hash?

Hash je jedno veľké číslo (väčšinou s veľkosťou rádovo 2^{128} – 2^{160}), ktoré jednoznačne identifikuje dokument a jeho obsah. Môžeme to prirovnať k odtlačku prstu u človeka. Dokument na hash premieňa tzv. hashovacia funkcia, označme si ju H. Jej vstup označme *M* a jej výstup ako *H(M)*. *M* môže mať ľubovoľnú veľkosť, od niekoľkých bajtov až po stovky gigabajtov. A H(M) bude mať vždy veľkosť charakteristickú pre danú hashovaciu funkciu (už spomínaných 2^{128} – 2^{160}). Funkcia H musí spĺňať tieto predpoklady:

- pokiaľ je dané M, musí byť jednoduché vypočítať H(M)
- pokiaľ je dané H(M), je prakticky nemožné vypočítať M – čiže H je jednocestná funkcia
- pokiaľ je dané M, je prakticky nemožné nájsť M‘, také aby H(M) = H(M‘) – H je odolná voči kolízií

Tieto predpoklady spĺňa aj odtlačok prsta. Pokiaľ máme jedinca, vieme veľmi ľahko získať jeho odtlačok prsta. Ak máme odtlačok prsta, je nemožné z neho zrekonštruovať jedinca. A tiež keď máme daného jedinca, je nemožné nájsť jedinca s rovnakým odtlačkom prsta.

Je veľa rôznych hashovacích funkcií. Niektorým z nich bola už nájdená kolízia, preto boli prehlásené za nie bezpečné hashovacie funkcie.

Čiže digitálny podpis pracuje potom takto:
Bob vypočíta hash svojho dokumentu a hash zašifruje pomocou svojho súkromného kľúča a výsledok pripojí k dokumentu ako podpis a pošle Alici.
Alica vypočíta znovu hash dokumentu, odšifruje podpis a porovná so svojou hash. Ak sa zhodujú dokument je od Boba.

6.2.2 Digitálny podpis na Slovensku

Zákon č. 215/2002 Zb. upravuje používanie digitálneho podpisu na území Slovenskej republiky. Samozrejme upravuje aj podmienky overovania verejného kľúča osôb (jednoduchá možnosť prelomenia podpisu je zameniť niekoho verejný kľúč za kľúč útočníka) – tzv. certifikáty.

6.2. Šifrovanie v každodennom živote

Občas si pri práci s internetom môžeme všimnúť, že miesto adresy „http://xxx.yy“ máme adresu „https://xxx.yy“. Značí to, že komunikácia medzi nami a naším počítačom prebieha šifrovanie pomocou protokolu SSL (vo svojom vnútri pracuje približne ako PGP – dohodne sa kľúč pomocou asymetrickej šifry a potom šifruje dáta symetrickou šifrou). Toto sa využíva hlavne v službách, kde je nutné zaručiť bezpečnosť informácii posielaných medzi klientov a serverom (napr. internet banking). Taktiež sa niekedy pri emailovej komunikácii môžeme stretnúť s použitím digitálneho podpisu, hlavne pri komunikácii na vyšších úradných miestach.

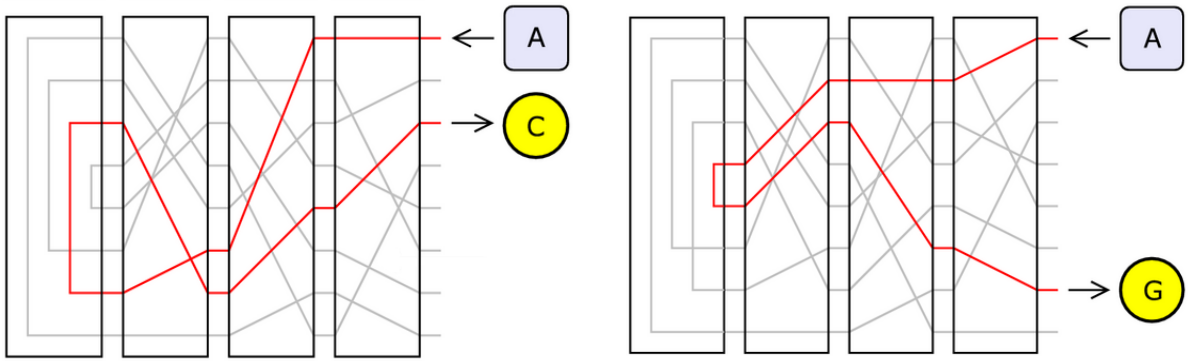
7. Záver

Podarilo sa mi zachytiť historický vývoj šifrovanej komunikácie od počiatkov v antike až po súčasnosť. Ukázalo sa, že kryptografia a kryptoanalýza mali významný vplyv aj na vývoj vojnových udalostí (dá sa už len polemizovať ako by vojny vyzerali, keby niektoré šifry neboli prelomené). Taktiež sa ukázalo, že v súčasnom živote má kryptológia významné postavenie. Vynorila sa však aj filozofická otázka, či má štát právo obmedziť šifrovanie, aby mal prístup ku komunikácii a mohol toto využívať pri stíhaní zločincov, ale zároveň tým obmedzovať osobnú slobodu jednotlivca.

Zoznam použitej literatúry

- Singh, S.: Kniha kódu a šifer, Praha, Dokořán a Argo 2003
- en.wikipedia.org
- www.zbierka.sk

Príloha – Obrazový popis nemeckého šifrovacieho stroja Enigma



Obr. 1 - základný princíp práce scramblerov a reflektora v Enigme (pre zjednodušenie, len pre 8 písmen), vpravo – prvý scrambler posunutý o 1 otáčku

Obr. 2 – celkový pohľad na Enigmu