Historia utajovanejho oboru

Vložil/a friedo [1], 19 Říjen, 2004 - 18:54

- Encryption [2]
- Security [3]

Každý odbor ľudskej činnosti má svoje dejiny. Inak to nie je ani pri téme nášho článku, ktorým je kryptológia (z gréc. kryptós, skrytý a logos, náuka) . Jej história je dlhá viac než 4000 rokov a behom storočí sa udiali veľmi zaujímavé a poučné príbehy. Vojvodcovia, kráľovia a cisári pomocou šifier a kódov ukrývali svoje úmysly, plány pred zvedavými očami nepriateľov. Školáci a milenci si pomocou nich posielali zašifrované odkazy. V súčasnosti sa využívajú v tak bežných technických prostiedkoch ako napr. rádiové a televízne vysielače, počítačové, satelitné siete, mobily, apod. Moderná doba nám teda priniesla a naďalej prináša ďalšie výzvy a kryptológii vtlačila novú úlohu. Úlohu všestranného informačného ochrancu dát pre všetky oblasti využitia počítačových technológií.

História utajovaného odboru - 1.časť

Úvod

Už od nepamäti sa ľudia (**odosieľateľ**, **príjemca**) pokúšali komunikovať pomocou rôznych prostriedkov, ako napr. reč, písmo atď. takým spôsobom, ktorý by zabezpečoval ochranu obsahu pred neželanými osobami (**dôvernosť**)a ich vplyvu na prenášané správy (**integrita** a **autentizácia**). Takéto techniky poskytuje podobor kryptológie - **kryptografia** (z gréc. *kryptós*, a *graphein*, píšem) **.** Je to vlastne zbraň, ktorá je štítom v boji proti nepriateľom na pomyselnej informačnej "diaľnici". Ak by sme chceli utajiť samotnú existenciu správy, musíme využiť služby inej vednej disciplíny zvanej **steganografia** (z gréc. *steganos*, schovaný a *graphein*, píšem) **. Kryptoanalýza** (z gréc. *kryptós*, a *analýein*, uvolniť)je mladšia sestra kryptografie a jej postupy využijeme pri pokuse o získanie informácii bez znalosti spoločného "tajomstva" - **šifrovacieho kľúča**, informácie, ktorú ako jedinú musia komunikujúce strany udržiavať v tajnosti.

Úsvit kryptografie - Starovek

Rozvoj umenia tajného písma a rapídne využívanie šifrovacích metód mohlo nastať iba v tom prípade, že v oblasti výskytu veľkých civilizácií (Mezopotámia, Egypt) sa nachádzalo písmo a reč v konečnom štádiu vývoja. Nie je teda žiadnym prekvapením, že práve v oblasti - delte Nílu sa našli prvé hlinené tabuľky obsahujúce prvé netradičné hieroglyfy. Majster pisár ich zhotovil okolo roku 1900 p.n.l. Boli to symboly nahradzujúce konvenčne používané hieroglyfy, a ich primárnym cieľom nebolo písaný text utajiť ale dodať mu vznešenosť. Ako keby sme povedali Leta pána tisícdeväťstodeväťdesiatdeväťnamiesto v roku 1999. V popise tejto metódy je aj ukrytý názov - **jednoduchá substitúcia.** Jednoduchá preto, že tu ide o zámenu jednej entity (písmena, číslice, znaku, symbolu) za 1 iný symbol z množiny prípustných entít, a substitúcia znamená náhradu.

Ďalší nález jednoduchých šifier pochádza z Mezopotámie (približne rok1500 pred naším letopočtom). Boli to záznamy hrnčiarov, ktorí týmto spôsobom chceli utajiť svoje recepty na výrobuglazúr.

Napríklad v takej Číne by sme v tých časoch takmer márne hľadali človeka, ktorý by sa pokúšal objavovať nové šifrovacie postupy. Príčiny sú prosté, vlastná znalosť písma znamenala už aj tak veľké obmedzenie počtu ľudí, ktorí by sa písaním správ a ich utajovaním mohli zaoberať. Avšak ajtu existuje tá povestná výnimka, potvrdzujúca pravidlo. V pojednaní ***Wu-tching tsujao*** (z 11. stor. pr. n. l. , v slov. preklade Základy klasického vojenstva) sú 40 otvoreným správam priradené kódové výrazy prevzaté z jednej básne, napr. žiadosť o luky a šípy by mohla po zašifrovaní znieť "Ó ako

krásne rozvitá je táto ruža."

Hebrejskí spisovatelia píšúci poznámky na okraj Jeremiášovej knihy používali jednoduchúsubstitučnú šifru s obrátenou (reciprokou) abecedou známu pod názvom **ATBASH (Š)**. Názov atbaš je odvodený od toho, že prvé písmeno hebrejskej abecedy alef je nahradené posledným písmenom tav, druhé bet je nahradené predposledným sin.(**Jeremiáš** začal s diktovaním **Baruchovi** v r. 605 p.n.l., ale kapitoly obsahujúce tieto kúsky šifry sa pripisujú zdroju označenému písmenom `` **C** '' (predpokladá sa, že to nebol Baruch), ktorým by mohol byť vydavateľspisu po Babylónskom exile v r. 587 p.n.l, nejaký súčasník Barucha alebo dokonca samotný Jeremiáš.) **ATBAŠ** bol jednou z mála hebrejských šifier tej doby. Ďalšie systémy boli **Albam** a **Atbah**.
ATBAŠ : A B C D E F G H I J K L M Z Y X W V U T S R Q P O N
Albam : 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
Atbah : A B C D J K L M E S T U V I H G F R Q P O N Z Y X W

Okolo roku 300 pr. n. l. sa v starej Indii používala substitúcia písmen za písmená, ktoré sú im foneticky príbuzné. V klasickom diele o štátnictve atajnej diplomacii
Arthra-šastra, ktoré je priprisované Kautilijovi, nie je len naznačené, že sa India priam hemžila špiónmi, ale výslovne doporučuje používanie tajného písma. Dokonca doporučuje velvyslancom lúštiť tajné nápisy na maľbách a odhaľovať neviditeľné atramenty.

Vátsajánovo majstrovské dielo o erotike ***Kámasútra***, (okolo roku 400 pr. n. l.) zahŕňa tajné písmo pod dve (v poradí 44. a 45.) z celkovo 64 umení (jóg) , ktoré má žena poznať a používať.

Antické šifry

Nový impulz a konjunktúru požívala kryptografia v antike. V starom Grécku v Sparte používali prvúznámu mechanickú pomôcku na šifrovanie – **skytalé**. Využívali ju spartskí stratégovia na vojenských výpravách okolo roku 550 p. n. l. Tento šifrátor mal tvar dreveného valca, na ktorý sa prúžok za prúžkom tesne vedľa seba namotal pruh papyrusu, kože alebo pergamenu. Správa sa vypisovala smerom od jedného konca valca k druhému, až sa zaplnil celý papyrus. Potom sa pruh odmotal. Správa na ňom nedávala zmysel, pokiaľ sa u príjemcu nenamotala na rovnako hrubý valec, pretože písmena boli **poprehadzované** (**transponované**). Toto je asi prvý príklad použitia **transpozičnej** šifry v dejinách. Viaže sa k nej táto legenda. Raz, bolo to asi v r. 440 pr. n. l., dorazil ku kráľovi Sparty Lysandrovi ranený a skrvavený posol, ktorý ako jediný z piatich prežil ťažkú cestu z Perzie. Podal svoj opasok kráľovi, ktorý použil valec správneho priemeru a tak sa dozvedel správu, že sa ho perzský Farmazus chystá napadnúť. Vďaka tomu sa Lysandros včas pripravil, a nakoniec úspešne útok Peržanov odrazil.

Rímsky vojvodca **Aeneas Tacticus** vo svojom spise ***O obrane pevností*** (asi 360 pr. n. l.), v XXXI. časti zvanej *Tajné správy* odporúča používať asi 22 šifrovacích kľúčov rozdelených na substitúciu a transpozíciu. Substitučná šifra spracováva otvorený text správy na šifrový pomocou náhrady (substitúcie) jednotlivých znakov. Špecifickým príkladom substitučného kľúča je **kód**, kde sa okrem znakov nahradzujú celé slová alebo i vety číselnými alebo písmenovými dvoj až šesťmiestnymi skupinami. Základom transpozičnej šifrovacej metódy je zmena pozície al. poradia (t.j. **anagram**) znakov v otvorenom texte použitím vopred dohodnutého kľúča.

Tacticus ďalej popisuje šifrovací kameň s 24 otvormi, ktoré zodpovedali 24 písmenám gréckej abecedy. Pomocou tohoto kameňa sa šifrovalo tak, že sa písmená správy postupne prevliekalaniťou príslušnými otvormi kameňa.

Z ďalších antických metód spomeňme tzv. **Polybiov fakľový ďalekopis**. Bol to asi prvý prakticky používaný "telegrafický kód", ktorý umožňoval vysielaťaj dopredu nedohodnuté správy.

Vysielanie prebiehalo po písmenách tak, že na viditeľnom mieste stáli za dvoma nepriehľadnými panelmi fakľonosiči, ktorí po začínajúcom pohotovostnom signále prijímacej strany začali "vysielať". A to tak, že najprv sa nad ľavým panelom objavilo toľko fakieľ, aké je poradové číslo stĺpca, v ktorom sa nachádza prvé vysielané písmeno, a potom sa nad pravým panelom objavil taký počet fakieľ, ktorý zodpovedal číslu jeho riadka. Takto sa ďalej odvysielalo druhé písmeno,tretie, atď.

Rímsky historik **Titus Lívius** (žil v rokoch 59 pr. n. l. až17 n. l.) popisuje takmer neznámu udalosťzo života veľkého vojvodcu **Hannibala** (246-183 pr. n. l.). Vraj poslal posla z Talianska do Kartága so zašifrovanou správou. Ale použitú šifru ďalej bližšie nešpecifikuje. Ak by to bola substitučná šifra, jednalo by sa o prvý zdokumentovaný záznam jej využitia na vojenské účely.

Ale zanechajme špekulácie. Jednou z najznámejších substitučných šifier je tzv. **Caesarova šifra** +3 (**Gaius Julius Caesar**, 100-44 pr. n. l.). Princíp je zrejmý: šifrový text dostaneme tak, že písmená otvoreného textu postupne nahradíme znakmi abecedy, ktorá je posunutá o tri miesta doprava.

Tab. Caesarova šifra

OT: 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
ŠT: 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

Ak zašifrujeme napr. výrok **AJ TY BRUTUS**, dostaneme šifru **DM WBEUXWXV**. Ako väčšina šifrovacích systémov aj tento má svoj tajný prvok - **šifrovací kľúč**. Samozrejme je to rozdiel polôh písmen v abecede OT a ŠT. Celkovo máme k dispozícii 25 použiteľných hodnôt posunu abecedy ŠT, ak uvažujeme ako abecedu 26 písmen súčasnej medzinárodnej angličtiny. (Posun +0, t.j. žiadny je triviálnym príkladom, pretože obe abecedy sú navzájom totožné.)

V tomto starovekom svete našla uplatnenie aj metóda **steganografie** spomenutá už vyššie. Je to vlastne spôsob komunikácie, ktorá je utajená pomocou ukrytia správy. Zmienka o jej použití pochádza od **Herodota** - "otca histórie" ako ho nazval **Cicero**. Vo svojich ***Dejinách*** popisuje udalosť , kde práve ukrytie textu postačilo k bezpečnému zaslaniu správy. **Histiaios** potreboval poslať svojmu zaťovi **Aristagorasovi Milétskému** správu o povstaní proti Perzii. Aby zaslal posolstvo bezpečne, oholil **Histiaios** hlavu starostlivo vybranému otrokovi, napísal správu na kožu lebky a počkal, až poslovi znovu narastú vlasy. Potom ho vyslal cez nepriateľské územie. V cieli jeho cesty mu **Aristagoras** hlavu oholil a správu si prečítal. Ďalším spôsobom ako preniesť nepozorovane tajnú správu bol (taktiežho spomína **Herodotos**) nasledovný: Na drevené doštičky sa vyryla tajná správa a tie sa potom zaliali voskom. Dosky sa poslali po poslovi, ktorý ju niesol príjemcovi. Stráže, ktoré kontrolujú pri vstupe, ho s kľudným svedomím prepustili, lebo nenašli nič len dve nepopísané doštičky. Ako sa však mýlili!!!

V nasledujúcich obdobiach sa mnoho ľudí inšpirovalo, a vymysleli rôzne obmeny ako napr. vkladanie správ do útrob ulovených rýb, ukrývanie vzkazov do malieb, pašovanie drog v telových dutinách,neviditeľné atramenty a pod.

"Temné" obdobie

Po páde Rímskej ríše nastalo v Európe nie príliš plodné obdobie, snáď s výnimkou Škandinávskych krajín (runové šifry). Všetko v týchto časoch "temna" bolo postupne objavované znova, stagnovala vynalezavosť tvorcov nových šifrovacích systémov. Snáď jedinou svetlou výnimkou boli obdobiapontifikátu **Sylvestra II.** (999-1003 n.l., známeho pod reholným menom **Gerbert zAurillacu**) a vlády cisára svätej ríše rímskej **Karola Veľkého** (768-814 n.l.,na jeho dvore pôsobil **Alkuin zYorku**), ale aj vtedy sa uplatňovali velmi jednoduché šifry, ako napr. písanie viet zvislo a opačne, nahradzovanie samohlások bodkami, používanie písmen cudzích abecied namiesto vlastných, eventuálne znakové písmo alebo posun písmen o jedinú pozíciu (pamätajte na Caesara!). Mnísi v
stredovekej Európe sa tak postarali o návrat kryptografie do západnej civilizácie. Prvou európskou rukopisnou knihou o kryptografii bola ***De secretis artis et naturae operibus et denullitate magiae*** (List o tajných postupoch a neexistencii mágie). Jej autorom je známy anglický františkán a polyhistor **Roger Bacon** (nar. 1214-zomr. 1294). Nie je bez zaujímavosti spomenúť, že prvými systémami po tejto "dobe temna" boli opäť substitučné šifry, tzv. **nomenklátory**. Skĺbili v sebe výhody i slabé stránky kódov aj šifier a používali sa takmer až do vynálezu telegrafu.

Arabské príspevky

Väčšina výskumu a prác z oblasti kryptografie z tohoto obdobia pochádza z oblasti blízkeho Východu, Strednej Ázie, Severnej Afriky a časti Indie. Všade tam sa dostal islam pri svojej expanzívnej tendencii. Šíritelia tohto náboženstva - Mohamed a jeho nasledovníci - arabskí chalífovia pri svojich dobyvačných plánoch podporovali vedu a umenie na podrobených územiach. Z tohoto faktu plynul vzostup arabskej vzdelanosti, čoho dôkazom sú len nedávno (v roku 1987, Sulajmanovosmanský archív) objavené rukopisné knihy známeho arabského vedca a polyhistora **Abu JusufJa'qub ibn Is-haq ibn as-Sabbah 'Omran ibn Ismail al-Kindiho**. Jedna s názvom ***Rish alah f 'istikhr' aj al-Mu‘amm 'a***, čo v preklade znamená "Rukopis o dešifrovaní kryptografických správ" okrem popisu arabskej fonetiky a syntaxe, rozdelenia šifier na substitúciu a transpozíciu a podrobnej štatististickej analýzy obsahuje prvé použitie tzv. **frekvenčnej analýzy**. Jadrom tejto metódy je zistenie, že v každom jazyku sa v texte určité písmená vyskytujú častejšie než iné. Napr. najčastejšie sa vyskytujúcim písmenom anglickej abecedy je E s frekvenciou 12,7%, druhým je T s 9,1% atď. Postupnosť písmen anglickej abecedy zoradená podľa frekvencií ich výskytu v bežnom texte je: e t a o i n s h r d l c u m w f g y p b v k j x q z. Ďalej musíme preskúmať šifrový text a
stanoviť početnosť výskytu hlások. Ak sa v ňom ako najčastejší symbol vyskytuje napr. Q, potom je to veľmi pravdepodobne preto, že toto písmeno nahradilo samohlásku e. Pokiaľ je druhým najčastejším písmeno R, potom zrejme ide o náhradu za t, atď. Táto technika nám ukazuje spôsob ako bez skúšania každého kľúča z miliárd možných (26!) zistiť obsah zašifrovaného textu jednoduchou analýzou početností výskytu znakov šifrového textu.

Samozrejme nejde ju používať úplne mechanicky. Usporiadanie frekvenčnej tabuľky abecedy v náhodne vybranom texte je úplne iné ako napr. v literárnej angličtine resp. vo vojenskom texte. Táto pomôcka je iba nápoveďou, ktorú musíme zvažovať ale nesmieme jej bezvýhradne veriť. Vezmime si napr. anglickú frázu "A quick brown fox jumps over the lazy dog". Ak ju zašifrujeme jednoduchou substitúciou, bude takmer nemožné ju vylúštiť pomocou princípov frekvencie. Takže sa dá všeobecne povedať, že čím kratší text máme vylúštiť, tým sa jeho početnosti budú odlišovať od štandardných početností prirodzeného jazyka. Hranica lúštiteľnosti je daná tzv. **vzdialenosťoujednoznačnosti**, čo je teoretická hodnota počítaná zo štatistických zákonitostí daného jazyka. Pre anglický jazyk je to asi D = 40 písmen. Tento pojem je súčasťou vedeckej disciplíny - teórie informácie, ktorá je mimo rámec nášho článku. Určitými technikami, ktoré nám pomáhajú zdolať nástrahy substitučných šifier sú napr. využitie frekvencie **bigramov** (dvojíc písmen, ktoré v texte za sebou bezprostredne nasledujú), **trigramov** (písmenových trojíc), a vo všeobecnosti **polygramov**, tzv. **metóda predpokladaného slova**, atď. Práve posledne menovaná pomohla ďalšiemu z arabských vedcov a filozofov **Al-Khalilovi** (celým menom **Abu `Abd al-Rahman al-Khalil ibn Ahmad ibn`Amr ibn Tammam al Farahidi al-Zadi al Yahmadi**) pri rozlúštení gréckej tajnej depeše určenej pre byzantského vládcu. Uhádol, že sa začína oslovením "V mene Boha", čo mu pomohlo pri
identifikovaní niektorých šifrových znakov. Bolo to okolo roku 755 n. l. a táto príhoda ho inšpirovala k napísaniu knihy o kryptografii s názvom ***Kitáb al-Mu‘amma*** - "Kniha kryptografických správ", ktorá je však v súčasnosti považovaná za stratenú.

Okolo roku 855 je taktiež známa kniha napísaná **Abú Bakr Ahmadom** a popisujúca rôzne šifrovacie systémy. Súhrnom arabských poznatkov o všetkých vedných disciplínach je 14-zväzková encyklopédia ***Sub al-'asha***, vydaná v roku 1412 a obsahujúca jednu kapitolu o kryptografii a kryptoanalýze.

Slovníček

kryptoanalýza — zaoberá sa štúdiom možností prelomenia šifry, tj. získania otvoreného textu zo šifrovaného bez znalosti kľúča
kryptografia — znamená návrh a metodiku šifrovacích systémov
kryptológia — odbor zastrešujúci kryptoanalýzu a kryptografiu
otvorený text — text určený k zašifrovaniu
steganografia — skúma metódy utajenia existencie správy
substitučná šifra — transformuje otvorený text na šifrový náhradou (substitúciou) znakov

šifrovacia funkcia — transformuje otvorený text na šifrový
šifrovací kľúč — vstupuje do šifrovacej funkcie – utajovaný prvok bezpečnej komunikácie
šifrový text — výsledok šifrovacej funkcie
transpozičná šifra — transformuje otvorený text na šifrový zámenou poradia znakov

Záver

V dnešnej prvej časti sme si popísali históriu kryptológie od jej počiatkov a dostali sme sa až k významným objavom v kultúrnej oblasti arabských krajín. V ďalšej časti sa pozrieme na klasické šifrovacie systémy používané na sklonku stredoveku a počas prvej polovice novovekých dejín (približne do polovice 19. storočia). Môžeme sa tešiť napríklad na Albertiho, Trittheimove a Vigenérove objavy tzv. polyalfabetickej substitúcie.

URL článku: https://security-portal.cz/clanky/historia-utajovanejho-oboru

Odkazy:
[1] https://security-portal.cz/users/friedo
[2] https://security-portal.cz/category/tagy/encryption
[3] https://security-portal.cz/category/tagy/security