Praktické základy Kryptologie a Steganografie

Vložil/a 3022 [1], 2 Prosinec, 2004 - 18:20

- Encryption [2]
- Science & Technology [3]
- Security [4]

Velmi zajímavý a obsáhlý článek o všech základních poznatcích z kryptologie a steganografie.

Tento dokument je určenou pouze pro informativní a studijní účely, neklade si nároky na absolutní přesnost a úplnost. Právní a morální důsledky použití zde nabytých vědomostí spočívají výhradně na osobní zodpovědnosti každého jedince.

Steganografie

Slovo steganografie pochází z řečtiny - ze slov steganos (schovaný) a graphein (psát). Je to věda o utajení komunikace prostřednictvím ukrytí zprávy. Do oblasti steganografie patří například neviditelné inkousty nebo mikrotečky. Steganografie má obecně tu závadu, že sice poskytuje jistý stupeň utajení, ale když už se zprávu podaří odhalit, je celý její obsah prozrazen - pouhé zachycení zprávy se rovná i prozrazení jejího obsahu. Steganofrafie se proto zpravidla kombinuje s kryptografií.

První zdokumentovaný případ steganografie pochází z 5. století před naším letopočtem, kdy Řek Demaratus, žijící v Sůsách poslal varování o perských přípravách na invazi do Řecka vyryté do voskové psací tabulky, z níž nejprve seškrábal vosk a po vyškrábání zprávy do dřevěného podkladu ji voskem opětovně zakryl. V jiném případě který se odehrál jen několik desítek let po této události, byla otrokovy oholena hlava, zpráva napsána na jeho holou lebku a on byl vyslán s poslestvím na cestu poté, co mu vlasy dorostly.

Podobně "zajímavou" metodu přenosu zpráv vymysleli i staří Číňané, kteří čas od času psaly tajné zprávy na jemné hedvábí, které pak zmačkaly do malé kuličky a zalili voskem. Posel pak voskovou kuličku polkl. Většina steganografů však dávala přednost poněkud... pohodlnějším a konvenčnějším metodám - zprávy se schovávaly v různě důmyslných, nápaditých i zcela prostých skrýších, jako byli například berle, protézy, fůry hnoje, nebo fekální vozy - informace se tedy v podstatě schovávali velmi podobně jako každý kontraband (drogy etc.). Pokud jde o specializované steganografické praktiky, pak šlo především o "neviditelné inkousty" z mléčné šťávy pampelišky nebo citronové šťávy, které se zviditelňovaly po zahřátí, případně později o inkousty ze složitějších syntetických sloučenin viditelných jen pod speciálním světelným zdrojem, nebo po přetření jinou chemikálií. Krátké zprávy se psaly pod poštovní známky a nakonec se objevili i tzv. mikrotečky - mikroskopické zmenšeniny, kdy na jednom milimetru byla vtlačena třeba celá stránka textu, kterou tak bylo možné ukrýt například v tečce za větou, a posléze s odpovídajícím zvětšovacím přístrojem bez problémů přečíst.

Dalším zajímavým typem "moderní" steganografie je její kombinace s kódy (kódy blíže dále), kdy prostřednictvím veřejných sdělovacích prostředků (rozhlas, rádio), denního tisku (inzeráty, nekrology), nebo cenzurované korespondence obě strany komunikují díky zprávám zdánlivě nevinného významu (nositelem informace zde může být například jen odlišná formulace stejného - a samostatně vcelku bezvýznamného - sdělení, například popisu počasí, kvalit inzerovaného výrobku, nebo utrpení truchlící rodiny "zesnulého").

Velké možnosti dnes nabízí tzv. digitální steganografie - žijeme ve věku počítačů a v nich se nachází spousta datových formátů ve kterých je velmi snadné zprávu ukrýt, aniž by ji normální člověk byl schopen odhalit. Zprávu je možné "přibalit" i do textových, nebo datových souborů, ale nejlépe se

informace schovávají ve grafických (bitmap), nebo zvukových fomátech, které přirozeně (s)nesou určitý "šum", aniž by zjevně byly znehodnoceny a u nihž jsou také veškeré vedlejší vlivy na "funkci" souboru eliminovány přirozenou nedokonalostí lidských smyslů.

Největší pozornosti se u digitální steganografie těší ukrývání informací do obrázků, zřejmě proto, že obrázky lze bez problémů umístnit na web a relativně diskrétně si je prohlédnout na každém počítači, zatímco hudba vyžaduje přecejen specializovanější software i hardware a pokud neužíváme sluchátka, ruší okolí. Digitální formáty obrázků jsou v podstatě dvojí - komprimované (jpg, gif) a pevné (bmp, tiff). Pro steganografii jsou obecně vhodnější formáty pevné a to hned ze dvou důvodů. Prvním je jejich velikost, která nám dovoluje do nich buď uschovat větší objem dat, nebo stejný objem dat více rozptýlit a tím jej i o něco lépe ukrýt. Druhý důvod souvisí s asi nejpodstatnějším problémem digitální steganografie, který spočívá v tom, že jakýkoliv editační zásah do souboru (například otočení obrázku o 90 stupňů) s sebou nese vysoké riziko úplného znehodnocení celé zprávy. Každá taková úprava totiž znamená, že se zpráva prožene matematickým algoritmem, který samozřejmě s ukrytou steganografickou zprávou nepočítá a nebere na ni ohled. U komprimovaných formátu je pochopitelně takový algoritmus "drastičtější", nicméně ani pevné formáty nejsou vůči tomuto efektu nějak zvlášť imunní - například i nepatrná změna velikosti obrázku je naprosto jistou cestou ke spolehlivé likvidaci steganograficky ukryté zprávy, o změně formátu vůbec nemluvě. Jinak jsou pro ukrytí zprávy ideální takové soubory, které obsaují mnoho "detailů" - obrázek na němž je jednolitá azurová obloha, nebo zvukový záznam pravidelně odtikávajícího chronometru zkrátka není právě tím nejvhodnějším. Ačkoliv v tomto ohledu není důvod podléhat nějakému zvláštnímu perfekcionismu, zpráva se přecejen musí mít "kde schovat" a na bílém pozadí, či v nahrávce "hlubokého ticha" se schová jen velmi těžko.

Pokud jde o způsob aplykace digitální steganografie, specializovaný software prostě do souboru podle určitých zákonitostí - které jsou vyjádřeny klíčem jež zná pouze odesilatel a příjemce - "přisype" určitá data. Není-li poměr mezi "nevinnými" a zabezpečovanými daty vyložene nevhodně zvolen, je velmi obtížné cokoliv postřehnout. A z toho nám vyplývá hned další omezení, jímž je přenosová kapacita. Velikost ukryté zprávy zkrátka nemůže být větší než velikost nosného média, ale musí být naopak podstatně menší. Zpravidla se volí poměr kolem 1:10 - větší "hustota" může zvýšit riziko odhalení, nižší je naopak nepraktická z hlediska objemu přenášených dat.

Proti každé zbrani existuje i protizbraň a ani moderní steganografie není výjmkou. Některé její problémy jsme si už nastínily. Zbývá dodat snad jen tolik, že stejně jako existuje specializovaný software pro ukrývání zpráv, existuje i podobný software určený k jejich vyhledávání. Bližší informace o této oblasti se mi bohužel nepodařilo získat.

Digitální steganografie dnes nachází rozsáhlé využití například při ochraně autorských práv - umístníte-li například na svém webu obrázek stažený z komerkční stránky Playboye aniž by jste jej nějak upravovaly, existuje možnost vás z této krádeže usvědčit právě prostřednictvím steganografie, tedy jakýmsi "digitálním vodoznakem". Ve státech kde je šifrování drasticky omezeno zákonem (např. Francie) - zpravidla pod záminkou boje s organizovaným zločinem či terorismem - steganografie bývá často zcela legální (podle "politické logiky") a jde tedy jít o příhodnou alternativu. Jinak je její použití pravděpodobně relativně vzácné - pro přenos kratších zpráv se za výhodnější považují kódová slova, u delších zpráv převažuje šifrování.

Pozn.: steganografický software lze poměrně snadno získat - existuje bezpočet komerčních, shareware i freeware programů. Jeden z nejkvalitnějších freeware pro Linux/UNIX je k dipozici na http://www.outguess.org/ [5] - včetně podrobné dokumentace i zdrojového kódu.

Kryptologie, kryptografie a kryptoanalýza - základní pojmy

Kryptologie je věda o šifrování (kryptografii) a dešifrování (kryptoanalýze). Její název vychází z řeckého slova kryptos (skrytý) a vyjadřuje, co je jejím cílem - nikoliv utajování samotné existence zpráv, ale skrýtí jejího význam. Aby nešlo zprávu přečíst, je otevřený text (zpráva před zašifrováním) podle pravidel předem dohodnutých příjemcem a odesilatelem změněn v šifrový text (zpráva po zašifrování), který je bez této úpravy nečitelný. Pokud taková zpráva padne do ruky nepřítely, je pro něj odhalení jejího obsahu bez znalosti přesných pravidel použitých k jejímu dešifrování jen velmi

obtížné nebo dokonce zcela nemožné.

Ústredním pojmem kryptologie jsou kódy a šifry. Pojem kód má v běžném jazyce velmi široký význam a často se používá obecně pro jakoukoliv metodu komunikace. Ve skutečnosti je však význam tohoto slova velmi specifický. V rámci kódu se slovo či fráze nahrazuje jiným slovem, číslem či symbolem. Například tajní agenti mají svá krycí (kodová) jména chránící jejich identitu, tedy slova používaná namísto skutečných jmen. Podobně lze slovní spojení Útok za úsvitu nahradit kódovým jménem Jupiter a to zaslat veliteli na bitevní pole, aby informace zůstala nepříteli skryta. Pokud se odesilatel a legitimní příjemce předem dohodli na kódu, pak jim význam slova Jupiter bude zřejmý, zatímco nepřítel který zprávu zachytí z ní nezjistí nic. Problémem kódů je skutečnost, že jsou nevyhnutelně poněkud nepružné - příjemce i odesilatel nebudou moci komunikovat mimo dohoduné kódy, jejich "slovní zásoba" bude omezena. Podoba kódových slov bývá volena pokud možno náhodně - kódové slovo by nemělo mít jakoukoliv souvislost se samotným sdělením. Hrubou chybou by například bylo označovat letadla jmény ptáků, nebo lodě jmény ryb (pokud kódy slouží k utajení infomace, nikoliv jen k jejímu urychlení). Samo kódové slovo by nepřítely nemělo prozradit vůbec nic, nemělo by vzbuzovat jakékoliv asociace blízké zprávě jež ve skutečnosti ukrývá. Největším nebezpečním pro kódová slova představuje samozdřejmě ztráta kódové knihy, ale hned za ní následuje opakované použití identických kódových slov, vzláště v situacích, kdy si je lze spojit s popisovaným dějem, místem, či událostí.

Alternativou kódu je šifra, což je technika která působí na nižší úrovni, tím že nahrazuje písmena (respektive jakékoliv fragmenty informace) namísto celých slov, nebo slovních spojení (informačních celků). Pokud například nahradíte písmeno tím, jež po něm následuje v abecedě (tedy místo A napíšeme do zprávy B, místo B napíšeme C atd.), pak Útok za úsvitu přepíšeme jako "Vupl ab vtwjuv" (mezery se zpravidla vynechávají, aby se protivníkovy ztížil odhad významu slov).

Každou šifru můžeme popsat pomocí obecné metody, které se říká algoritmus, a pomocí klíče, který který specifikuje detaily použitého šifrování. Padne-li nepříteli do rukou šifrový text, může se stát, že dokáže odhadnout jaký algoritmus byl použit, avšak nebude znát klíč (může se například domývat, že každé písmeno otevřeného textu bylo nahrazeno jiným písmenem šifrové abecedy, ale nebude vědět o jakou šifrovou abecedu jde). U šifry tedy stačí, aby se odesilatel a příjemce dohodli na klíči, který definuje význam 26 znaků abecedy, a už si mohou vyměňovat libovolné zprávy. Pokud by chtěli dosáhnout stejné pružnosti u kódu, bylo by třeba nejprve podstoupit obtížný proces definování kódového slova pro každé z tisíců slov, jež se mohou vyskytnout v otevřeném textu a taková kódová kniha by pak musel mít stovky stránek a vypadala by jako slovník. Distribuce šifrového klíče je naopak velmi jednoduchá, použití šifry pruzné i přiměřeně bezpečné. Je-li klíč spolehlivě střežen, pak nepřítel nemůže zachycenou zprávu dešifrovat bez velkého úsilí. Zpravidla se volí taková složitost klíče, která zajišťuje bezpečnost před běžnými průlomovými prostředky - například tak, aby dešifrování zprávy vyzkoušením všech možných klíčů bylo tak časově náročné, že už na prozrazení zprávy nebude záležet (velmi důležité zprávy se například běžně šifrují tak, aby čas nutný k jejich dešifrování byl větší, než dosud známý věk vesmíru).

Šifrování můžeme rozdělit na dvě hlavní větve - transpozici (změnu pozice) a substituci (náhradu). Při šifrování transpozicí se písmena otevřeného textu změní v text šifrový tím, že se podle jistého klíče přeházejí (jde tedy vlastně o přesmičku). Takový způsob šifrování zpravidla není příliš bezpečný u krátkých zpráv, zatímco u dlouhých naopak přináší jisté komplykace. Zprávu skládající se z jediného písmena tímto způsobem prakticky nelze zašifrovat, zprávu o třech písmenech lze zašifrovat jen šesti různými způsoby, což je z hlediska bezpečnosti naprosto nevyhovující. S rostoucí délkou sice bezpečnost exponenciálně stoupá, ale problémem se zde naopak stává složitost použití - transpozicí vznikne velmi složitý anagram, jehož luštění je obtížné jak pro nepřítele, tak i pro legitimího příjemce. Aby byl tento způsob šifrování efektivní z hlediska času, je se třeba držet nějakého poměrně jednoduchého systému, který však zvyšuje pravděpodobnost odhalení, v souvislosti se zvýšenou pravděpodobností detekce zákonitostí v šifrovaném textu.

Historicky první šifrovací zařízení například pracovalo na základě transpozice. Pocházelo ze starověké Sparty a šlo o tzv. scytale. Ve skutečnosti to byla jen obyčejná dřevěná tyč kolem níž se ovinul proužek kůže nebo pergamenu. Odesilatel jednoduše ovinul "papír" okolo tyče předem dohodnutého průměru, napsal podél ní zprávu, pak proužek odmotál a tím získal posloupnost přeházených, zdánlivě nic neříkajících znaků. Dešifrování zachycené zprávy však bylo při znalosti

základního principu poměrně jednoduché - stačilo jen vyzkoušet několik průměrů tyče, které připadaly v úvahu v souvislosti s délkou daného pruhu. Obecně se transpozice významnějí neuplatnila až do příchodu počítačů a s nimi souvisejícího elektronického šifrování. V určitých případech se však kombinovala se substitucí (jako například u německé šifry ADFGVX z roku 1918).

Monoalfabetická substituční šifra

Alternativou k transpozici je substituce - tedy vpodstatě nahrazení určitého písmena jiným písmenem, nebo případně několika různými písmeny (čísly, znaky). Krása substitučního systému spočívá v tom, že zaručuje velký stupeň bezpečnosti a zároveň se relativně snadno používá - algoritmus může být identický pro všechny odeslané zprávy, mohou jej znát všichni včetně nepřítele a bezpečnost to neohrozí. Utajen naopak musí zůstat klíč na základě něhož se budou zprávy šifrovat i dešifrovat. Tento klíč je ovšem snadné definovat a proto i měnit. Krátké zprávy šifrované tímto způsobem jsou navíc daleko bezpečnější než zprávy dlouhé a bez opakování klíče mohou být opravdu nerozluštitelné.

První zdokumentovaný případ použítí transpozice s objevuje v Zápiscích o válce galské od Julia Caesara, kdy byla ve zprávě nahrazena římská písmena řeckými, nečitelnými pro nepřítele. Dalším typem substituční šifry který Caesar používal a který se měl stát v následujících staletích velmi populárním je tzv. Caesarova posunová šifra, nebo jen Caesarova šifra. Ta využívá šifrovou abecedu, která vznikne posunutím šifrové abecedy o určitý počet míst. Ukážeme si například šifrování posunem o 3 místa:

```
Otev?ená abeceda: 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
Šifrová abeceda:  D E F G H I J K L M N O P Q R S T U V W Y Z Y A B C

Otev?ený text:    veni, vidi, vici
Šifrový text:     YHQL, YLGL, YLFL
```

Caesarova substituční šifra byla po celá staletí považována za přiměřeně bezpečnou - s primitivními šifrovacími pomůckami bylo její "prolomení" vyzkoušením všech alternativ dostatečně obtížné. Luštitelé šifer však nakonec našli zkratku - našli způsob jak si místo několika miliard let vystačit pár minutami.

Počátek kryptoanalýzy - frekvenční analýza a zlomení monoalfabetické substituční šifry

Substituční šifra, v níž je šifrová abeceda tvořena písmeny, symboli nebo jejich směsí se nazývá monoalfabetická substituční šifra. Tento druh šifry byl považován dlouhá staletí za přiměřeně bezpečný. Arabským kryptoanalytikům se však kolem 10. století našeho letopočtu podařilo najít metodu jak monoalfabetickou šifru zlomit. Vznikla kryptoanalýza. Mohlo k tomu pravděpodobně dojít až v období, kdy společnost dosáhla dostatečně vysoké úrovně v několika vědních disciplínách, mezi něž patří především matematika, statistika a lingvistika. Zdá se však, že bylo potřeba i cosi víc...

Islámská civilizace byla ideální kolébkou kryptoanalýzi, neboť islám vyžaduje dosažení spravedlnosti ve všech oblastech lidské aktivity a k tomu jsou podle jeho učení nezbytné znalosti tzv. ilm. K úlohám každého muslima tedy patří rozvíjet své znalosti ve všech oblastech. Důležitý byl však i jiný aspekt náboženské motivace, neboť Korán a hádíh (souhrn Prorokových proslovů) nebyli tak hezky uspořádány jako například Bible - panovaly pochybnosti o chronologickém uspořádání i pravosti jednotlivých pasáží. Arabští teologové se tedy neomezily jen na studium Prorokových myšlenek a žití v souladu s jeho odkazem, ale byli nuceni i k vědeckému zkoumání jeho spisů - a užití lingvistiky, statistiky a znalosti vývoje arabské fonetiky.

Neméně důležité ovšem byly i materiální faktory, tedy především ekonomický úspěch prvních islámských zemí, který vedl k tomu, že jejich učenci měly dostatek času, prostředků i dalších zdrojů k tomu, aby se mohly plně věnovat vědeckým problémům. Mimo to se šifrování prakticky uplatňovalo i v arabské administrativě, neboť základem státní správy je, byla a bude bezpečná komunikace (je

CC-BY-SA Security-Portal.cz | secured by paranoid sense | we hack to learn

doloženo, že se v islámských zemích pomocí šifer chránily nejen citlivé státní záležitosti, ale například i daňové záznamy).

Islámští učenci se navíc snažily převzít maximum znalosti i od předchozích civilizací - překládali egyptské, babylónské, indické, čínské, perské, syrské, arménské, hebrejské a latinské texty do arabštiny, což se samozdřejmě neobešlo bez rozsáhné znalosti lingvistiky.

Spojení mnoha oborů s sebou přineslo jedno velmi zajímavé poznání - totiž že jistá písmena jsou v rozličných jazycích různě frekventovaná, můžeme je v textu nacházet s tou či onou četností. A z toho nám logicky vyplývá, že pokud se frekvence užití jistého písmena v šifrovém textu blíží frekvenci jiného písmena obecně využívaného v dané řeči, jde pravděpodobně o jedno a totéž písmeno, respektive o jeho ekvivalent v rámci otevřeného textu. Výsledkem této úvahy je frekvenční analýza, technika díky níž není třeba zkoušet každý klíč, není třeba prolamovat kód "hrubou silou", ale je možné jej zdolat chytrostí :-).

Na druhou stranu tuto techniku nelze používat zcela mechanicky a není až tak jednoduchá jak by se zprvu mohlo zdát - obecná četnost jednotlivých písmen totiž nemusí odpovídat jejich četnosti v daném otevřeném textu. Tak například nejčetnějším písmenem v anglickém jazyce je písmeno e (12.7%), po něm následuje t (9.1%) a poté a (8.2%). Zet je zde naopak zastoupeno jen relativně vzácne (0.1%). Pokud však bezmyšlenkovitě použijeme frekvenční analýzu například na větu: "From Zanzibar to Zambia and Zaire, ozone zones make zebras run zany zigzags" ("Od Zanzibaru až po Zambii běhají Zebry bláznivě cikcak kvůly ozónovým zónám"), výsledkem bude pochopitelně nesmysl. Obecně lze říci, že u kratších textů jsou odchylky pravděpodobnější a pokud jde o méně než sto písmen, je dešifrování velmi obtížné. Není však nemožné. Dobrý lingvista dokáže kód zlomit tím, že frekvenci správně analyzuje i v rámci kontextu - namísto pouhého počítání četností se podívá jak často se jednotlivá písmena vyskytují v sousedství jiných. Už to mu poskytne vodítko k rozšifrování textu - pro angličtinu je napríklad typický výskyt h před e (jako ve slovech the, then, they apod.), zatímco se naopak jen velmi vzácně vyskytuje h po e, neboť t jen sotva najdeme vedle d, b, g, j, k, m, q či v.

Lze tedy říci, že každé písmeno má v určité řeči svou vlastní "individualitu", danou jak jeho obecnou frekvencí použití, tak i jeho vztahem k jiným písmenům. A právě na základě této individuality pracuje frekvenční analýza. Ta se nám na první pohled může zdát velmi obtížnou záležitostí, ale ve skutečnosti postupuje velmi rychle jakmile identifikujeme už jen nekolik málo písmen - vodítka nám poskytnou především kratší slova, které se vyskytují v každé řeči, případná slovní spojení a na závěr i celý kontext zprávy, který nám umožní několik posledních chybějících písmen doplnit bez jakýchkoliv pochybností.

Nomenklátory, nuly, klamače

Zatímco arabský svět běžně užíval výdobitků kryptografie i kryptoanalýzi, nacházela se křesťanská Evropa v době temna - ještě na počátku 15. století zůstávala frekvenční analýza před Evropou utajena a prostá, monoalfabetická šifra zde byla považována za dostatečnou záruku bezpečnosti. Brzy nato se však objevili první (Soro, Babou, Viéte), kteří kteří - snad nezávisle, snad zprostředkovaně - objevily tajemství frekvenční analýzi. Ti kdo si byli vědomi slabin monoalfabetické šifry jich intenzivně využívaly ve svůj prospěch a sami se naopak snažily vyvinout lepší metodu šifrování, která by bezpečně ochránila jejich vlastní komunikaci před nepřítelem.

Jedním z nejjednodušších zdokonalení monoalfabetické substituční šifry bylo zavedení tzv. klamačů či nul, tedy symbolů nebo písmen, které nereprezentují písmena původního textu, ale mají jen klamat kryptoanalytika - z hlediska obsahu jsou to jen bezvýznamné vsuvky. Například můžeme nahradit každé písmeno číslem od jedné do 99, takže - pokud vezmeme v úvahu že anglická abeceda má 26 písmen - 73 čísel neodpovídá žádnému písmenu. Pokud je náhodně rozmístníte po šifrovaném textu, a to s rozmanitou četností, drasticky tím ztížíte analýzu. Nuly (klamače) přitom nebudou pro příjemce zprávy představovat žádnou větší komplikaci - protože bude vědět které znaky skutečně odpovídají skutečným písmenům, bude vše ostatní prostě ignorovat. Velmi podobný účinek může mít i záměrně špatný pravopis otevřeného textu, ponivač spúsobý zmjenu freqenze jednotlivíh hlázeg a kryptoanalytikovi se bude pracovat daleko obtížněji, zatímco příjemce zprávu standartním způsobem

CC-BY-SA Security-Portal.cz | secured by paranoid sense | we hack to learn

dešifruje a pak si už s poněkud pokrouceným, ale stále ještě čitelným pravopisem nějak poradí.

Další možností je využití Nomenklátorů. Nomenklátor je kódovací systém který vychází z šifrové abecedy, jež slouží k zašifrování většiny textu, ale je doplněn o seznam kódových slov. Jde vlastně o vložení kódových slov do otevřeného textu a jeho následné zašifrování. Kódovými slovy zde nahradíme nejrizikovější části depeše, jako jsou například názvy a jména, ale také třeba i předložky a spojky, které jsou z hlediska frekvenční analýzi velmi nebezpečné. Navzdory tomu není tento systém o mnoho bezpečnější než obyčejná šifra, protože většinu textu lze rozluštit frekvenční analýzou a zbylá kódová slova lze zpravidla uhodnout z kontextu. A tak stejně jako si dovedli poradit s pozměněným pravopisem a klamači, dokázali dobří kryptoanalytici při odpovídajícím objemu komunikace nakonec pracovat i s nomenklátory.

Schopný kryptoanalytik nejprve vyloučil nejsnáze řešitelné metody - například prostou frekvenční analýzou zjistil pouhou přítomnost klamačů a nomenklátorů. Pomocí opakující se komunikace postupně vyřadil klamače, symboli které očividně musely představovat jen falešné stoupy, protože v jejich užití není žádný systém, nebo alespoň systém který by dával nějaký smysl. Zároveň identifikuje kódy - symboli jejihž frekvence a umistnění sice naznačuje nějaký smysl, ale prozatím jej nelze uhodnout. Následně provede prostou frekvenční analýzu. Z kontextu je pak zpravidla význam většiny nomenklátoru zřetelný, případně jej lze v souvislosti s událostmi které vyslání zprávy předcházeli, nebo po jejím doručení následovali uhodnout.

Tato skutečnost byla mezi nejlepšími kryptoanalytiky "veřejným tajemstvím" až do 8. února léta páně 1587, kdy byla na základě hlavního důkazu obžaloby popravena Marie Stuartovna za velezradu. Oním hlavním důkazem totiž nebylo nic jiného, než věřejná ukázka kryptoanalýzi "šifry Marie Stuartovny" - vpodstatě běžné monoalfabetické substituční šifry s klamači a nomenklátory - díky níž se obžalovaná ze svého vězení "tajně" dorozumívala s ostatními spiklenci. Šlo o dramatickou ukázku slabin monoalfabetické substituce. Náhle bylo všem zřejmé, že v bitvě mezi kryptografy a kryptoanalytiky mají navrch ti druzí. Každý kdo odesílal šifrovanou zprávu musel počítat s tím, že někdo dostatečně schopný ji dokáže dešifrovat a následně si bude moci přečíst všechna tajemství v ní obsažená. Před kryptografy stála úloha vymyslet novou, silnější šifru, na níž by luštitelé nestačily.

Vigenérova šifra - Le chiffre indéchiffrable

Nová šifra však již dávno existovala - roku 1586 totiž bývalí francouzský diplomat Blaise de Vigenére publikoval svou práci Traicté des chiffres (Traktát o šifrách) ve které nejen demonstroval slabiny monoalfabetických (jednoabecedních) šifer a předvedl jejich kryptoanalýzu, ale do detailu i popsal nový druh šifry a přesně rozvedl způsob jejího použití. Jednalo se polyalfabetickou (mnohoabecední) šifru, údajně zcela odolnou vůči frekvenční analýze. Základ této šifry však položil již někdy v 60. letech 15. století florentský umělec Leon Batist Alberti, když ve své eseji popsal "zcela novu šifru", která používala dvě či více šifrových abeced které se v průběhu šifrování střídaly a tak mátly kryptoanalytyka. K šifrování rovněž sestrojil pomůcku, známou jako Albertiho šifrovací disk.

CC-BY-SA Security-Portal.cz | secured by paranoid sense | we hack to learn

Šlo o jeden z prvních šifrovacích nástrojů (tzv. scramblerů), které zpracovávají otevřený text znak po znaku a převádějí jej na něco jiného. Alberti vzal dva měděné kotouče, jeden z nich o něco větší než druhý a umístnil je na společnou osu tak, že s nimi šlo vzájemně otáčet. Po jejich obvodu napsal písmena abecedy. Pomůcka tak mohla sloužit k jednoduchému převodu z jedné abecedy do druhé, ale Alberti doporučoval bezpečnost šifrování zvýšit tím, že by se koly po zašifrování každého znaku o jednu, či několik pozic otočilo a šifrovací abeceda by se tak v průběhu šivrování měnila. Dále však Alberti ve své práci neopokračoval, svůj objev více nerozvíjel. To za něj udělaly až jeho pokračovatelé - německý opat Johannes Trihemius, italský vědec Giovanni Porta a konečně Vigenére, který se s jejich díly seznámil na diplomatické misi v Římě. Ač měl o věc zprvu jen ryze praktický zájem a byl velmi zklamán nevyzrálostí celé myšlenky, později ji sám dopracoval do skutečně funkční a prakticky použitelné podoby.

Síla Vigenérovy šifry spočívá v tom, že k zašifrování zprávy nepoužívá ne jednu, ale hned několik ze 26 odlišných abeced, které spolu nemusejí mít žádnou souvislost a jsou jednoduše definovány posloupností znaků - klíčem, kterým může mít například i podobu kódového slova. První šifrovací krok spočívá v tom, že se vypíše tzv. Vigenérův čtverec - což je otevřená abeceda následovaná 26 šifrovými abecedami, z nihž každá je vůči předchozí posunuta o jedno písmeno (řádek 1 odpovídá posunu o jedno písmeno, řádek 2 posunu o dvě písmena atd.). Podstata šifrovaní pak spočívá v tom, že pro zakódování každého písmene použijete jiný řádek čtverce, tedy jinou šifrovou abecedu. Jinými slovy: první řádek je vlastně otevřenou abecedou a ostatní jsou různými abecedami šifrovacími. Odesilatel může zašifrovat první písmeno zprávy pomocí řádku 5, druhé podle řádku 14, třetí řádkem 21 a tak dále. Aby příjemce získal zpět čitelný text, musí vědět, kterým řádkem Vigenérova čtverce šifroval odesilatel každé písmeno zprávy, musí tedy mezi nimi existovat předem dohodnutý systém, podle něhož se řádky střídají. Toho se dosahuje právě pomocí klíčového slova.

CC-BY-SA Security-Portal.cz | secured by paranoid sense | we hack to learn

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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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

Pro ilustraci si předveďme jak prostřednictvím Vigenérova čtverce zašifrovat krátkou zprávu diverttroopstoeastridge ("odkloňte jednotky k východnímu hřebenu") za použití hesla WHITE ("bílý"): Jako první krok napíšeme heslo nad text zprávy - opakovaně, tolikrát, kolikrát je třeba, abychom pokryli celou její délku. Pak šifrujeme následujícím způsobem: k zašifrováním prvního písmene (jímž je d), se nejprve podíváme, jaké písmeno klíče se u něj nachází. Je to W, čímž je dán řádek Vigenérova čtverce - šifrová abeceda pro dané písmeno, která začíná právě písmenem W. V průsečíku sloupce označeného jako d a řádku označeném W najdeme písmeno Z, což je první písmeno hledaného šifrového textu. Pro zašifrování druhého písmene, opakujeme stejný postup - písmeno kódového slova nadepsané nad aktuálním písmenem volného textu nám určuje šifrovou abecedu jíž použijeme. Dešifrování probíha opačným postupem.

Vigenérova šifra je tak odolná vůči klasické frekvenční analýze - kryptoanalytik užívající frekvenční analýzu totiž vychází z frekvence jednotlivých písmen v celém šifrovaném textu, který je však v daném případě šifrován hned několika různými šifrovými abecedami a tudíž v něm ta samá písmena mohou reprezentovat jiné znaky volného textu.

Homofonní substituční šifra

Polyalfabetická povaha Vigenérovy šifry dává této šifře velkou sílu, ale zároveň podstatně ztěžuje její použití. Obtížnější práce s šifrou mnoho uživatelů odradila a tak se v 17. století příliš neuplatnila. Pro většinu kryptografů té doby byla ve skutečnosti monoalfabetická šifra přímo ideální - byla rychlá, snadná a s transpozicí a nulami plně bezpečná proti komukoliv, kdo nebyl tehdejším odborníkem v kryptoanalýze. Pro civilní sektor 17. století zkrátka zcela vyhovující. Monoalfabetická substituční šifra tak v různých formách zůstala v užívání po staletí. Profesionální kryptografové pracující pro vládu, či vysoké státní činitele nicméně potřebovali k boji s profesionálními kryptoanalytiky lepší nástroj.

Vigenérovu šifru však odmítaly pro její složitost, nebo lépe řečeno časovou náročnost. V dané době totiž sice už v Evropě panoval čilý komunikační ruch a proudily jí stovky šifrovaných depeší vysoké důležitosti, ale na druhou stranu ještě nebyly k dispozici složitější šifrovací pomůcky které by praktickou kryptografii ulehčily. Stávající administrativní oddělení jednotlivých úřadu by proto nebyla schopna takovou zátěž, jakou by představoval plný přechod od monoalfabetické k polyalfabetické

CC-BY-SA Security-Portal.cz | secured by paranoid sense | we hack to learn

substituční šifře zvládnout. Použití Vigenérovy šifry se tak omezilo pouze na ty nejdůležitejší státní dokumenty. Jinde se hledal kompromis - větší bezpečnost než měla monoalfabetická šifra při menší provozní složitosti než měla šifra polyalfabetická.

Hlavním kandidátem byla homofoní (stejnozvučná) substituční šifra - šifra v níž se každé písmeno nahrazovalo celou řadou reprezentaci, jejíž počet byl úměrný četnosti daného písmena. Například písmenu které tvoří asi 8% psaného textu se zde přidělí osm různých interpretací. Kdykoliv se objeví v šifrované textu, nahradí se jedním z těchto osmi symbolů, zvoleným náhodně. Na konci šifrování potom dojde k tomu, že každý z těchto sedmi symbolů bude tvořit asi 1% šifrového textu. Výsledná frekvence použití jednotlivých znaků v šifrovém textu pak nebude o skutečné podstatě znaků v otevřeném textu vypovídat vůbec nic. Nebo ano?

Na první pohled se skutečně zdá, že tu frekvenční analýza nemůže fungovat, neboť se všechny symboli v šifrovém textu vyskytují zhruba stejně často. I v tomto případě však šifrový text obsahuje různé drobné nápovědy, kterých může kryptoanalytik využít. Jak jsme si už řekly, každé písmeno má svou "osobnost" danou nejen frekvencí v níž se v tom či onom jazyku vyskytuje, ale i vztahem k jiným písmenům. Tyto vzájemné vazby lze využít i když je zpráva šifrována homofonní substitucí, která potlačila nejvýraznější projevy frekvence písmen. V angličtině je nejvýraznějším příkladem takového osobitého chování hláska q, za níž může následovat jen jedna jediná hláska a to sice u. Pokoušíme-li se tedy dešifrovat homofonní substituci, začneme konstatováním, že písmeno q se v textu vyskytuje pomerně vzácně... Kryptoanalytik tedy nevyužije četnost písmen, kterou kryptograf ošetřil homofonní šifrou, ale udeří na jejich chrakteristické vazby. Dříve nebo později, ale (se vzrůstající délkou šifrovaného textu) nakonec zákonitě zcela jistě narazí na takovou kombinaci, která mu poskytne naprosto spolehlivé informace nezbytné k dalšímu průlomu.

Je si totiž důležité uvědomit, že ač se homofonní šifra na první pohled podobá polyalfabetické, přinejmenším v tom, že se jeden a tentýž znak otevřeného textu šifruje několika různými symboly, ve skutečnosti je tu ten podstatný rozdíl, že jeden symbol šifrovaného textu naopak může reprezentovat jen jedno jediné písmeno - jakmile se jednou sestaví šifrová abeceda, zůstává v průběhu celého šifrování identická, ač má pro určité znaky více šifrových symbolů. Skutečnost, že máme u většiny písmen na vybranou mezi několika symboli není z dlouhodobého hlediska podstatná - kryptoanalýza je tím ztížena, ale nikoliv znemožněna. Prakticky vzato se tedy využijeme frekvenční analýzu na úrovni dvojic či rovnou skupin znaků (písmen), případně k počátečnímu průlomu využijeme opačného spektra frekvenční analýzi než tomu bývá zvykem u klasické monoalfabetické šifry (nejméně četná písmena) a následně zbytek odvodíme od konkrétních vztahů.

Ikdyž ovšem lze homofonní šifru rozluštit, jde stále o mnohem bezpečnější prostředek než jakým je monoalfabetická substituční šifra a její použití je přitom daleko snažší než u Vigenérovy šifry. Jde tedy o dokonalý kompromis - z pohledu 17. století.

Charles Babbage vs. Le chiffre indéchiffrable

18. století bylo charakteristické příchodem mnoha změn. Svět se překotně měnil a pomalu vybíhal ze starých zavedených kolejí. Pro nás je důležité především to, že si světové mocnosti uvědomily ohromnou důležitost informací, v důsledku čehož stavy kryptoanalytiků náhle prudce narostly. Objevují se "Černé komnaty" - početné tými specializovaných kryptoanalytiků, jakési "šponážní manufaktury". Rozšiřují se různé, kdysi jen velmi primitivní a zřídka užívané šifrovací pomůcky. Tomuto náporu homofonní subsituční šifry nemohou čelit. Vigenérova šifra je však dosud považována ze nerozluštitelnou a ve známost již vešla jako Le chiffre indéchiffrable - nerozluštitelná šifra. Logicky se proto má stát hlavní zbraní kryptografů proti kryptoanalytikům...

CC-BY-SA Security-Portal.cz | secured by paranoid sense | we hack to learn

Na světě však už je člověk který má veškeré naděje kryptografů pohřbít - Charles Babbage. Vyděděný syn bohatého londýnského bankéře, nezávislý, mohostranný učenec, autor jednotné ceny poštovného, tabulek úmrtnosti pro pojišťovnictví, první objevitel souvislosti mezi letokruhy a stářím stromu, iniciátor kampaně za vyhnání flašinetářů a pouličních muzikantů z Londýna, autor prvního funkčního návrhu mechanického počítače a také první přemožitel Le chiffre indéchiffrable...

K práci na zlomení Vigenérovy šifry se přitom Charles Babbage dostal zdánlivě jen náhodou - prostřednictvím výzvy jejího samozvaného vynálezce, jistého zubaře Johna Halla Brocka Thwaiterse, který na jeho poznámku v tom smyslu že "nejde o žádný nový vynález ale o starou Vigenérovu šifru" odpověděl "ať si tedy pan vědec tu starou šifru kterou prý tak dobře zná rozluští..." A stalo se - úkol považovaný za nemožný byl splněn krátce po Babbagově střetu s Thwaitesem roku 1854. Nikdo se však o tom nedozvěděl. Babbage totiž svůj úspěch nezveřejnil. Proč se tak stalo se dodnes s jistotou neví. Existují spekulace, že Babbage svůj objev nezveřejnil na žádost britské rozvědky - právě totiž probíhala krymská válka. Roku 1863 však řešení publikoval jistý vysloužilý důstojník pruské armády jménem Friedrich Wilhelm Kasinski, který na ně přišel nezávisle na Babbagovi. Příslušná kryptoanalytická technika je proto známa jako Kasinského test. Babbagův vklad byl zcela ignorován a přišlo se na něj vlastně až ve dvacátem století, při zpětném studiu jeho osobních dokumentů (tedy zhruba ve stejné době, kdy byla ověřena funkčnost jeho návrhu Differencial Engine No.2 - stroje který v dané době nebylo v lidských silách vyrobit).

Připomeňme, že zásadní výhoda Vigenérovy šifry spočívá v tom, že stejné písmeno lze zašifrovat více způsoby, konkrétně tolika, kolik znaků má celé klíčové slovo. A z toho nám vyplývá, že i celá slova budou zašifrována různými způsoby, podle toho v jaké se při šifrování nachází pozici oproti klíčovému slovu. Babbage i Kasinský ovšem vyšly z předpokladu, že pokud otevřený text obsahuje dané slovo několikrát, pak je velmi pravděpodobné, že šifrový text bude v určitých případech také stejný, protože pozice šifrového klíče se bude v několika případech náhodně shodovat. A právě tato pravidelnost nám může poskytnout opěrný bod, který potřebujeme k rozlomení celé šifry. U delšího textu je totiž ve skutečnosti vysoce pravděpodobné, že na podobná identická a často se opakující slova narazíme - může jít například o předložky, spojky, nebo přímo o často užívané výrazy, jména, označení a názvy.

Základní slabinou Vigenérovy šifry je zkrátka její cyklická povaha - má-li klíčové slovo pět písmen, pak se každé páté písmeno otevřeného textu šifruje podle stejné šifrové abecedy. Podaří-li se kryptoanalytikovi stanovit délku klíče, může pak s šifrovým textem nakládat jako se sadou monoalfabetických šifer a poté jednu po druhé rozluštit pomocí běžné frekvenční analýzy. Bezpečnost proto přirozeně klesá úměrně k opakování klíče v průběhu šifrování, které stoupá přímo úmerně s délkou klíče a nepřímo úmerně s délkou šifrovaného textu. Jinými slovy, pokud je klíč

CC-BY-SA Security-Portal.cz | secured by paranoid sense | we hack to learn

stejně dlouhý jako sama zpráva, je frekvenční analýza nemožná, pokud má jedno písmeno (monoalfabetická substituční šifra), je velmi snadná. Jak se říká: všeho moc škodí - zatímco krátký klíč není bezpečný, klíč dlouhý jako sama zpráva je naopak poměrně nepraktický - prakticky se totiž už nejedná o šifrování, ale jakousi lepší alternativu kódování, s většinou výhod a nevýhod které tato metoda má, jako je například obtížná distribuce "kódových knih". Kódové slovo - klíč - proto pravděpodobně nejenže nebude dlouhé jako sama zpráva, ale pravděpodobně bude velmi krátké, zpravidla bude mít délku mezi peti až dvaceti písmeny.

Postup při dešifrování Vigenérovy šifry proto vlastně spočívá v hledání klíčového slova - úplné sestavení otevřeného textu na základě vztahů by bylo obtížné, ale protože se stejné klíčové slovo používá jak šifrování tak i k dešifrování, kryptoanalýza je po jeho odhalení snadná. Metodou jak identifikovat klíčové slovo je hledání sekvencí které se v šifrovém textu několikrát opakují. U kratších sekvencí existuje jistá pravděpodobnost, že k opakování došlo náhodně, po zašifrování jiných písmen otevřeného textu jiným umístněním klíčového slova. U delších sekvencí které se opakují vícekrát je ale naopak pravděpodovnost něčeho podobného jen nepatrná.

Zřídka můžeme identifikovat celé klíčové slovo okamžitě po nalezení opakujících se sekvencí, velmi snadno však z nich můžeme vydedukovat délku klíčového slova prostřednictvím mezer které jednotlivé sekvence dělí. To nám umožní rozdělit si celý šifrovaný text na několik monoalfabetických šifer, které už umíme vyřešit obyčejnou frekvenční analýzou. Rozdíl je pouze v tom, že v daném případě nás otevřený text v zásadě ani příliš nezajímá - jednotlivé jeho fragmenty které jsme schopni odhadnout například na základě nejčastěji užívaných spojek (ale, ani) nám pouze umožní odhalit klíčové slovo a díky němu pak následně budeme moci dešifrovat celý text najednou, standartním postupem který by použil i legitimní příjemce.

Jednorázová tabulková šifra (one-time pad)

Jak již bylo řečeno výše, základní slabinou Vigenérovy šifry je její cyklická povaha a celá šifra je tím zranitelnější, kolikrát došlo k prostřídání klíčového slova v celé zprávě. Co ovšem v případě, je-li klíč skutečně stejně dlouhý jako sama zpráva? Z hlediska praktické kryptografie je to sice poněkud nepohodlné řešení, ale u zpráv jejihž důležitost je opravdu enormní se kryptograf může odhodlat i k tomuto kroku aby zajistil maximální možnou bezpečnost. Ve skutečnosti ovšem sám klíč dlouhý jako zpráva nestačí a ani v nejmenším nezaručuje bezpečnost šifrové komunikace. Ukážeme si proč.

S ohledem na ohrožení jež představuje cyklická podoba Vigenérovy šifry, lze dlouhý klíč očekávat především tehdy, je-li i zpráva velmi dlouhá. Má-li ovšem zpráva délku stovky písmen, musí je mít i klíč. A v takovém případě se zdá, že než podobný dlouhý klíč vytvářet od nuly, je lepší jej poskádat z několika jmen, názvů, nebo rovnou celých vět opsaných kupříkladu z nějaké z mnoha knih. Klíč který dává jistý smysl si totiž lze poměrně dobře zapamatovat, distribuovat, nebo ho vyhledat. Podobné řešení by ovšem kryptoanalytikovi také umožnilo průlom...

Kryptoanalýza zde vychází z předpokladu, že otevřený text obsahuje některá běžná slova, jako například anglický určitý člen the, který je v tomto jazyce velmi frekventovaný. Pokud toto slovo rozložíme na různých místech šifrového textu a zkusíme jej převést Vigenérovým čtvercem, v okamžiku kdy bude náš odhad polohy inkriminovaného řetězce správný dešifrujeme z šifrového textu nikoliv text otevřený který vkládáme, ale naopak fragment klíčového slova. Je-li zpráva dostatečně dlouhá, máme šanci že k tomu dojde vícekrát a pak - dává-li klíč nějaký smysl - můžeme z jeho fragmentů uhodnout i vedleší pasáže a následně celý jeho zbytek, obdobným způsobem - testováním prostřednictví odhadovaných pasáží prostřednictvím jejich převodu Vigenérovým čtvercem.

Tím jsme tedy zjistily, že sama délka klíče ještě bezpečnost nezaručuje - je se třeba vyhnout i klíčům které dávají nějaký smysl, neboť kryptoanalytik může využít i této skutečnosti ke zlomení šifry. Je tedy nutné sestavit zcela náhodný klíč, který po přečtení nedává žádný smysl. Takovou dlouhou hatmatilku bez zákonitostí ovšem není právě jednoduché vytvořit, lze si ji jen velmi obtížné zapamatovat a pro více zpráv bude potom potřeba čehosi co nebezpečně připomíná objemnou kódovou knihu. Nabízí se proto logická myšlenka: co podobný dlouhý náhodný klíč využít při šifrování několika různých zpráv? Ani tudy cesta nevede.

CC-BY-SA Security-Portal.cz | secured by paranoid sense | we hack to learn

Pokud totiž zachytíte dva, nebo více textů zašifrovaných jedním klíčem, lze je dešifrovat v zásadě stejný způsobem - celá kryptoanalýza vyjde ze stejného základního předpokladu, jako v předcházejícím případě. Výsledkem aplykace vašeho odhadu na první zprávu sice bude i v případě že se trefíte jen několik znaků nedávajících žádný smysl, ale pokud takto získanou část klíče aplykujete i na další text zašifrovaný stejným klíčem, objeví s největší pravděpodobností fragmenty otevřeného textu dávajícího smysl (v případě správného odhadu otevřeného textu v první zprávě) a to vám zpětně ukáže že váš původní předpoklad ohledně prvního otevřeného textu byl správný. Budete-li touto metodou postupovat v obou textech, bude pravděpodobnost dešifrování zpráv dokonce ještě větší než v předchozím případě.

Z následujících příkladů tedy vyplývá, že jediným typem 100% nerozluštitelé Vigenérovy šifry je jednorázově použitá šifra s klíčem o stejné délce jako sama zpráva, přičemž klíč sám o sobě nesmí dávat žádný smysl, musí být utvořen náhodně. Tento typ šifry se nazývá jednorázová tabulková šifra (one-time pad), v češtině se používá také termín "jednorázové heslo". Jde o jedinou absolutně bezpečnou metodu klasického šifrování, která je dána naprosto náhodným charakterem klíče a jeho jednorázovým použitím. Ačkoliv byl koncept náhodného jednorázově použitelného klíče vypracován již roku 1918 (majorem Josephem Mauborhne, šéfem kryptografického vyzkumu armády USA), kupodivu se tento způsob šifrování nikdy příliš nepoužíval. Nepřekonatelným problémem pro jeho praktického využití byla především distribuce klíčů, která představovala podobný problém jako u kódových knih. Tento způsob šifrování se proto údajně nikdy nepoužil přímo v boji a je považován za vhodný pouze pro spojení, kde se vyžaduje extrémně vysoké utajení, bez ohledu na možné praktické komplykace se zajištění provozu. Touto šifrou je zabezpečena například horká linka mezi prezidenty Ruska a USA.

Enigma a mechanizace kryptografie

Navzdory vzniku jednorázové tabulkové šifry lze říci, že od chvíle kdy Babbage a Kasinski prolomili bezpečnost Vigenérovy šifry až do 70. let 20. století kryptografové hledaly způsob jak obnovit utajení komunikace prostřednictvím lepších šifer, ale neuspěli. Velký tlak na kryptografy vyvíjela především armáda a to v souvislosti s novým, nadějným, ale také dosti problematickým vynálezem - rádiem . Rádio totiž na jednu stranu omožňovalo přímou komunikaci mezi dvěma body, bez nutnosti spojovat je kabely a téměř bez ohledu na jejich pozici (vyjma vzdálenosti a rušivých vlivů terénu). Zatímco telegraf plnil velmi dobré služby na souši, do vynálezu rádia neexistovala žádná možnost jak s obdobnou efektivitou komunikovat s loděmi na moři nebo s pohyblivými cíly obecně. Rádio mělo potenciál k vyřešení tohoto problému a slibovalo velký užitek, ale zároveň přinášelo i jeden velký problém - rádiové vlny se totiž šířily všemi směry a tak to co zachytil legitimní příjemce mohl stejně dobře zachytit i kdokoliv v okolí, pokud byl v dosahu a monitoroval danou frekvenci. Když ovšem zprávu nebylo možné před protivníkem skrýt, bylo možné ji zašifrovat tak, aby ji nedokázal přečíst...

Mnozí si dělali naději, že dojde v oblasti kryptografie k průlomu a bude objevena nová šifra, která zajistí spolehlivé utajení vojenských komunikací na dalších několik desítek, nebo snad i stovek let. K ničemu takovému však nedošlo - nové šifry byli víceméně jen kombinacemi, nebo variacemi těch stávajících a buď byli příliš složité pro běžné použití, nebo je týmy kryptoanalytiků po krátké době intenzivního úsilý prolomili. Jednou z nejslavnějších šifer první světové války byla například německá šifra ADFGVX užívaná vyšším velením od 5. března 1918. Její síla spočívala ve spletité povaze kombinující substituci s transpozicí. Bylo to mistrovské dílo kryptografie, ale přesto byla v relativně krátké době prolomena - již 2. června večer ji francouzký kryptoanalytik Georges Painvin pokořil - zhubl při tom sice o 15 kg, ale i díky jeho výkonu byla velká Ludendorfova ofenziva - jeden z nejvážnějších zvratů v celé průběhu války, který ještě mohl zvrátit její výsledek - zastavena. Další velkou ranou německé kryptografii jejíž dopad na válečné úsilý byl pravděpodobně ještě větší, bylo předchozí dešifrování tzv. Zimmermannova telegramu - diplomatické depeše nejvyšší důležitosti určené politickým představitelům Mexika a obsahující návrh společného ujednání proti Spojeným státům, které dosud nebyli ve válce, ale jejich vstup do ní se v budoucnu jevil jako nevyhnutelný. Právě dešifrovaný text této depeše přesvědčil amerického prezidenta Woodeowa Wilsona k okamžitému vstupu USA do války a společně s ním zemřela i šance na Německé vítězství, po velmi příznivém vývoji na ruské frontě roku 1917.

Podle výsledků první světové války se tedy zdálo, že kryptoanalýza poráží kryptografii. Po válce

CC-BY-SA Security-Portal.cz | secured by paranoid sense | we hack to learn

"která měla skončit se všemi válkami" se tím však v zásadě nikdo příliš netrápil - vítězné mocnosti byli sebevědomé až na půdu a poražení měli zprvu dost starostí sami se sebou a o svém fiasku na poly kryptografie vlastně ani nevěděly - dva nejdůležitějších případy selhání jejich kryptoanalytiků jim totiž byli jejich protivníky zamlčeny (v případě Zimmermannova telegramu Němci například věřily, že byl ukraden až dešifrovaný text v Mexiku, takže obviňovali mexické úřady, nikoliv vlastní kryptografy). Roku 1923 však vyšel najevo pravý stav věcí, neboť britská strana již dále nepovažovala za nutné, ani přínosné uchovávat své bývalé protivníky v nevědomosti a zveřejnila skutečný stav věcí hned v několika oficiálních dokumentech. Pro německé kryptografy to představovalo těžkou deziluzi. Pochopitelně okamžitě začaly zkoumat způsoby jak se v budoucnu podobnému fiasku vyhnout.

Řešení jim nabídl Arthur Schreibus a jeho Enigma. Enigma se nakonec stala jednou z největsích legend v historii kryptoanalýzi, ale v zásadě nebyla ničím až tak úžasným. Vpodstatě šlo o důmyslné šifrovací zařízením pracující na principu polyalfabetické substituční šifry kombinované s monoalfabetickou šifrou. Nešlo tedy ani tak o nějaký zázračný nový způsob šifrování, jako spíše o prostou mechaninizaci těch předcházejících. Dokonce bychom snad mohly říct, že německá šifra ADFGVX z roku 1918 byla principielně daleko složitější.

Enigma byla nicméně působivým strojem, který odstartoval novou epochu v historii šifrování a dešifrování. Její jádro tvořilo několik "elektrifikovaných Albertiho šifrovacích disků" (scramblerů), které se při šifrování (podle jistých, přesně daných pravidel) automaticky otáčely a tak vlastně neustále přecházeli od jedné šifrovací abecedy k jiné. Pravidla podle nihž se scramblery otáčely (nebo-li jejich "převodové poměry",chcete-li) se dala měnit změnou jejich pořadí - scramblery totiž nebyly pevné, ale vzájemně vyměnitelné. Mimo to zde byl i další bezpečnostní prvek - rozvodná deska propojující klávesnici s celým vnitřním mechanismem. Na rozvodné desce se šest párů (nejfrekventovanějších) písmen dalo propojit bezpočtem různých způsobů.

Bezpečnost kterou Enigma zajišťovala při velké pružnosti v provozu tak byla do té doby nevídaná. První verze Enigmy měla 3 scramblery. Každý ze těchto tří scramblerů se dal nastavit do jedné z 26 různých pozic odpovídající 26 písmenům abecedy. Celkem tedy nastavení scramblerů nabízelo 26 x 26 x 26 (tj. celkem 17.576) různých nastavení. Tyto tři scramblery však šlo vzájemně uspořádat šesti různými způsoby (kombinace: 123,132,213,231,312,321). Propojovací deska umožňovala prohozením propojení šesti párů písmen dosáhnout 100.391.791.500 různých kombinací. Celkový počet klíčů, který byl dán součinem výše zmíněných kombinací - 17.576 x 6 x 100.391.791.500 - tedy dohromady činil (přibližně) 10.000.000.000.000.000.

CC-BY-SA Security-Portal.cz | secured by paranoid sense | we hack to learn

Jak je patrné, zdaleka největší vliv na počet klíčů měla propojovací deska. Můžeme se tedy ptát, proč se Scherbius namáhal se scramblery. Propojovací deska však sama o sobě produkovala jen monoalfabetickou substituční šifru, v níž se otevřená a šifrová abeceda liší jen ve dvanácti písmenech. Sama o sobě proto žádnou zvláštní ochranu proto kryptoanalýze neposkytovala. Problém propojovací desky zkrátka spočíval v tom, že se během šifrování její nastavení neměnilo a tak výslednou šifru nebylo samo o sobě problémem rozluštit pomocí frekvenční analýzy. Naopak scramblery sice přispívaly k celkovému počtu klíčů jen relativně málo, ale jejich nastavení se v průběhu šifrování měnilo, takže výsledný šifrový text nebylo možné pomocí frekvenční analýzy rozsluštit. Díky kombinaci scramblerů s propojovací deskou tedy Scherbius svůj stroj velmi účinně ochránil proti frekvenční analýze a zároveň jej vybavil nesmírným množstvím možných klíčů. Hlavním důvodem proč zvolil kombinaci výše zmíněných opatření byly důvody prostorové, výrobní a cenové - nejspolehlivějším způsobem jak zvýšit bezpečnost šifrování by bylo jednoduché zvýšení počtu scramblerů, řekněme ze tří na dvanáct, dvacet, padesát, nebo třeba dvěstě. Enigma by tak ovšem vycházela příliš velká, težká a také drahá, protože scramblery (a s nimi úzce související součásti) byli nejdražšími a nejkomplykovanšjšími částmi celého šifrovacího stroje.

První patent získal Scherbius už roku 1918. Přístroj měl tehdy podobu kompaktní skříňky o rozměrech pouhých 34 x 28 x 15 cm, a vážil jen něco kolem 12 kg. Šlo tedy o velmi praktický, rychlý a bezpečný šifrovací nástroj, velikostí i vnějším vzhledem zhruba odpovídající psacímu stroji. Podobné přístroje ale nebyli jen doménou Německa - roku 1919 byly jen nepatrně odlišné přístroje patentovány například i ve Spojených státech a Nizozemí. Problémem byla ve všech případech vysoká cena, která většinu kupců odrazovala a to zvláště v poválečné období. Deziluze německých kryptografů roku 1923, kdy vpodstatě zjistily, že lví zásluhu na porážce Německa měla právě jejich prohra v boji se spojeneckými kryptoanalytiky, však poskytla dostatečně silný impuls, potřebný k zavedení Enigmy do armádního použití ve velkém - roku 1925 byla zahájena velkovýroba a již o rok později se začala používat v německé armádě, následně i ve státní správě a různých státem řízených organizacích, například na železnici. Během dalších dvaceti let koupila jen německá armáda přes 30.000 přístrojů. Scherbiův vynález tak poskytl Německu nejdokonalejší šifrovací systém na světě...

Bomby, Colossus a komputerizace kryptoanalýzi

Roku 1926 začali britští kryptoanalytici v "Kanceláři č. 40", francouzi v Bureau du chiffre a Američané z U.S. Cipher Bureau zachycovat depeše, které je zcela zmátly. Enigma začala pracovat. Jak počet přístrojů rostl, jejich schopnost získávat informace rapidně klesala. Všichni se krátce snažili bojovat s novou šifrou, ale jejich snaha nepřinášela absolutně žádné výsledky a tak se velmi brzy vzdali. Rychlost s jakou tehdy podlehly se snad dnes může zdát překvapivá, ale s ohledem na některé skutečnosti byla vlastně zcela pochopitelná - po první světové válce se státy Dohody nikoho nebáli, Německo bylo porážkou ochromeno, do roku 1935 prakticky nemělo armádu která by stála za zmínku a oni cítily že jsou jasně v dominantní pozici. Jejich kryptoanalytické nasazení vůči Německu tedy zcela pochopitelně ochablo, počet kryptoanalytiků i jejich kvalita poklesly. Navíc tu před nimi byla nová "nerozluštitelná šifra"...

Existoval však jeden stát, který si nemohl dovolit odpočívat na vavřínech - Polsko. Poláci se cítily ohroženi. Zdálo se jim, že v každé další válce budou jako první na řadě. Jejich pozice byla opravdu nepříjemná -na východě sousedily s Německem a na západě zas s Ruskem - zeměmi, kterým se samostatné Polsko nikdy příliš nelíbilo, které chtěly "svá území na která měly historické právo" a které toužili šířit svou ideologii právě přes polské území. Země vtisknutá mezi dva nepřátele samozdřejmě potřebovala rozvědku a její informace. Poláci proto záhy založili šifrovací oddělení které nazvali Biuro Szyfrow. Už během rusko-polské války v letech 1919-1920 prokázalo svou užitečnost ohromným přísunem dešifrovaných zpráv a podobně úspěšně si polští kryptoanalytikové vedli i proti německým kryptografům - až do roku 1926.

Tehdy začal souboj kryptoanalýzi s kryptografií, který se nakonec stal jednou z největších legend kryptoanalýzy a jehož historie nám dnes může připomínat vzrušujícímu špionázní triller. Zprvu to ovšem nevypadalo nijak slavně - Poláci měly k dispozici jen civilní verzy Enigmy, ale i na té si zvládly vylámat zuby. Kapitán Maxmilian Ciezki, odpovídající za dešifrování německých komunikací, z toho byl dokonce tak zoufalý, že najal jasnovidce v urputné snaze vydobýt ze zaširovaných zpráv alespoň

CC-BY-SA Security-Portal.cz | secured by paranoid sense | we hack to learn

nějaký smysl. Jak se dá očekávat, jasnovidec nedosáhl takového průlomu, jaký by Biuro Szyfrow potřebovalo...

8. listopadu 1931 se nicméně francouzské rozvědce podařilo získat tajnou dokomentaci k Enigmě a následně postavit i přesnou repliku vojenské Enigmy. To ovšem k dešifrování zpráv ještě nestačilo - síla šifry totiž nespočívala v utajení přístroje, ale v utajení jeho počátečního nastavení, které se den ode dne měnilo. Bez jeho znalosti by kryptoanalytik pokoušející se celý problém řešit hrubou silou musel vyzkoušet každý z miliónů miliard klíčů. Vytrvalý kryptoanalytik, který by vyzkoušel jedno nastavení za minutu, by potřeboval k prověření všech možností dobu delší, než je dnes známý věk vesmíru. Čily zdánlivě nemožný úkol. Francouzské Bureau du chffre to tedy jednoduše vzdalo. O deset let dříve však Francouzi podepsali smlouvu o vojenské spolupráci s Polskem a Poláci vyjádřili zájem o vše co s Enigmou soviselo. Francouzi se domývaly, že pokud s tím co mají nic nepořídí oni, je to zcela bezcenné i pro Poláky - a tak s nimi o to rádi podělili :-). Polsko tak dostalo několik dokumentů o Enigmě z nihž vyplývala její konstrukce, obecná podoba kódových knih i způsob praktického požití Enigmy.

Ze začátku to nevypadalo na nijak potěšující informace. Operátoři Enigmy obdrželi každý měsíc novou kódovou knihu, která udávala klíč pro každý konkrétní den. Nejjednodušším způsobem jak užívat Enigmu by bylo šifrovat všechny zprávy příslušným denním klíčem. Bezpečnost takového postupu však oslabovalo samotné rozšíření Enigmy - denně se jí šifrovaly stovky zpráv. Pokud by se pro takové množství materiálu použil stejný klíč, usnadnila by se tím práce nepřátelským kryptoanalytikům. Lstivý Němci proto jako chytré dodatečné opatření zavedli pravidlo, že denním klíčem se šifruje pouze takzvaný klíč zprávy. V podstatě šlo o to, že si odesilatel a příjemce dohodly prostřednictvím deního klíče vlastní klíč pro svou zprávu. Kdyby Němci tento systém nepoužívali, pak by se celý denní provoz celé armády - patrně tisíce zpráv obsahujících miliony písmen - šifroval týmž klíčem. Když se však denní klíč používal jen k přenosu klíčů zpráv, šifrovalo se jím jen velmi malé množství textu.

V praxi tedy odesilatel nejprve zapojil kabely na propojovací desce a umístnil scramblery podle denního klíče. Poté nastavil i polohu scramblerů podle denního klíče na kód - řekněme QCW. Následně náhodně vybral novou kombinaci - řekněme PGH - kterou pak zašifroval podle denního klíče. Klíč zprávy do Enigmy zapsal dvakrát, aby vyloučil překlep, nebo jinou chybu (rušení při přenosu rádiem apod.). Zašifroval tedy PGHPGH a vyšlo mu například KIVBJE - všimněte si, že PGH se pokaždé zašifrovalo jinak, jednou jako KIV, podruhé jako BJE, protože scramblery se otáčely v průběhu šifrování a tím měnily jeho režim pro každý znak. Na straně příjemce se Enigma rovněž nastaví podle denního klíče. Po předepsaném příslušném zapojení propojovací desky a umístnění scramblerů se tedy nastaví taktéž kód QCW. Příjemce zapíše prvních šest písmen zprávy a čte PGHPGH. Mezitím už odesilatel změnil nastavení scramblerů na PGH a šifruje vlastní zprávu podle tohoto klíče. Příjemce nastaví své scramblery rovněž na PGH a dešifruje vlastní text zprávy. Jednoduché a účinné.

Na první pohled vypadá takový systém neproniknutelně, ale Poláci se nedaly zastrašit. Ve svém zoufalství byly připraveni prozkoumat každou cestičku, aby našly slabinu Enigmy i nedostatky celého systému. Konfrontováni se složitostí Enigmy a její mechanickou podstatou byli povolali do boje kryptoanalytiky zcela nového typu. Po staletí se mělo za to, že nejlepsími kryptoanalytiky jsou odborníci na strukturu jazyka, lingvisté s určitými statistickými znalostmi. Enigma však přinutila Poláky, aby toto stanovisko přehodnotily. Jelikož se jednalo o "mechanickou šifru", Biuro Szyfrow došlo k názoru, že lepší šance by proti ní mohly mít techničtěji orientované mozky. Mezi novými kandidáty byl i jistý Marian Rejewski - třiadvacetiletý mladíček s brýlemi, který studoval statistiku na Poznaňské univezitě a po jejím dokončení chtěl pracovat v pojišťovnictví. Na univerzitě měl dobré výsledky, patřil k nejnadanějším matematikům a protože pocházel z území které do roku 1918 patřilo Německu, mluvil i plynně německy. Biuro Szyfrow se pro něj nakonec stalo tím pravým působištěm a Enigma jeho největší výzvou. Pracoval zcela sám a veškerou svou energii soustředil na záludnosti Schreibiova přístroje. Pokusil se analyzovat z matematického hlediska všechny aspekty činnosti Enigmy, testoval účinky scramblerů a propojovací desky.

Jeho strategie vycházela ze staré známé skutečnosti, že opakování je nepřítelem bezpečnosti - umožňuje odhalit zákonitosti podle nihž systém pracuje a ty pak dovolí kryptoanalykům luštit šifrované zprávy. Nejnápadnějším opakováním byl v případě Enigmy samotný klíč zprávy,

CC-BY-SA Security-Portal.cz | secured by paranoid sense | we hack to learn

zašifrovaný vždy dvakrát na začátku každé první zprávy mezi oběma operátory Enigmy. Němci trvali na opakování, aby se vyhnuli chybám způsobeným překlepem nebo rádiovou interferencí. Nepředvídali však, že tím mohou ohrozit bezpečnost komunikace - rozhodně ne tolik, aby to hrálo nějakou podstatnou roli. Docela logicky považovaly Enigmu za naprosto bezpečnou - stejně jako všichini ostatní. To, že první a čtvrtý znak jsou zašifrováním téhož písmene (stejně jako druhý a páty, třetí a šestý), však Rejewskému umožnilo vyvodit drobná omezení týkající se denního nastavení přístroje. To se může zdát jako příliš mlhavé a neužitečné, protože tu zatím bylo plno jiných neznámých, ale alespoň to bylo něco. S každou další zachycenou zprávou toho dne totiž šlo identifikovat další vztahy mezi prvním a čtvrtým písmenem opakovaného klíče a tak když Rejewski dostal během jediného dne dostatek zpráv, mohl sestavit úplnou "abecedu vztahů", množinu vzájemných závislostí. A s tím už se dalo něco podniknout.

Rejewski neznal denní klíč ani neměl představu, jaký klíč zprávy operátor zvolil, ale věděl, že výsledkem je tato tabulka vztahů. Kdyby byl denní klíč jiný, potom by také tabulka vztahů byla naprosto jiná. Důležité bylo že existuje jistá souvislost, z níž by teoreticky bylo možné odvodit příslušný denní klíč. A tak Rejewski začal hledat v tabulce zákonitosti - struktury, které mohly denní klíč naznačit.

Počet možných kombinací byl příliš velký... ovšem převážná většina z nich byla dílem rozvodné desky. Díky znalosti funkce Enigmy a rozsáhlé analýze tabulek vztahů tak Rejewski mohl postupně identifikoval alespoň tu vlastnost řetězce, která byla výhradně důsledkem nastavení scramblerů, a oddělit ji od té kterou v Enigmě zajišťovala rozvodná deska. Takže místo toho, aby se trápil, který z 10.000.000.000.000.000 denních klíčů odpovídá určité sadě řetězců, se mohl soustředit na mnohem jednodušší problém: které z 105.456 nastavení scramblerů odpovídá pozorovanému počtu spojení v rámci sady řetězců? Toto číslo je stále ještě poměrně velké, ale také je zhruba sto miliardkrát menší než celkový počet možných denních klíčů. Jinými slovy, náročnost úkolu by tím poklesla o řád sta miliard (!). Rejewsky tedy katalogizoval řetězce, které byly každým nastavením generovány. Dokončit katalog mu sice zabralo celý rok, ale jakmile nashromáždil všechna data, prakticky už mohl dešifrovat Enigmu. Když totiž identifikoval scramblerovou (polyalfabetickou) část denního klíče, zbývalo jen odhalit nastavení propojovací desky. Ačkoli mu sice zbylo něco kolem sta miliard možností, byl to už poměrně jednoduchý úkol, protože šlo o prostou monoalfabetickou šifru, řešitelnou obyčejnou frekvenční analýzou - tedy postupem známým již něco přes devět staletí.

Navíc tu ani nešlo o úplnou monoalfabetickou substituční šifru, neboť se substituce týkala pouze šesti párů písmen. Po katalogizování řetězců tedy Rejewsky nastavil scramblery podle zjištěné scramblerové části denního klíče. Potom odstranil všechny kabely z propojovací desky, aby neměla na šifrování žádný vliv. Nakonec vzal část zachycené zprávy a naťukal ji do přístroje. Výsledkem byla převážně jakási hatmatilka, protože správná kabeláž propojovací desky byla zatím neznámá. Ale zhruba polovina znaků byla čitelná a tak se poměrně často objevovali mlhavě rozeznatelné věty jako třeba plijedtedobelrina - což velmi pravděpodobně mohlo znamenat "přijeďte do Berlína". A tím byla vlastně celá záležitost vyřešena - analýzou vět pak bylo možné identifikovat další písmena, jež je třeba vzájemně prohodit pomocí propojovací desky. Když se takto podařilo určit nastavení celé propojovací desky při známém nastavení scramblerů, měl Rejewsky k dispozici úplný denní klíč - mohl rozšifrovat jakoukoliv zprávu zaslanou toho dne.

Z hlediska kryptoanalýzi šlo o obdivuhodný úspěch. Za jeho provedením se sice skrývala celý dlouhý rok práce, ale původně se předpokládalo, že ověřit každý možný klíč k Enigmě by zabralo delší dobu, než je celkové stáří vesmíru. Rejewski strávil sestavováním svého katalogu řetězců "pouhý" rok. Poté již mohl najít denní klíč téhož dne, kdy jej nepřítel začal používat. A jakmile měl denní klíč, disponoval stejnou informací jako zamýšlený příjemce, a tak mohl zprávu snadno dešifrovat. Polský národ se tak náhle stal kryptoanalytickou velmocí - Marian Rejewsky se svými kolegy po velkou část 30. let 20. století měsíc po měsíci, rok po roku dešifroval nekončící přísun zašifrovaných odposlechů. Když Němci učinily malou změnu ve způsobu vysílání zpráv a jeho starý katalog řetězců byl k ničemu, namísto toho aby dával zdlouhavě dohromady druhý, raději sestavil jeho mechanickou verzi, která automaticky vyhledávala správná nastavení scramblerů. Rejewského vynález byl vlastně kryptoanalytickou adaptací kryptografické Enigmy, strojem který byl schopen rychle prověřit každé z 17.576 nastavení, dokud nenarazil na to správné. Protože existovalo šest různých uspořádání scramblerů, bylo potřeba šest Rejewského přístrojů pracujících paralelně. Každý z nich představoval jedno z šesti možných uspořádání a dohromady tvořily jednotku, která byla asi metr vysoká a

dovedla najít denní klíč zhruba do dvou hodin. Říkalo se jim Bomby (jméno mohlo narážet na hlasitý tikot, který vydávali, když prověřovali nastavení scramblerů, jiná verze však říká, že Rejewsky dostal nápad postavit toto zařízení když v kavárně jedl "bombu" - zmrzlinu ve tvaru polokoule).

V rozhodujícím okamžiku však dostalo Polsko ránu pod pás - v prosinci roku 1938 němečtí kryptografové (bez nějakého zvláštního důvodu, prostě jen v rámci válečných příprav) zvýšili bezpečnost Enigmy. Všechny přístroje byli vybaveny dvěma dalšími scramblery. Předtím byly k dispozici tři scramblery se šest způsoby jejich uspořádání. Nyní, když přibily další dva počet uspořádání vzrostl na 60. Následující měsíc se situace ještě zhoršila, když Němci zvýšili počet kabelů propojovací desky ze šesti na deset. Místo dvanácti písmen, která se měnila před vstupem do scramblerů, se jich nyní měnilo dvacet. Počet možných klíčů tím vzrostl na 159.000.000.000.000.000.000.

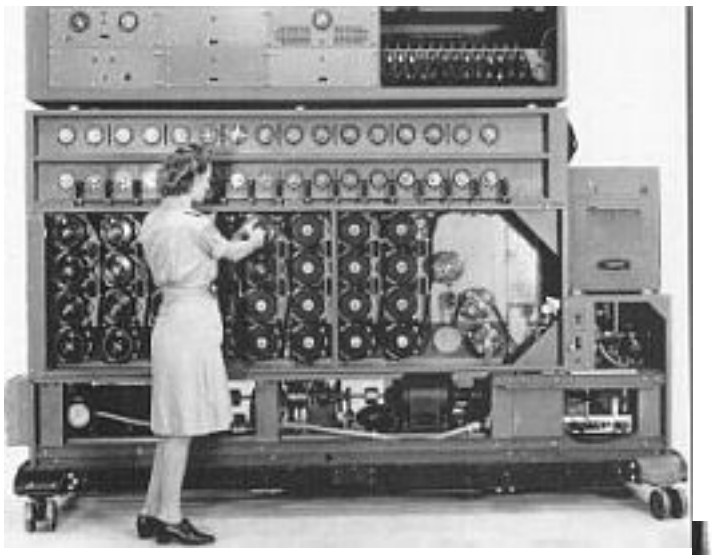
Hlavním problémem nicméně opětovně nebylo prosté navýšení všech kombinací, ale především vyšší počet uspořádání scramblerů, ke kterému by bylo potřeba postavit desetkát více Bomb. Náklady potřebné k vybudování takovéto baterie však patnáctinásobně převyšovaly roční rozpočet celého Biura. V roce 1938 tedy dosáhly dovednosti Poláků v odposlechu a dešifrování svého vrcholu, ale začátkem roku 1939 posílení bezpečnosti Enigmy zcela zarazilo tok jejich kryptoanalytických špionážních informací. Rejewski sice dokázal, že Enigma není nerozlomitelná šifra, ale bez prostředků nutných k prověření každého nastavení scramblerů zkrátka nemohl dost rychle najít denní klíč - složitost systému byla příliš velká, kryptoanalytický postup příliš pracný a časový interval příliš krátky. Dešifrování bylo za těchto podmínek skutečně nemožné.

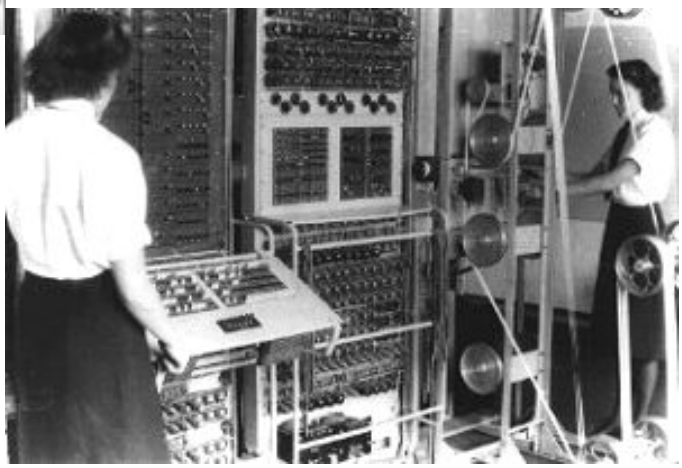
Nová nezranitelnost Enigmy byla pro Polsko zdrcujícím úderem, protože Enigma nebyla jen prostředek komunikace, ale také klíčový prvek Německé strategie. Samotná koncepce bleskové války vyžadovala bezpečnou, rychlou a snadnou komunikaci kvůly nutnosti koordinace nezávisle operujících, rychlých a mobilních sil. A přesně tím bylo pro německou armádu rádio spojené s Enigmou. Pokud Poláci nemohli přijít Enigmě na kloub, vpodstatě neměli naději, že by se svou archaicky organizovanou armádou mohli zastavit moderní německou válečnou mašinerii. Dobře to však věděly a také věděly, že jim schází čas - do zahájení útoku už zbývalo jen několik měsíců a za tu dobu s tím už zkrátka nešlo nic udělat.

Pokud však Polsko nemohlo mít užitek z Rejewského práce, potom ji měli mít možnost využít jiní. 24. června 1939 vedoucí francouzští a britští kryptoanalytici dorazili do ústředí Polských kryptoanalytiků, aniž by věděli, co je čeká. Zpravodajský důstojník je uvedl do místnosti, ve které stál objekt zakrytý černou látkou. Důstojník látku stáhl a tak dramaticky odhalil jeden z Rejewského přístrojů. Publikum užaslo, když slyšelo, jak Rejewski po léta luštil Enigmu. Poláci byli o deset let popředu před kýmkoli jiným na světě, Američany a Brity nevyjímaje. 1. září 1939 Hitler vpadl do Polska a nejstrašnější válka v dějinách lidstva začala.

Díky Rejewskému britští kdyptoanalytici přesně věděli, co je k porážce Enigmy potřeba a britské nejvyšší politcké a vojenské vedení si okamžitě uvědomilo důležitost zpravodajských informací, které jim kryptoanalýza Enigmy mohla poskytnout. Kryptoanalýza Enigmy se okamžitě stala prioritní záležitostí a tak se jí dostalo i přiměřené - tedy prakticky neomezené - podpory. Britská kancelář č.40 byla sice jako většina ostatních ovládána lingvisty, ale rychle začalo hledání vhodných matematiků kteří by doplnily jejich tým. Byla založena nová cenrála v hrabství Buckinghamshire, v Bletchley Parku, budově tzv. Government Code and Cypher School (GC&CS), která mohla poskytnout prostor daleko více pracovníkům, neboť se (v důsledku masivního rozšíření rádia) očekával nesrovnatelně větší příliv šifrovaných depeší než tomu bylo v první světové válce. Do GC&CS byli přepraveno i několik exemplářů Rejewského Bomb a kompletní dokumentace. Během podzimu 1939 si vědci a matematici v Bledchley osvojili techniku Poláků a s ohledem na objem materiální podpory byli schopni Enigmu brzy prolomit.

CC-BY-SA Security-Portal.cz | secured by paranoid sense | we hack to learn





1. května 1940 Němci změnily svůj protokol výměny klíčů a přestali opakovat klíč zprávy, což bylo ústředním prvkem Rejewského metody prolomení Enigmy. Britové však podobný krok očekávaly již dříve a byli na něj dobře připraveni - jistý Alan Mathison Turing vyšel z vypozorovaného opakování určitých řetězců ve zprávách samotných - typicky například slova wetter (počasí) v předpovědi meterologické situace, kterou Němci vysílaly každodenně po šesté hodině ranní. V jeho hlavě také vznikla myšlenka "univerzálního stroje", která později vedla ke stroji zvanému Colossus - prvnímu programovatelnému počítači, který byl složen z 1500 elektronek, které byly mnohem rychlejší než pomalá elektromechanická relé používaná v Bombách. Zlomena tak nakonec byla nejen dokonalejší námořní verze Enigmy, ale i šifrovací systém německého nejvyššího velení - Lorenz SZ40. Nastala nová éra kryptografie a kryptoanalýzi. Technologie aplykovaná kryptografy vyprovokovala kryptoanalytiky k nasazení ještě mocnějších pomocníků. Z nich se nakonec vyvinuly první programovatelné počítače a díky nim společnost pomalu vstupovala do informačního věku.

Zrození elektronických šifer - DES, AES

Šifrování pomocí počítače se v zásadě příliš neliší od tradičních forem šifrování. Jsou tu jen tři základní rozdíly, z nihž principielně hraje roli jen jeden. První rozdíl spočívá v tom, že jakýkoliv mechanický šifrovací přístroj je limitován svou fyzickou podobou, která nevyhnutelně podléhá jistým omezením a je poněkud nepružná co se týče změn, zatímco (programovatelný) počítač pracující na elektronickém základě může po funkční stránce napodobit šifrovací přístroj téměř libovolné velikosti i složitosti a okamžitě poté přejít k napodobení zcela jiného šifrovacího přístroje o naprosto jiných charakteristikách. Druhý rozdíl je v rychlosti, protože elektronika obecně pracuje mnohem rychleji, než mechanická zařízení. Počítač naprogramovaný kupříkladu k napodobení přístroje Enigma tak dokáže zašifrovat srovnatelně dlouhou zprávu ve zlomku času, který by k tomu potřebovala skutečná Enigma.

Třetí a asi nejdůležitější rozdíl spočívá v tom, že počítač šifruje ve skutečnosti čísla, nikoliv písmena abecedy. Počítače totiž pracují s binárními čísly (binary digits - zkráceně bits) - s posloupností

CC-BY-SA Security-Portal.cz | secured by paranoid sense | we hack to learn

jedniček a nul. Před šifrováním se proto každá zpráva musí nejprve převést do jedniček a nul. To lze provést podle různých protokolů, jako je například ASCII (American Standard Code for Information Intercharge), ale nám pro základní orientaci postačí, když si binární čísla představíme jako posloupnost jedniček a nul, která jednoznačným způsobem určuje každé písmeno, stejně jako Morseova abeceda určuje každé písmeno jednoznačnou sérií teček a čárek.

I když pracujeme s počítači a čísly, nikoliv s přístroji a písmeny, probíhá proces zašifrování v zásadě stále stejně jako za starých časů, a to na základě principu substituce a transpozice, při kterých se prvky zprávy buď nahrazují jinými znaky, nebo se mění jejich pozice, případně probíhají obě tyto změny najednou. Každé zašifrování, i to nejsložitější, lze rozdělit na tyto dvě jednoduché operace. Jedinečným aspektem počítačového šifrování je snad pouze možnost práce na úrovní binárních čísel, tedy jakoby uvnitř písmene.

Právě této možnosti využíval i jeden z nejsilnějších poválečných šifrovacích nástrojů - šifrovací systém Lucifer německého emigranta Horsta Feistela, který vznikl na počátku 70. let 20. století v laboratořích IBM. Lucifer je poměrně složitý systém a tak si jeho fungování vysvětlíme jen velmi zjednodušeně. Představte si, že máte zprávu zapsanou řetězcem bitů. Tento řetězec nejdříve rozdělíte na větší množství bloků o určité velkosti. Tyto bloky pak rozdělíte na poloviny, které budete šifrovat samostatně. Jednu polovinu z každého bloku zašifrujete kombinací transpozice a substituce, podobně jako například u německé šifry ADFGVX, ovšem s každým bitem budete zacházet jako se samostatným znakem. K zašifrované části přičtete (neboť je to vpodstatě číslo) nezašifrovanou polovinu bloku. Tím dostanete malý fragment šifrového textu v binárních číslech. Obdobným, ale obráceným postupem zašifrujete i druhou polovinu bloku, u kterého rovněž zkombinujete transpozici se substitucí a nakonec výsledek sečtete s binárním zápisem otevřeného textu první části bloku. Celý proces se nakonec ještě několikráte zopakuje na úrovni bloků. Přesné podrobnosti této "bláznivé míchanice" se mohou měnit a jsou to právě ony, které tvoří klíč, na základě něhož bude zpráva opětovně dešifrována a to přesně opačným postupem (stejně jako u každé jiné šifry se kterou jsme se zatím seznámily). Celý proces vypadá složitě, protože jednoduše složitý také je. Lucifer využívá nejklasičtějších šifrovacích technik, ale díky propojení s moderní výpočetní technikou je dokáže zkombinovat v takové složitosti, ve které je pro kryptoanalytika nesmírně obtížné najít nějaké zákonitosti a souvislosti, které by mohl použít k průlomu, obdobně jako to udělal například Rejewsky v případě Enigmy, nebo jak tomu můžeme udělat u vícenásobně použíté tablkové šifry.

V době svého vzniku byl Lucifer považován za jeden z nejsilnějších komerkčně dostupných šifrovacích produktů a proto jej používalo mnoho různých organizací. Když elektronické šifrování postupně začalo pronikat i do civilní sféry zdálo se být nevyhnutelné, že právě tento systém bude přijat jako americký standard. Síla Lucifera však představovala problém pro NSA (National Security Agency), která nechtěla pro veřejné použití schválit zádný šifrovací standart, který by nedokázala sama prolomit. Nakonec se našlo vskutku šalamounské řešení - NSA lobbovala ve prospěch omezení maximálního počtu klíčů Lucifera, tak aby jej byla sama schopna prolomit svou hrubou silou. Argumentovala tím, že takový klíč by běžné společnosti měl poskytnout dostatečnou bezpečnost, protože žádná civilní organizace tehdy neměla dostatečně výkonný počítač, schopný prověřit všechny klíče "lobotomizovaného" Lucifera v rozumném čase - narozdíl od NSA, která by díky svému přístupu k nejmodernější výpočetní technice takové zprávy v "případě potřeby" ještě byla schopna vyluštit. 56-bitová verze Feistlerova Lucifera tedy byla 23. listopadu 1976 oficiálně převzata jako americký šifrovací standart a označena DES (Data Encryption Standart), což vyřešilo problém standaritizace kryptografie v civilním sektoru a podpořilo velké firmy, aby k zajištění bezpečnosti svých informací používaly šifrování. Logicky však bylo jen otázkou času kdy bezpečnost DES přestane s ohledem na stoupající výkon hardwaru vyhovovat. Došlo k tomu dříve než se původně očekávalo - již v letech 1998-1999 proběhlo několik demonstrativních luštících akcí, které vážně podlomily důvěru v DES. Nejvážnějším ohrožením se ukázalo být propojení většího množství počítačů prostřednictvím internetu a využití jejich společného výkonu k prolomení jediné šifry. Od roku 2002 proto úlohu DES nahrazuje nový standard AES (Advaced Encryption Standard). I jeho prolomení je však považováno jen za otázku času - dříve nebo později technologie poskytne prostředky které umožní prolomení AES obyčejnou hrubou silou.

Kryptografie a asymetrickým klíčem - DHM, RSA, PGP

Problém distribuce klíčů trápil kryptografy po celá staletí. Postupně však nabíral na důležitosti, až se v 70. letech 20. století stal nejvážnějším problémem celé kryptografie. Již během druhé světové války muselo například německé vrchní velení distribuovat měsíční knihu denních klíčů všem operátorům Enigmy, což byl ohrommý logistický problém, nehledě na s tím spojená bezpečnostní rizika. Také ponorky, které trávili mnoho času mimo základnu, musely pravidelnou dodávku klíčů obdržet. Vládní organizace a vojenské kruhy se nicméně s problémem distribuce klíčů dokázaly do určité míry vyrovnat už jen díky pouhému objemu prostředků který měly k dispozici - jejich zprávy byli často tak důležité, že pro distribuci klíčů byli odesilatelé připraveni udělat doslova cokoliv, včetně distribuce kódových knih a jednorázových tabulkových šifer. S příchodem informačního věku se však problém distribuce klíčů stal nejvýznačnějším problémem celé kryptografie. Distribuce klíče nebyla v elektronickém světě počítačů jen nepohodlná, mohla se stát pro šifru i největším bezpečnostním problémem, bez ohledu na to jak byla sama šifra dobrá. Dilema soukromého sektoru bylo zjevné - jestliže vláda přes všechny své vynaložené prostředky těžce zápolila, aby zajistila bezpečnou distribuci klíčů, jak mohly civilní společnosti dosáhnout spolehlivé distribuce, aniž by zbankrotovali?

Navzdory převládajícímu názoru, že distribuce klíčů je neřešitelný problém, zanícení specialisté jdoucí proti všem zažitým předpokladům opětovně zvítezily. Přestože počítače změnily implementaci šifer, největší revolucí v kryptografii 20. století byl vývoj metod, které překonaly problém distribuce klíčů. Tento průlom je považován za největší kryptografický úspěch od vynálezu monoalfabetické šifry před dvěma tisíci lety.

Jak k tomu došlo? Začněme jednoduchou analogií. Představme si, že chcete příteli cosi poslat, aniž by to mohl spatřit kdokoliv jiný. Klasické řešení v rámci kryptografie by vypadalo asi nějak tak, že vezmete velkou, pevnou bednu s masivním zámkem a dvěma k němu náležejícímu klíči. Jeden z klíčů pak předáte svému příteli např. při nějakém osobním setkání které odeslání předchází (distribuce klíčů). Svou zásilku pak jednoduše vložíte do oné velké pevné bedny, tu zamknete svým klíčem a poté odešlete standartními kanály. Váš přítel ji po doručení bude moci odemknou dvojčetem vašeho klíče, zatímco nikdo jiný nemůže vaši zásilku otevřít, protože prostě nemá klíč který existuje jen ve dvou exemplářích, z nihž jeden vlastní legitimní příjemce a druhý legitimní odesilatel. Samozřejmě můžeme spekulovat o tom, že lze rozbít celou bednu, nebo zámek vypáčit, ale obojí je poměrně namáhavé - jedno vyžaduje velkou "hrubou sílu" a druhé zas velkou odbornost. Rozbíjení beden a zámků je tedy zhruba stejné jako rozbíjení kódů, celá zásilka je relativně dobře zabezpečena, obdobně jako při šifrování. Stejně tak ovšem problém nastává, když nemáte možnost si mezi sebou klíče bezpečně předat.

Představme si ale, že na oné transportní bedně není žádný pevný zámek, ale jsou tam místo toho dva páry ok pro dva vysací zámky: odesilatel vloží zprávu do bedny, zamkne ji vlastním vysacím zámkem a odešle příjemci. Příjemce dostane zásilku, avšak nemá odesilatelův klíč, takže nemůže bednu otevřít a zprávu skutečně přijmout. Vezme však svůj zámek a zamkne jím bednu podruhé. Takto zabezpečenou bednu se dvěma zamčenými zámky pak pošle zpátky původnímu odesilateli. Ten bednu přijme, odemkne svůj zámek, sejme ho a zamčenou bednu opět vrátí příjmci, zabezpečenou pouze jeho vlastním zámkem, jehož klíč si příjemce pochopitelně ponechal... Došlo tedy k výměně zabezpečené zprávy bez výměny klíče, respektive klíčů - odesílána byla jen zpráva zamčená v bedně, zajištěné jedním či dvěma zámky.

Metoda distribuce klíčů na tomto základě byla nazvaná podle iniciálů svých objevitelů DHM (Diffie-Hellman-Merkle) a vešla ve známost v červenci 1976. Byla obrovským skokem dopředu, neboť popřela axiom, dogma platné dva tisíce let. Měla však hned několik základních nedostatků.

Prvním, nikoliv bezvýznamným, avšak v žádném případě nejzávažnějším z nich byla ta skutečnost, že "šifry nejsou zámky" a proto nemají zcela identické vlastnosti - zatímco zámky jsme vedle sebe mohly bez problémů umístnovat paralelně, šifrování probíhalo až dosud sériově - problémem je tu zkrátka pořadí šifrování a dešifrování, neboť u většiny šifer musíme dodržovat pravidlo "jako první dovnitř, jako poslední ven". Jinými slovy poslední krok dešifrování musí odpovídat prvnímu kroku šifrování. Důležitost pořadí je snáze pochopitelná, pokud si ji ukážeme na něčem všedním - pokud si například oblečeme ponožky a následně obujeme boty, nemůžeme poté sundat ponožky aniž bychom si nejdříve nezuly boty - opětovně se musíme řídit pravidlem "jako první dovnitř, jako poslední ven". Tento problém se nicméně později podařilo vyřešit nalezením šifer u nihž na pořadí

vzájemného šifrování a dešifrování nezáleží.

Druhým problémem byla skutečnost, že podobný postup s sebou někdy nese i jisté problémy, ke kterým by zas jindy nemohlo dojít. Nejznámnější z nich je schéma útoku zvané Man-in-the-middle-attack (tzn. zhruba "útok muže uprostřed"). Jde vlastně o velmi jednoduchý způsob jak proniknout do komunikace prostřednictvím podvržené zprávy. Vraťme se k naší analogii s bednou a představme si, že zásilku na její cestě mezi oběma legitimními adresáty zachytí třetí strana která bude mít obecné povědomí o způsobu jakým komunikace mezi objema adresáty probíhá. Nebezpečí spočívá v tom, že tato strana se nyní nachází v naprosto stejně pozici jako legitimní příjemce (!) - sice sama nemá klíč od zámku odesilatele, kterým je zásilka zabezpečena, ale přesto může zprávu získat. Protivník který zásilku zachytí jednoduše umístní na bednu vlastní zámek a pošle ji zpět odesilateli. Odesilatel vidí to samé, co by viděl v případě, kdy by vše šlo přesně podle plánu - bedna je zabezpečena dvěma zámky, z jihž jeden je jeho a on od něj má klíč. Pravděpodobně tedy sejme svůj zámek a pošle bednu stejnou cestou k příjemci, aniž by si uvědomil, že jediný zámek, který nyní zabezpečuje zásilku, není zámkem legitimního příjemce, ale zámkem protivníka. Ani tento problém ovšem není neřešitelný - jeho řešení je víceméně zjevné - odesilatel zprávy musí být schopen rozpoznat zámek (šifru) příjemce, ikdyž ji sám není schopen dešifrovat.

Dalším problémem systému DHM byla jeho zdlouhavost a nepohodlnost - jak vidíme už na příkladu se zámky, zatímco klasická šifrovaná zpráva překonává cestu k příjemci jen jednou a je také jen jednou šifrována a dešifrována, při systému DHM zpráva překoná vzdálenost mezi příjemcem a odesilatelem hned třikrát a je jí také nutno dvakrát zašifrovat a dvakrát dešifrovat. Tato skutečnost by pravděpodobně byla zásadním problémem ve všech obdobích před vynalezením telegrafu. V době informačního věku, kdy existuje telegraf, rádio a internet však nejde o problém zásadní a nepřekonatelný.

Žádný z problémů spojených se systémem DHM ve skutečnosti nebyl neřešitelný - problém distribuce klíčů se jím podařilo překonat, ačkoliv nalezené řešení nebylo právě tak pohodlné a pohotové jako klasické šifrování a vyžadovalo i určitá, dosud neobvyklá bezpečností opatření. Nakonec se ale objevila jiná, daleko praktičtější metoda která jej odsoudila téměř až k bezvýznamnosti.

Vraťme se k naší analogii se zámky a představme si nyní, že oba účastníci navrhnou svůj vlastní, jedinečný zámek a k němu náležející jedinečný klíč, následně vyrobí potřebný počet kopií tohoto zámku a samostatně je rozešlou běžnými kanály všem s nimiž by v budoucnu mohli chtít zabezpečeně komunikovat. Oba účastníci tedy mají vlastní klíč a jeden z mnoha (vzájemně identických) zámků toho druhého. Pokud si nyní chtějí něco sdělit, je postup velmi jednoduchý - odesilatel vezme onu velkou, masivní bednu, vloží do ní zprávu a zacvakne na ní zámek příjemce. Zacvaknutí jeho zámku nevyžaduje klíč, ani nic neprozrazuje o tom, jak zámek otevřít. Sám odesilatel od tohoto okamžiku nemůže bednu otevřít - to může pouze ten, kdo má jedinečný klíč náležející k danému zámku a ten existuje pouze v jediném exempláři, který má - jak se dá očekávat - jen sám příjemce. Ten po přijetí zásilky jednoduše vezme svůj klíč a odemkne jím svůj zámek. Obdobným postupem může sám poslat zásilku komukoliv jinému za použití jeho zámku. Vlastní zámky přitom není třeba nijak chránit, je je naopak žádoucí distribuovat v co nejširším měřítku (dalo by se sice argumentovat tím, že zámek lze rozebrat a podle něj pak vyrobit příslušný klíč, ale to je jednak daleko obtížnější než odemikání a zamikání - tzn. jde vpodstatě o řešení hrubou silou - a druhak můžeme samotný zámek vybavit něčím ve smyslu autodestrukčního zařízení, které takovéto alternativě zabrání). Chránit je nutné pouze vlastní klíč.

Jak tedy vidíme, může být distribuce klíčů vyřešena prakticky se stejnou mírou pohodlí jako v případě klasického šifrování - zpráva překonává vzdálenost mezi odesilatelem a příjemcem jen jednou, jednou je takéž zašifrována i dešifrována a její bezpečnost závisí jen a pouze na typu použité šifry. Distribuci klíčů (která představuje mj. i bezpečnostní riziko) se lze vyhnout, distribujeme-li "zámky". Problém útoku typu Man-in-the-middle-attack tu sice v určité míře zůstal zachován, ale v daném případě už jej nešlo využít k přímému získání odeslané zprávy, nebyl dlouhodobě udržitelný a také jej bylo možné relativně snadno vyřešit ověřením identity odesilatele prostřednictvím např. digitálního podpisu (viz. dále).

Tento systém šifrování se kterým přišla v roce 1977 trojice vědců z MIT (Massachusetts Institute of

Technology), se nazývá RSA (Rivest, Shamir, Adlerman) a zcela nahradil původní koncepci DHM. I on ovšem vypadá velmi jednoduše je-li vysvětlen v pojmech zámků, nebylo však ani zdaleka snadné najít způsob jak původní myšlenku realizovat. To co bylo potřeba byl především onen "zámek" který je by sice bylo jednoduché "zacvaknout", ale naopak obtížné odemknout bez klíče - tedy šifra kterou je snadné zašifrovat, ale obtížné dešifrovat bez určité speciální vědomosti (dešifrovacího klíče).

Všechny šifry, kterými jsme se až dosud seznámili vyžadovali bezpečnou distribuci klíčů především proto, že byli symetrické - tzn. jejich dešifrování probíhalo stejným způsobem jako samo šifrování, šifrovací klíč odpovídal dešifrovacímu. U asymetrického šifrování toto odpadá, neboť šifrovací klíč neodpovídá dešifrovacímu, nic o něm nevypovídá a není jej tedy nutné nijak zvlášť chránit - lze jej naopak bez obav distribuovat všem okolo, bez jakýchkoliv bezpečnostních opatření. V tajnosti je třeba zachovat pouze vlastní dešifrovací klíč, o který se ovšem příjemce s nikým nemusí dělit.

Všechny formy šifrování (natož pak ty elektronické) můžeme v zásadě pokládat za funkce - matematické operace, které jednomu číslu přiřadí číslo jiné (například "zdvojnásobení" je funkce, protože číslu 3 přiřadí číslo 6), na základě určité zákonitosti mění znak po znaku otevřeného textu ve znaky textu šifrového. O počítačovém šifrování je velmi snadné uvažovat jako o funkcích, protože jak už jsme si řekly, všechny zápisy v počítači jsou realizovány čísly. A tak se v podstatě hledala jednosměrná matematická funkce, která by vykonala stejnou práci jako onen snadno zamikatelný, ale obtížně odemykatelný zámek - něco co by šlo využít ve skutečném kryptografickém systému. Hledala se matematická funkce kterou by za normálních podmínek nešlo invertovat, taková, která by k tomu potřebovala určitý objem speciálních dat (klíč).

Většina matematických funkcí je obousměrná, protože je lze jednoduše obrátit (invertovat). Například zdvojnásobení je oboustranná funkce, protože je stejně jednoduché zdvojnásobit číslo jako dostat ze zdvojnásobeného čísla to původní - pokud víme, že výsledek zdvojnásobení je 26, je triviální odvodit, že původní číslo bylo 13. Jednosměrné funkce je naopak těžké obrátit - obousměrné funkce jsou zkrátka vratné, jednosměrné nikoliv. Existuje však oblast matematiky která je na jednosměrné funkce velmi bohatá - modulární aritmetika (nebo-li také hodinová matematika). V modulární aritmetice pracuje matematik s konečnou množinou čísel uspořádaných do kruhu, což připomíná čísla na ciferníku hodin. Pokud například k 10 hodinám přičteteme čtyři hodiny, modulární výsledek není 14, ale 2. Funkce v modulární matematice se tak mnohdy chovají nevypočitatelně, což z nich za určitých okolností dělá jednosměné funkce. Vezměme si náš modulárním součet 10+4=2 - známe-li výsledek (2) a jedno ze sečítaných čisel (kupříkladu 10), příliš toho ještě nevíme o druhém čísle, neboť jím sice bylo číslo 4, ale podle toho co víme jím stejně tak dobře mohla být kupříkladu i čísla 16, 28, 40, 52, 64, 76, 88, 100, 112, 124, 136... a celá řada dalších čísel. Modulární funkce nám tak neposkytne mnoho užitečných nápověd, inverze funkcí je daleko těžší a jednoznačný výsledek nejsme schopni s jistotou získat bez testování všech hodnot které by jím mohly být. Po určitém čase samozdřejmě nevyhnutelně musíme dospět k výsledku, ale jde o řešení "hrubou silou", což může být při šifrování z praktického hlediska zcela bezvýznamné, neboť obdobně jako tomu bylo například u Enigmy, pokus o takové otrocké řešení hrubou silou by nám mohl zabrat čas delší, než je nám dosud známé stáří vesmíru. V daném případě platí, že je-li hodnota dostatečně velká, je prakticky nemožné k ní dospět v nějakém rozumeném časovém intervalu, nebo z ní něco odvodit. Pokud známe klíč, je naopak dešifrovní otázkou okamžiku.

Bylo tedy jasné, že to co funguje v teorii na "zámkové analogii", může fungovat i prakticky. Dále se už hledal jen ten nejlepší způsob provedení. Základem se stala prvočísla - tedy čísla která nemají jiné dělitele než číslo 1 a sebe sama (např. číslo 7 které nelze bezezbytku dělit jinými čísly než je 1 a 7). Postup je asi takový, že příjemce vybere svá prvočísla, například p=17.159 a q=10.247. Jejich vynásobením mezi sebou pak dostane N = 175.828.273. Toto N se stane jeho veřejným šifrovacím klíčem, který může tisknout na své vizitky, publikovat na internetu nebo zveřejnit v seznamu veřejných klíčů spolu s hodnotami N kohokoliv dalšího. Když mu někdo jiný chce zašifrovat zprávu, najde si jeho hodnotu N, tedy číslo 175.828.273, a potom ji vloží do obecné podoby jednosměrné funkce, která je také veřejně známa. Tím odesilatel získá jednosměrnou funkci konkretizovanou veřejným klíčem příjemce. Do ní vloží zprávu, zapíše výsledek a pošle jej příjemci. Od okamžiku zašifrování je zpráva bezpečná, protože ji nikdo kromě příjemce není schopen dešifrovat - byla zašifrována jednosměrnou funkcí, k jejímuž invertování je třeba znát informace - hodnoty p a q - kterými disponuje pouze příjemce. Každý kdo by chtěl zjistit hodnotu p a q by musel nejprve vypočítat která čísla by bylo mutno vynásobit, aby výsledek byl N - což je proces který se nazývá

CC-BY-SA Security-Portal.cz | secured by paranoid sense | we hack to learn

faktorizace a je nesmírně náročný - a poté by je musel každou variantu vyzkoušet. Je-li hodnota N dostatečně velká, je tedy dešifrování prakticky nemožné - pokud by například bylo použito N o délce 10130, počítači s procesorem 100 MHz Intel Pentium a s 8 MB RAM by sama faktorizace zabrala 50 let. Protože však vždy existuje možnost, že někdo použije k dešifrování daleko výkonější počítač, nebo propojí větší množství počítačů, doporučuje se používat pro důležité bankovní transkakce N větší než 10(na)308. Běžnou praxí je nicméně používat N tak vysokou, že by veškeré počítače na zeměkouli potřebovali k rozlomení šifry delší čas než dosud známý čas vesmíru.

Je ovšem známo, že výkon počítačového hardware stále roste. Rychlost křemíkových čipů se údajně zdvojnásobuje každých 18 měsíců. Teoreticky tedy šifra RSA nemusí být dlouhodobě bezpečná. Ve skutečnosti ovšem prozatimní rychlost výkonostního růstu hardware nestačí - stejný proces který urychluje kryptoanalýzu totiž urychluje i kryptografii a tak lze současně s růstem výkonu zvyšovat i N a současný vývoj výkonu hardware byl prozatím vcelku předvídatelný. K ohrožení šifry RSA by zkrátka bylo třeba překvapivého skoku. Za největším riziko RSA je však považováno něco zcela jiného a to možnost, že by v budoucnu někdo přišel na rychlý způsob faktorizace. Od toho okamžiku by byla RSA v její současné podobě nepoužitelná. Matematici nicméně takovou zkratku hledají už několik tisíc let a zatím se jim to příliš nedaří. Faktorizace zůstává velmi náročným procesem a většina matematiků se domývá, že to plyne jaksi z podstaty věci a že existuje nějaká matematická zákonitost, která takovou zkratku nepřipouští. Prozatím se zdá, že mají pravdu.

Proces šifrování pomocí RSA byl bezpečný a řešil problém distribuce klíče. Vyžadoval však velký početní výkon, který měly na počátku 80. let k dispozici jen velké komerkční firmy a vládní organizace. Phill Zimmermann se domýval, že v informačním světě, v němž je (narozdíl od toho "fyzického") neskutečně snadné cizý zprávy ve velkém měřítku zachycovat a analyzovat pomocí klíčových slov, by měly kvalitním šifrovacím systémem disponovat i širší masy - tedy veřejnost. Přišel proto s vlastním projektem PGP (Pretty Good Privacy - "Docela Dobré Soukromí"). Jeho hlavním cílem bylo zrychlit proces šifrování pomocí RSA. Aby urychlil šifrování a dešifrování, použil elegantní trik, kdy spojil asymetrické šifrování RSA se staromódním symetrickým šifrováním. Tradiční symetrické šifrování totiž může být stejně bezpečné jako asymetrické a je rychlejší na provedení. Jeho problémem je pouze distribuce klíče. A právě tady mu přichází na pomoc RSA, protože ji lze použít k zašifrování symetrického klíče. Zimmermann navrhl šifru známou jako IDEA (která je do jisté míry podobná DES) a vyvinul uživatelsky přívětivý software který využije systému RSA k distribuci klíče. Proces vypadá v jednoduchosti tak, že první zpráva obsahuje zároveň otevřený text zašifrovaný šifrou IDEA a klíč k jejímu dešifrování, zašifrovaný asymetrickou šifrou typu RSA.

Do PGP byl rovněž implementován digitální podpis. Ten vychází z principu který vyvinuly už autoři DHM, když si uvědomily, že systém veřejných a soukromých klíčů by bylo mozné využít i obráceně - soukromý klíč k šifrování a veřejný k dešifrování. Takový způsob použití sice není přínostný z hlediska utajeného přenosu zpráv, protože zprávu dokáže pomocí veřejného klíče dešifrovat kdokoliv, ale je naopak bezpečným způsobem jak ověřit autorství, protože ji může zašifrofat jen ten, kdo má k dispozici soukomý klíč. Pokud se použijí obě možnosti, zaručí DHM i RSA jak soukromí, tak i autorství.

Do léta 1991 byl Zimmermann na dobré cestě udělat z PGP skvělý komerkční produkt. Byli tu pouze dva problémy, z nichž ani jeden neměl technickou podstatu. Prvním problémem byla skutečnost, že RSA, tvořící jádro PGP byla patentovaným produktem a patentový zákon vyžadoval, aby Zimmermann obdržel licenci od RSA Data Security Inc., než PGP uvede na trh. Zimmermann se rozhodl dočasně tento problém ignorovat s tím, že PGP je určeno především pro jednotlivce, nikoliv pro firmy a organizace a tak přímo nekonkoruje RSA Data Security Inc. což mu dávalo naději, že od této společnosti dostane svolení bez větších problémů.

Vážnějším problémem byl návrh nového Trestního zákona, který přišel z amerického senátu v roce 1991 a obsahoval i pasáže zaměřené proti poskytovatelům technologií znemožňujícím vládním organizacím odposlech. Spojené úsilý RSA Data Security Inc., telekomunikačního průmyslu a občanských aktivistů vedlo k vynechání inkriminovaných pasáží, ale obecně se předpokládalo, že jde o pouhý odklad. Zimmermann se obával, že dříve či později se vláda pokusí znovu přijít s novým, podobně zaměřeným zákonem, který prohlásí šifru PGP za nezákonou. Původně sice měl v úmyslu PGP prodávat, ale nyní to znovu zvážil. Místo toho aby se pokusil ze svého výtvoru něco vytěžit, dal raději přednost tomu, aby byl PGP dostupný zadarmo všem, okamžitě, dřív, než bude pozdě. V

červnu 1991 podnikl drastický krok, když umístnil PGP na vývěsku (bulletin board) Usenetu (předchůdce www). Vycházel při tom z toho, že PGP není nic jiného než software, tedy informace a tak si ji každý může z této vývěsky stáhnout a s ohledem na právo šířit a schromažďovat informace mu v tom nikdo nemůže bránit.

Výsledek na sebe nedal dlouho čekat - PGP se lavinovitě rozšířil do celého světa, po všech koutech digitální komunity. V mžiku jej začali používat zastánci lidských práv na celém světě, disidenti, odbojové skupiny i zločinci a teroristé. V roce 1993 byl Phil Zimmerman vládou USA obviněn z nelegálního exportu zbraní. Vláda Spojených států totiž zahrnula šifrovací software do své definice zbraní. PGP se tak - vedle raketových střel, minometů, kulometů, děl, tanků, bojových letadel a zbraní hromadného ničení - nesměl exportovat bez povolení ministerstva zahraničí. Rozpoutala se zuřivá právní bitva do níž se na jedné straně zapojily vládní organizace typu FBI a NSA, na druhé neziskové skupiny pro ochranu lidských a občanských svobod jako napčíklad Center for Democracy and Technology nebo Electronic Frontier Foundation. Skutečnost, že autora vyšetřuje FBI a že NSA nelibě nese dostupnost PGP, však sami o sobě ještě pozvedly jeho reputaci a zrychlili jeho šíření - vždyť to byl tak silný šifrovací nástroj, že vystrašil i federály a nejsilnější kryptoanalytickou organizaci na světě. Jak se vyšetřování protahovalo, Zimmermannova podpora rostla. Štěstím se však pro něj nakonec ukázalo především to, že PGP neprodal, ale prostě zveřejnil, nevyvezl na disketě, ale umístnil na americkém Usenetu. Právní kličky tak nakonec více než cokoliv jiného vedly k tomu, že roku 1996, po třech letech intenzivního vyšetřování, úřad amerického prokurátora stáhl žalobu. Domývat se, že "pravda a láska zvítězila na lží nenávistí" by však bylo poněkud krátkozraké...

Obě strany měly v onom sporu jak se zdá stejně pádné a logické argumenty. Jedni se oprávněně obávají rapidního omezení možnosti států v boji s organizovaným zločinem a terorismem, druzí mají napak více něž dost důvodů bát se prostředků které dnes státní moc má k šmírování a špiclování svých občanů, prostředkům které až nepříjemně připomínají vize George Orwella.

Obecné mínění nicméně tvrdí, že v daném sporu nevzvítězil nikdo jiný než čas - roku 1996 si FBI uvědomila, že už je příliš pozdě. PGP pronikl na internet a soudním stíháním Zimmermanna se již nedalo ničeho dosáhnout, ikdyby byl odsouzen třeba k smrti. Zimmermanna mimo to podporovali nejen "idealističtí blázni, anarchysté, zločinci a teroristé", ale i mnohé důležité a obecně respektované instituce, jejihž samotné jméno mělo velkou váhu a jejich akce si nikdo nedovolil napadnout - například vydavatelství Massachusetts Institute od Technology Press publikovalo zdrojový kód PGP v 600 stránkové knize, kterou distribuovalo po celém světě. Soudní stíhání Zimmermanna by tak nevyhnutelně znamenalo i stíhání MIT Press, odnože jedné z nejvlivnějších a nejrespektovanějších vědeckých organizací na území USA. PGP se tak stal legitimním produktem a Zimmermann byl volný. Vyšetřování z něj učinilo kryptografického hrdinu a každý marketingový manager mu musel závidět reputaci a reklamu které se tím jeho PGP dostalo.

Zatímco pro osoby a jednotlivce zůstalo PGP zadarmo a každý si je může stáhnout například na http://pgpi.com/ [6] (mezinárodní domovská stránka PGP), pro firmy a organizace se stalo komerkčním produktem, z jehož prodeje má jeho autor jistě oprávněnou (finanční) odměnu.

Kvantová kryptografie a kvantový počítač

Dříve něž začnete číst následující řádky, dbejte prosím varování, které vyslovil Niels Bohr, jeden z otců kvantové mechaniky: "Každý kdo přemýšlí o kvantové mechanice, aniž by se mu zatočila hlava, jí nerozumí." Jinými slovy, připravte se, že se setkáte s některými poměrně šílenými myšlenkami.

Abychom si vysvětlili kvantovou teorii, vrátíme se k práci Thomase Younga, který roku 1799 publikoval svou "vlnovou teorii světla", což je jedna z nejklašičtějších fyzikálních statí všech dob. Cesta která vedla Younga k jejímu napsání začala, když během svéhou zkoumání povahy světla narazil na zajímavý jev. Young prováděl pokus kdy svítil na přepážku ve které byli dvě úzké štěrbiny. Očekával, že na stěně za přepážkou uvidí dva světlé pruhy, projekce světla. Místo toho pozoroval, že světlo vycházející ze dvou štěrbin vytvořilo na stěně vzor několika světelných pruhů. S pruhovaným světelným zdrojem si Young dlouho nevěděl rady, až náhle jednou spatřil dvě kachny plující na rybníce a zpozoroval, že za sebou zanechávají dvojici zvlněných stop, které se prolínají a vytvářejí zvláštní vzor z klidných a vlnících se míst. Youngovi tehdy kachny připoměly vlastí pokus a napadlo

jej, že světlo má podobu vlny. Pokud se světlo vyzařující ze dvou štěrbin chová jako vlna, pak pro něj platí stejný princip, jako pro dvě kachní stopy (brázdy) na hladině rybníka - světlé a tmavé pruhy na stěně za přepážkou tedy byli způsobeny stejným vzájemným působením.

Dnes víme, že se světlo opravu chová jako vlna, ale rovněž víme, že se také může chovat jako částice. To zda vnímáme světlo jako vlnu, nebo jako částici záleží na okolnostech. Tato dvojznačnost světla je známa jako "korpuskulární dualita". My ji nepotřebujeme rozebírat podrobněji, pouze si řekněme, že moderní fyzika vychází z představy světelného paprsku, který je tvořen nesčetnými jednotlivými částicemi, známými jako fotony, jež mají vlnové vlastnosti. Z tohoto pohledu lze Youngův pokus interpretovat pomocí fotonů, které zaplaví štěrbiny a potom spolu interferují na druhé straně přepážky.

Dosud nebylo na Youngově experimentu nic skutečně neobvyklého. Moderní technologie však fyzikům umožnila pokus opakovat s využitím světelného zdroje tak slabého, že vysílá pouze jediný foton. Řekněme, že takový zdroj každou minutu vyšle jeden foton k přepážce. Někdy foton projde jednou ze dvou štěrbin a narazí na stěnu. Přestože naše oči nejsou tak citlivé, abychom mohly spatřit jednotlivé fotony, můžeme je pozorovat prostřednictvím speciálních přístrojů. Za nějakou dobu, řekněme za hodinu, můžeme získat celkový obrázek. Protože v každém konkrétním okamžiku prochází přepážkou pouze jediný foton, neměli bychom očekávat, že uvidíme pruhovaný vzor pozorovaný Youngem, protože ten je zdřejmě vytvořen přinejmenším dvěma fotony, jež současně prolétnou různými štěrbinami a navzájem se střetnou na druhé straně. U pokusu s jedním fotonem prostě očekáváme, že uvidíme jen jednoduchý průmět štěrbiny v přepážce. Je tomu však jinak - z nějaké neobyčejné příčiny je i s jednotlivými fotony výsledný obraz stále tenýž - vzor světlých a tmavých pruhů.

Výsledek tohoto pokusu se vzpírá zdravému rozumu. Neexistuje způsob jak takový úkaz vysvětlit pomocí klasických fyzikálních zákonů, kterými popisujeme a zdůvodňujeme chování předmětů v našem každodenním životě. Jak se ukazuje, klasická fyzika může do detailů vysvětlit oběžné dráhy planet, nebo trajektorii dělové koule, ale nemůže popsat svět velmi malých měřítek, jako například trajektorii fotonu. Proto se fyzikové uchylují ke kvantové teorii, která popisuje, jak se objekty chovají v mikroskopickém měřitku. Ale ani kvantoví teoretikové se neschodují na tom, jak popsaný pokus vysvětlit.

První tábor zastává myšlenku známou jako superpozice. Ta začíná tvrzením, že v tomto pokusu víme s jistotou jen dvě věci a totiž že foton opustí zdroj a že nakonci své cesty narazí do stěny. Vše ostatní je naprosté tajemství, včetně toho, zda foton proletí pravou nebo levou štěrbinou. A protože přesná dráha fotonu je neznámá, superpozicionisté zastávají výstřední názor, že foton nějak proletí oběma štěrbinami najednou, což mu pak umožní interferovat se sebou samým a vytvořit námi pozorovaný pruhovaný vzor na stěně. Superpozicionisté argumentují následujícím způsobem: pokud nevíme, co částice dělá, potom může dělat cokoliv. V případě fotonu nevíme, zda proletěl levou, nebo pravou štěrbinou, takže předpokládáme, že prošel objema pozicemi najednou. Každé možnosti se říká stav, a protože naplní obě možnosti, říkáme že je v superpozici stavů.

Pro ty, jimž se tato teorie nezdá, je tu druhá kvantová teorie, která je bohužel neméně podivná. Tzv. interpretace mnoha světů tvrdí, že poté, co foton opustí zdroj, má dvě možnosti - buď proletět levou, nebo pravou štěrbinou - a v tomto bodě se údajně vesmír dělí na dva vesmíry, v jednomž foton letí pravou štěrbinou, zatímco v druhém levou. Tyto dva světy nějak intereferují navzájem, což vysvětluje pruhovaný vzor. Přívrženci interpretace dvou svěrů se jednoduše domívají, že kdykoliv má předmět možnost přejít do jednoho z několika různých stavů, rozdělí se vesmír do mnoha vesmírů, aby byla každá možnost naplněna v jiném vesmíru. O tomto rozrůstání vesmírů se mluví jako o multiversu, mnohovesmíru.

Obě kvantové teorie tedy zní poměrně šíleně. Mluví se však o nich jako o dvou nejpraktičtějších vědeckých teoriích, které kdy byli vymyšleny. Objasňují totiž nejen výsledky Youngova experimentu, ale i mnohé další fenomény, pro které bychom jinak jen velmi těžko hledali vysvětlení. Kvantová teorie dnes (kupodivu) není jen nějakým myšlenkovým experimentem, nebo hračkou. Právě kvantová teorie umožňuje fyzikům vypočítat následky jaderné reakce v elektrárně, nebo sestavit laser který čte CD ve vašem přehrávači. Ať se nám to líbí nebo ne a ať už to zní sebepodivněji, žijeme ve kvantovém světě. A co je důležité z hlediska našeho ústředního tématu, kvantová teorie nám

přináší zajímavé možnosti jak z hlediska kryptografie, tak i kryptoanalýzi.

Ze všech důsledků kvantové teorie je pravděpodobně technologicky nejvýznamnější kvantový počítač. S myšlenkou kvantového počítače poprvé přišel britský fyzik David Deutsch v roce 1984, kdy si na jedné vědecké konferenci uvědomil, že nevyřčeným předpokladem bylo, že všechny počítače fungují na základě klasické fyziky. Deutsch náhle došel k názoru, že by místo toho měly pracovat na základě fyziky kvantové, protože ta je "hlubší". Podle Deutsche obyčejné počítače pracují víceméně na makroskopické úrovni, na níž jsou kvantové a klasické fyzikální zákony téměř nerozlišitelné. Proto prý zatím nehrálo žádnou roli, že vědci obvykle uvažovaly o počítačích v pojmech klasické fyziky. Na mikroskopické úrovni se však tyto dva soubory zákonů odchylují a klasické zákony tu přestávají platit. Podstatné pro nás je, že počítače pracující na kvanotovém základě by pro nás byly výhodnější a to v jednoduchosti proto, že by nepracovali s binárními čísly (bity) které mohou nabívat pouze jednoho ze dvou stavů (jedna nebo nula), ale s kvantovými bity neboli qubity, čily jedničkami a nulami v superpozici, případně v multiversu. Ať už se totiž přikloníme k teorii multiversa, nebo superpozice stavů, zatímco obyčejný počítač je schopen v jediném okamžiku prověřit jen jedno řešení, kvantový počítač by měl být schopen prověřit řešení všechna. Využitím kvantové teorie by tedy zcela logicky měly vzniknout nepředstavitelně výkonné počítače, naprosto nesrovnatelné s těmi stávajícími. To by pochopitelně vedlo k okamžitému znehodnocení šifer jako AES, DES, nebo RSA, které by nebylo problémem prolomit "hrubou silou".

Základním problémem celé teorie kvantového počítače je to, že prozatím (jak se zdá) nikdo nemá tušení jak nějaké takové zařízení sestavit. Jednou z největších překážek je to, jak udržet částice v superpozici stavů v průběhu celého výpočtu, protože stávající teorie předpokládá, že superpozice stavů existuje pouze tehdy, když ji nepozorujeme, ale pozorování zahrnuje v nejobecnějším smyslu interakci s čímkoliv, co vystupuje vůči superpozici jako vnější prvek. Pouhý zatoulaný atom intereagující s jednou z částic by tedy zapříčinil neúspěch celého kvantového výpočtu. V době kdy David Deutsch přišel se svou vizí kvantového počítače byl dalším problémem program pro kvantový počítač, protože nikdo nevěděl jak by jej šlo naprogramovat, ikdyby nakrásně existoval. Dnes už je prý situace jiná. Obvzláště zajímavé je pro nás to, že první dva programy pro kvantové počítače, které vědci vymysleli byli přesně tím, co by kryptoanalytici daly ve svém seznamu priorit na první místo. V roce 1994 totiž Peter Shor z AT&T Bell Laboratories v New Jersey poprvé uspěl při definování programu pro kvantový počítač. Shorův program byl definicí série kroků, které by mohl kvantový počítač použít k faktorizaci obrovského čísla - tedy přesně to co by bylo zapotřebí pro rozlomení šifry RSA. Roku 1996 sestavil Lov Grover, pracující na stejném pracovišti další "kvantový program", který řeší pro změnu problém jak prohledat jakýkoliv seznam neuvěřitelně vysokou rychlostí - což je právě to, co je zapotřebí k rozlomení šifer jako je třeba DES. Nabízí se otázka, zda šlo pouze o náhodu...

Zatímco však kryptoanalytici předvídají příchod kvantových počítačů, kryptografové sní o vlastním technologickém zázraku - šifrovacím systému, který nastolí absolutní soukromí, dokonce i když bude čelit plné síle kvantového počítače - nové formě šifrování, která je zásadně odlišná od kterékoliv jiné šifry, na níž jsme dosud narazily, protože skutečně nabízí naději na dokonalé soukromí. Jinými slovy, tento systém šifrování nám zaručí na věky naprostou bezpečnost.

To může to vypadat jako velmi odvážné (nebo hloupé) tvrzení, zvláště ve světle předchozích podobných prohlášení, která se téměř bez výjmky ukázala jako mylná. V různých dobách během posledních dvou tisíc let se kryptografové domývali, že monoalfabetická šifra, polyalfabetická šifra, nebo šifrovací přístroje jako Enigma jsou nerozlomitelné. V každém z těchto případů se nakonec prokázalo, že se kryptografové mýlili, protože jejich tvrzení byla založena pouze na faktu, že složitost šifer v určitém dějinném okamžiku předehnala vynalézavost a technologii kryptoanalytiků. Při zpětném pohledu vidíme, že kryptoanalytici nakonec nevyhnutelně dají dohromady způsob, jak prolomit každou šifru, nebo rozvinou technologii, která ji prolomí za ně.

Tvrzení, že kvantová kryptografie je bezpečná, je však kvalitativně odlišné od všech předchozích. Kvantová kryptografie není pouze prakticky nerozlomitelná, je nerozlomitelná naprosto. Nestojí na složitosti šifrovacího systému, ale na samé podstatě určitého fyzikálního jevu - za nezlomitelnost šifry tu tedy neručí intelekt génia, ale sama matka příroda. Kvantová teorie, údajně nejúspěšnější teorie v historii fyziky, totiž znamená, že kryptoanalytik se nemůže o zachycení zprávy vyslané pomocí kvantové kryptografie ani pokusit, aniž by oba legitimní uživatelé nebyli varováni.

CC-BY-SA Security-Portal.cz | secured by paranoid sense | we hack to learn

Ale nepředbíhejme - jak by ona kvantová kryptografie měla fungovat? Vraťme se do 60. let 20. století kdy první praktické použití kvantové teorie rozvinul Stephen Wiesener, prostřednictvím své vize kvantových peněz. Princip Wiesnerových kvantových peněž vycházel ze skutečnosti, že padělání je dvoustupňový proces: padělatel nejdříve musí přesně změřit původní bankovku a potom ji replikovat. Tím, že Wiesner začlenil do bankovky fotony, však zařídil, že bankovku není možné změřit a tudíž ji ani replikovat. Vstupuje tu do hry tzv. princip neurčitosti, které trvdí že "nemůžeme poznat současnost ve všech jejích detailech" - tedy že je nemožné změřit každý aspekt určitého předmětu s dokonalou přesností. Naivní padělatel si může myslet, že pokud není schopen změřit polarizaci fotonů ve "světelných pastech" on, nedokáže to ani banka. Třeba se pokusí vyrobit bankovku s náhodnou sekvencí polarizací. Banka ale dovede ověřit která bankovka je pravá, protože ví, které polarizace má očekávat v každé světelné pasti u bankovky toho kterého daného čísla a tak může správně nastavit polaryzační filtr pro každou past a provést přesné měření. Pokud je bankovka padělaná, padělatelova náhodná polarizace povede ke špatnému měření a bankovka bude vyřazena jako falzifykát. Krátce řečeno, padělatel nemůže změřit polarizaci v pravé bankovce, protože neví, jaký typ fotonu je v každé světelné past a nemůže tedy vědět jak orientovat polarizační filtr, aby foton správně změřil. Na druhou stranu je banka schopna ověřit polarizaci pravé bankovky, protože polarizace sama vybrala a ví tedy, jak polarizační filtr orientovat pro každou světelnou past.

Kvantové peníze byly vynikající myšlenkou, bohužel však Wiesener natolik přehnal dobu, že mu nikdo nevěnoval pozornost. Kvantové peníze jsou nicméně přece jen poněkud nepraktické - zatím neexistuje technologie, která by umožňovala fotony lapat a i kdyby existovala, byla by pravděpodobně příliš drahá, než aby ji bylo možné aplykovat na bankovky běžné hodnoty (ochrana dolarové bankovky by mohla přijít i na několik miliónů dolarů). Přesto však ukázaly zajímavý způsob aplykace kvantové teorie, který přivedl roku 1984 Charlse Bennetta a Gilese Brassarda k nápadu, jak variací na Wiesenerovu myšlenku využít v kryptografii - čtrnáct let poté, co odborné časopisy odmítly Wiesenerovu stať inspirovala naprosto bezpečný komunikační systém.

Jeho jádro spočívá v jednoduchosti v tom, že vysláním emise fotonů zajistíme bezpečnou výměnu bitů, které pak mohou sloužit jako základ pro jednorázovou tabulkovou šifru (distribuce klíče). Odesilatel jednoduše využije řadu náhodně polarizovaných fotonů jako nosič infomací, tím že je vyšle k příjemci, přičemž si sám zaznamená jakou polarizaci použil pro jednotlivé fotony. Příjemce sice neví jaké polarizační schéma odesilatel použil a tak nemá možnost zachytit polarizaci všech fotonů, ale začne-li náhodně střídat polarizaci, nějaké procento jistě zachytí. Následně odesilatel pomocí běžné, nezabezpečené linky vyrozumí příjemce o tom, jaká polarizační schémata použil pro který foton, ne však o tom, jak jednotlivé fotony polarizoval. Příjemce na základě této informace odesilateli sdělí, u kterých fotonů uhodl správné polarizační schéma. V těchto případech totiž s jistotou změřil správnou polarizaci a zapsal ji pomocí řady binárních čísel. Příjemce i odesilatel pak nadále neberou v úvahu ty fotony, u nihž příjemce použil nesprávné schéma a soustředí se na ty, které určil správně. Tím vytvoří novou, kratší sekvenci bitů, skládající se pouze s příjemcových správných měření. To umožní příjemci i odesilately vytvořit společnou sadu číslic, jejíž základní vlastností je nahodilost, protože je odvozena veskrze náhodným výběrem z odesilatelovy původní sekvence která byla sama o sobě také náhodná. Takto "dohodnutá" sekvence netvoří zprávu, ale hraje roli náhodného tabulkového jednorázového klíče, který se použije pro symetrické šifrování.

Problémem každého kryptoanalytika pokoušejícího se zlomit danou šifru spočívá prostě v tom, že tutu šifru nelze zlomit - jednorázová tabulková šifra s náhodným klíčem je zcela bezpečná, neboť z ní nelze vydedukovat žádný vztah mezi otevřeným a šifrovým textem (protože tu v zásadě žádný není) a kryptoanalitik nedokáže klíč vytvořený kvantovou krypgofrafií zachytit. Pokud se totiž kryptoanalytik pokusí změřit fotony během přenosu podobně tak jako to udělal příjemce, jednak zvolí jiné uspořádání polatizačních filtrů, druhak se mu nedostane adekvátní nápovědy od odesilatele a - co je hlavní - nakonec i riskuje, že změní polarizaci fotonů jejihž polarizaci neodhadl správně, čímž v důsledku odhalí svůj odposlech na lince a varuje oba legitimní účastníky.

Myšlenka je to jistě pěkná, ale opětovně bylo otázkou zda ji lze prakticky realizovat. Dnes už s jistotou víme, že to možné je. V roce 1988 Bennet s pomocí postgaduálního studenta Johna Smolina experimentálně dokázal, že kvantová kryptografie možná je - byl to zcela jasný důkaz navzdory faktu, že k přenosu došlo na vzdálenost pouhých 30 cm. Již v roce 1995 výzkumníci ženevské univerzity implementovali kvantovou kryptografii do optického vlákna spojující města Ženeva a Nyon, vzdálené 23 km. V květnu 2002 se švýcarské firmě ID Quantique podařilo realizovat spojení na

základě kvantové kryptografie na vzdálenost 60 km. V červnu 2003 společnost Toshiba Research Europe realizovala přenos informací pomocí kvantové kryptografie na vzdálenost 100 km. Její odborníci vyjádřily názor, že tato technologie by mohlo do komerkční sféry proniknout do 3 let. Již 9. března 2004 však firma ID Quantique a americká společnost Magiq prohlásily, že mají k dispozici kvantovou technologii která umožňuje přenost zpráv pomocí kvantové kryptografie na vzálenost 120 km a mohou ji poskytnout komerkčnímu sektoru. Hlavní překážkou pro nevládní organizace je prozatím cena - optický kabel je sice relativně levný, ale cena jednoho rozhraní kvantové kryptografie se pohybuje mezi 50 a 100 tisíci USD. Obecně se však věří, že jde pouze o otázku času.

Hledání soukromí tak zdánlivě došlo ke svému konci - technologie je schopná zajistit zcela bezpečnou komunikaci pro vlády, armády, obchodníky i veřejnost. Pokud by se totiž někdy podařilo dešifrovat zprávu odeslanou kvantovou kryptografií, znamenalo by to, že celá kvantová teorie byla mylná, což by mělo pro fyziky zdcující důsledky - byli by nuceni znovu zcela přehodnotit celý svůj pohled na fungování vesmíru v jeho nejzákladnější úrovni. Zůstává tedy jediná otázka: dovolí vlády veřejnosti používat tuto technologii?

Neméně zajímavá je ovšem i skutečnost, že firma Maquiq ve svém prohlášení z 9. března 2004 zároveň oznámila i práce na vývoji komerkčního kvantového počítače. S ohledem na utajení ve vládním sektoru (doprovázející šifrovací technologie už od nepaměti) lze oprávněně předpokládat, že organizace jako je například americká NSA již kvantovou kryptografii dávno používají a že dokonce dávno mají i kvantový počítač...

Postranní kanály

V posledních několika letech se na poli kryptoanalýzi objevila metoda která nabízí nové cesty útoku i na ty nejdokonalejší šifry, které byli považovány za neprolomitelné. Takový je alespoň jeden pohled na tzv. postranní kanály. Místy se totiž objevuje i poněkud jiný názor na tuto metodu, tvrdící, že vlastně ani nejde o kryptoanalýzu. Jádro pudla je v tom, že postranní kanály jsou v zásadě prostředkem, jak se vyhnout nejsilnější stránce soudobých "elektronických" šifer - tj. jejich matematické podstatě - tím, že udeříme na jejich nejslabší část, kterou je způsob jejich implementace. Jinými slovy, postranními kanály jednoduše prolamujeme šifru, aniž bychom ji skutečně přímo prolamovaly.

Představme si například, že máme šifru, jejíž prolomení je absolutně nemožné - dnes, zítra, i za tísíc let, prostě navždy, s jakoukoliv technologií a za jakýchkoliv podmínek. Představme si že taková šifra skutečně existuje (podle toho co zatím víme by dobrým příkladem mohla být třeba jednorázová tabulková šifra). Představme si, že sám kryptoanalytik věří v absolutní neprolomitelnost této šifry a je si 100% jist, že nemá prostředky k jejímu prolomení a ani je nemůže získat. Podle teorie postranních kanálů však přesto může získat otevřený text. I ta nejlepší šifra totiž musí být nějakým způsobem použita - je ji nutné nejprve zašifrovat a poté opětovně dešifrovat. Logická úvaha praví, že pokud nemáme prostředky jak získat otevřený text v průběhu jeho zabezpečeného přenosu, přímo ze zašifrované zprávy (šifrového textu), můžeme jej jednoduše získat ještě před zašifrováním, nebo po dešifrování, kdy není neproniknutelně chráněn.

Jinými slovy jakákoliv kryptografická snaha je marná, pokud si během šifrování, nebo dešifrování necháte koukat přes rameno osoby před kterými chcete zprávu utajit. V klasickém pojetí bychom takové "kryptoanalytické" akce nejspíš označily za běžnou špionáž, která nemá s luštěním kódů a šifer nic společného. Nové technologie však vedou k novému pohledu na věc, neboť umožňují to, co kdysi možné nebylo - novodobý "špión" vám totiž nemusí přes rameno koukat přímo - může jít například o hackera který infiltruje váš počítač, nebo samotného výrobce vámi používaného šifrovacího software, který si ve vlastním produktu ponechá "zadní vrátka".

Postranní kanály mohou mít mnoho rozličných podob a proto je jejich přesná definice obtížná. Odborný termín nejčastěji uvádí, že postranním kanálem je každá informace, kterou program dá k dispozici útočníkovy o fungování šifrovacího systému. Toto tvrzení se snad může na první pohled zdát trochu přehnané, ale podívejme se na problematiku "uloupeni nezašifrované zprávy" z trochu jiného hlediska - víme, že zpráva je bezpečná po zašifrování, což nás logicky vede k závěru, že ji je nutné získat ještě před zašifrováním, nebo po dešifrování. Ovšem co v případě kdy prostě nemáme

CC-BY-SA Security-Portal.cz | secured by paranoid sense | we hack to learn

takovou možnost? Bylo by možné získat zprávu v průběhu jejího šifrování? Možné to je. Mimimálně můžeme získat vodítko, které nám původně nemožné dešifrování umožní. Jedna z metod útoku na šifru RSA v průběhu odšifrování, nebo podpisu kupříkladu vychází z myšlenky měření času nezbytného k šifrování a využití takto získané hodnoty k omezení množiny faktorizace. Podobné metodiky útoky byli vyvinuty i proti šifrám DES, AES a IDEA.

Celá oblast postranních kanálů je ještě dnes v plenkách, ale zdá se, že nabízí netušené možnosti. Její přitazlivost pro kryptoanalytiky spočívá především v tom, že podobné metody útoku dosud nebyly adekvátně zkoumány a tudíž proti nim kryptografové ani nemohly cíleně vyvinout adekvátní protiopatření. To kryptoanalytikům dává naději k dosažení rychlých a absolutích průlomů, což je po předchozích "hubených letech", kdy kryptoanalytické úspěchy spočívaly v "omezení strojního času nezbytného k průlomu z 50 let na 48.5 let" dostatečnou motivací ke zkoumání dané problematiky. Podle některých odborníků se dokonce předchozí kryptoanalýza vydala slepou uličku, když se soustředila jen na "zkoumání abstraktních schémat odtržených od reality" a "pravá podstata elektronického šifrování tak zůstala nepochopena".

Skutečně se zdá, že v budoucnu bude kryptologii třeba zkoumat v mnohem širších souvislostech. Je dost dobře možné, že stejně tak, jako si kdysi rozluštění Enigmy vyžádalo intenzivnější zapojení matematiky do tohoto interdisciplynárního oboru, bude do něj v budoucnu nutné zapojit hned několik dalších odborností kterým jsme zatím nevěnovaly dostatečnou pozornost. Obrana proti tomuto způsobu kryptoanalýzi bude každopádně velmi obtížná, neboť se ukazuje, že k průlomu lze využít i zdánlivě nepodstatných detailů. Na druhou stranu je ovšem nutné zmínit, že bezpečnost žádné šifry prozatím nebyla v důsledku postranních kanálů nově přehodnocena - veškeré výhrady se týkaly jen a pouze způsobu implementace těchto šifer.

Absolutní šifra?

Tvůrci kódů a šifer (kryptografové) vždy usilovali o stále dokonalejší utajení informací, zatímco jejich luštitelé (kryptoanalytici) naopak vyvíjeli ještě rafinovanější metody jak je prolomit. V této snaze o uchování i odhalení tajemství nasazovali obě strany vědomosti a technologie z rozmanitých oborů, od lingvistiky, přes matematiku až po kvantovou fyziku. Právě oblast šifrování byla mnohdy hnacím impulsem technického rozvoje.

V různých časových obdobích se zdálo že má kryptografie navrch před kryptoanalýzou, v jiných tomu bylo naopak. Postupem doby se ukázalo že jde o věčný zápas který nemá trvalé, ale pouze dočasné vítěze. Po prolomení několika šifer považovaných v určité době za "neprolomitelné" se začalo brát jako fakt, že zádný ze způsobů ochrany dat není dlouhodobě bezpečný, nakonec se vždy najde způsob jak mu čelit, bez ohledu na jeho rafinovanost.

Přesto však i ta nejednodušší šifra výrazně zvyšuje bezpečnost komunikace a mnohé šifry jsou za určitých podmínek - při správném použití - skutečně neprolomitelné. Neprolomitelná může být správně použitá kódová zpráva. Neprolomitelná může být krátka zpráva šifrovaná pomocí monoalfabetické šifry s nomenklátory i klamači, stejně jako obdobná zpráva šifrovaná homofonní substituční šifrou, nebo Vignérovou šifrou. Za zcela neprolomitelnou se dodnes považuje jednorázová tabulková šifra, ať už je použita klasickým způsobem, nebo ve spojení s kvantovou kryptografií. Šifry jako DES, AES, IDEA nebo RSA poskytují takový stupeň ochrany, že ač je jejich prolomení teoreticky možné, prakticky jsou téměř neprolomitelné.

Za největší nebezpečí pro moderní kryptografii se dnes považují postranní kanály. Ty však ve skutečnosti neohrožují ani tak samotné šifry, spíše jako jejich neschopné uživatele. Není to přitom jev nikterak vzácný, nebo nový - historie nám ukazuje, že špatně použitá šifra je horší než žádná šifra. Šifra Marie Stuartovny byla názorným příkladem, jak pomocí nevhodně použité kryptografie vstrčit hlavu do oprátky. Přístroje Enigma, Lorenz, nebo Purple z dob druhé světové války se příliš nelišily od spojeneckých přístrojů Type-X a SINGABA ze stejného období. Přesto však jedny byly prolomeny a druhé nikoliv. Svou roli zde jistě sehrály i schopnosti spojeneckých kryptoanalytiků (stejně jako prvotní polský vklad), ale jak se ukazuje tak průlomů by nebylo možné dosáhnout bez špatné metodiky použití šifrovacích přístrojů a místy velmi omezené kázni jejich operátorů.

CC-BY-SA Security-Portal.cz | secured by paranoid sense | we hack to learn

Velké pochybnosti dnes panují ohledně reálnosti koncepce i stávající existence či neexistence kvantového počítače. Problémem je skutečnost, že věda o utajování sama přísnému utajování podléhá. A tak zatímco objevy z většiny jiných oborů jsou svými autory rychle patentovány a publikovány, informace z oboru kryptoanalýzi byly v průběhu let a staletí pečlivě tajeny.

Za autora postupu dešifrování Vigenérovy šifry byl po více než sto let považován Kasinsky, nikoliv Babbage. O dešifrování přístrojů Enigma a Lorenz se svět dozvěděl až s odstupem mnoha desítek let. Za první programovatelný počítač byl po léta považován ENIAC, nikoliv Colossus. Systémy DHM a RSA byly ve skutečnosti vyvinuty v GCHQ (Government Communications Headquarters - britská obdoba NSA) již několik let před tím, než se jimi pánové Diffie, Hellman, Merkle, Rivest, Shamir a Aldermann vůbec začaly zaobírat. Je proto velmi pravděpodobné, že to co dnes považujeme za zcela nemožné je již někde jinde dávno docela možné. Ať už ovšem kvantový počítač existuje, nebo neexistuje, šifer, které by byly schopny čelit plné síle takových organizací jako je například NSA - organizací s přístupem k nejmodernější technice a zaměstnávající ohromné počty špičkových odborníků - je dnes jen velmi málo. S trochou nadsázky lze říci, že v absolutní bezpečnost té či oné šifry věří snad jen ten, kdo kryptologii vůbec nerozumí. Paradoxně ale naopak mohou být proti průlomu zcela bezpečné i ty nejslabší šifry, jsou-li správně použity...

Prameny:

Knihy

Kniha kódů a šifer, Simon Singh
Digitální svět, Nicholas Negroponte

Weby:

http://www.krypta.cz/ [7]
http://www.scienceworld.cz/ [8]
http://cml.fsv.cvut.cz/~kupca/qc/node25.html [9]
http://www.codesandciphers.org.uk/ [10]
http://webhome.idirect.com/~jproc/crypto/menu.html [11]
http://news.bbc.co.uk/2/hi/technology/3543495.stm [12]

Software:

Zajímavý shareware šifrovací program Kryptel 5.11 (šifry AES, Triple-DES, IDEA aj.) je k dispozici na www.bestcrypto.com/index.php [13]

Jeden z nejkvalitnějších steganografických freeware softwarů pro Linux/UNIX je k dipozici na http://www.outguess.org/ [5]

Mezinárodní domovská stránka PGP (pro jednotlivce freeware) http://pgpi.com/ [6]

Článek byl se svolením autora převzat ze serveru ">http://temneuzemi.webzdarma.cz [14]

URL článku:
https://www.security-portal.cz/clanky/praktick%C3%A9-z%C3%A1klady-kryptologie-steganografie

Odkazy:
[1] https://www.security-portal.cz/users/3022
[2] https://www.security-portal.cz/category/tagy/encryption
[3] https://www.security-portal.cz/category/tagy/science-technology
[4] https://www.security-portal.cz/category/tagy/security
[5] http://www.outguess.org/
[6] http://pgpi.com/
[7] http://www.krypta.cz/
[8] http://www.scienceworld.cz/

[9] http://cml.fsv.cvut.cz/~kupca/qc/node25.html
[10] http://www.codesandciphers.org.uk/
[11] http://webhome.idirect.com/~jproc/crypto/menu.html
[12] http://news.bbc.co.uk/2/hi/technology/3543495.stm
[13] http://www.bestcrypto.com/index.php
[14] http://temneuzemi.webzdarma.cz

CC-BY-SA Security-Portal.cz | secured by paranoid sense | we hack to learn