Dějiny kryptografie

Zpracováno podle knihy
Simon Singh: Kniha kódů a šifer

Obsah

1. **Ruční šifrování**
   - Monoalfabetické šifry
   - Polyalfabetické šifry
2. **Šifrovací stroje**
   - Šifrovací disky
   - Enigma
3. **Šifrování pomocí počítačů**
   - Standardní šifrovací protokoly
   - Šifrování s veřejným klíčem
   - Kvantové šifrování

Kryptografie

Kryptologie (= nauka o utajení) se skládá z

- kryptografie = utajené psaní
- kryptoanalýzy = rozbor, odhalování utajeného

Dějiny kryptologie jsou neustálým soubojem mezi kryptografií a kryptoanalýzou. Mnohé objevy byly prozrazeny až s velkou prodlevou, neboť znamenaly výhodu pro jednu válčící stranu.

Budeme používat pojmy

- otevřený text - původní zpráva (zapíšeme malými písmeny)
- šifrový text - zašifrovaná zpráva (zapíšeme velkými písmeny)

Otevřený text budeme psát bez diakritiky, stačí nám 26 písmen anglické abecedy.

Transpoziční šifry

Transpoziční šifry přehazují pořadí písmen v otevřeném textu.

- "Podél plotu" - píšeme písmena otevřeného textu střídavě nalevo a napravo podél plotu; šifrový text začíná celým textem, který je nalevo od plotu, a pokračuje textem napravo.
- "Pás kolem tyče" - kolem tyče ovineme pás a napíšeme na něj otevřený text napříč pásem v několika řádcích (tyč otáčíme a v textu pokračujeme podél tyče). Na rozvinutém pásu je pak šifrový text s přeházenými písmeny.
  K dešifrování je třeba použít stejně silnou tyč.

Substituční monoalfabetické šifry

Substituční šifry nahrazují písmena otevřeného textu jinými písmeny či znaky.

Caesarova posunová šifra

- Caesar, 100-44 př.n.l., Římská říše.
- Posune každé písmeno otevřeného textu o diferenci d, $p \to p + d$.
- Příklad: Posun $d = 3$.

Otevřený text	v	e	n	i.	v	i	d	i.	v	i	c	i.
Šifrový text	Y	H	Q	L.	Y	L	G	L.	Y	L	F	L.

- Rozluštění: Vyzkoušet všech 26 možností pro klíč d.

Substituční monoalfabetické šifry

Monoalfabetická šifra

- Lze použít libovolné vzájemně jednoznačné zobrazení mezi písmeny otevřené abecedy a písmeny šifrové abecedy.
- Počet bijekcí mezi abecedami, $26! \doteq 4 \cdot 10^{26}$. To už nelze vyzkoušet hrubou silou bez počítače.

Kerckhoffsův princip

- Kerckhoffs, 1885, Nizozemí
- Bezpečnost šifrovacího systému nesmí záviset na utajení algoritmu, pouze na utajení klíče.

Substituční monoalfabetické šifry

Monoalfabetická šifra

- Praktické provedení: Napsat klíčovou frázi na začátek šifrové abecedy bez mezer a opakujících se písmen a doplnit zbylá písmena "podle abecedy".
- Příklad: Klíčová fráze je Julius Caesar.

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

Otevřený text	v e n i. v i d i. v i c i.
Šifrový text	M S Y R. M R I R. M R L R.

Substituční monoalfabetické šifry

Frekvenční analýza

- Rozluštění monoalfabetické šifry přinesl rozvoj matematiky a lingvistiky v Arábii, 9. stol. (Evropa až 12. stol.).
- Frekvenční analýza textu - četnost výskytu písmen v textu daného jazyka je různá. Častý znak šifrového textu bude pravděpodobně znamenat časté písmeno v daném jazyce.

Angličtina:	e - 12,7%,	t - 9,1%,	a - 8,2%;
	q - 0,1%,	z - 0,1%	
Čeština:	e - 10,9%,	a - 9,6%,	o - 8,0%;
	w - 0,05%,	x - 0,03%,	q - 0,005%

- Pro zprávy kratší než 100 písmen frekvenční analýza selhává.

Substituční monoalfabetické šifry

Zdokonalené monoalfabetické šifry

- Umísťování klamačů na různá místa textu, znaky pro slova
  To nepomohlo - viz. poprava Marie Stuartovny, 1587, Anglie
- Šifrování po slabikách
  Velká šifra - otec a syn Rossignolové, 1650-1680, Francie.
  Jejich šifrová abeceda měla 587 různých znaků (trojčíslí).
  Dopisy králů Ludvíka XIII a Ludvíka XIV odolávaly rozluštění dalších 200 let.
- Homofonní substituční šifra
  17. stol., Evropa

Substituční monoalfabetické šifry

Homofonní substituční šifra

- Každému písmenu je přiřazeno tolik znaků (dvojčíslí), kolik je jeho průměrná četnost v daném jazyce. Tím se dosáhne průměrné četnosti 1% u každého znaku šifrového textu.
- Patří mezi monoalfabetické šifry, neboť šifrová abeceda je stejná v celém textu (témuž znaku šifrového textu odpovídá stejné písmeno otevřeného textu).
- K rozluštění lze použít frekvenční analýza pro dvojice písmen. Angličtina má časté kombinace: ee, th, qu
  Přitom písmeno q (výskyt 0,1%) je následováno jedině písmenem u (výskyt 2,8%). V šifrovém textu bude jediný znak pro q následován jedním ze tří znaků pro u.

Substituční polyalfabetické šifry

Polyalfabetické šifry

- Leon Battista Alberti, 1460, Itálie
  Navrhl pravidelné střídání dvou šifrových abeced.
- Blaise de Vigenère, Traktát o šifrách, 1586, Francie
  Navrhuje střídání více šifrových abeced podle domluveného klíče.
- Vigenèrova šifra připadala jeho současníkům složitá na používání. Ujala se za 200 let a rozšířila se s vynálezem telegrafu, 1851. (Tehdy vznikla i Morseova abeceda.)

Substituční polyalfabetické šifry

Vigenèrova šifra

- Vigenèrova šifra používá Vigenèrův čtverec všech posunutých šifrových abeced o distanci d, kde $1 \leq d \leq 26$.
- Klíčové slovo se opakovaně napíše nad otevřený text. Písmeno "P" klíčového slova udává posun příslušného písmene otevřeného textu - pro jeho zašifrování se použije abeceda v řádku začínajícím písmenem "P".
- Příklad: Klíčové slovo je "chléb".

Klíčové slovo	c	h	l	e	b	c	h	l	e	b	c	h
Posun o d	2	7	11	4	1	2	7	11	4	1	2	7
Otevřený text	v	e	n	i.	v	i	d	i.	v	i	c	i.
Šifrový text	X	L	Y	M.	W	K	K	T.	Z	J	E	P.

Substituční polyalfabetické šifry

Vigenèrův čtverec

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
:																									
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
:																									
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
:																									
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

Substituční polyalfabetické šifry

Prolomení Vigenèrovy šifry

- Charles Babbage, 1854, Anglie (během Krymské války); publikoval Friedrich Wilhelm Kasiski, 1863, Prusko.
- Všímáme si opakujících se slov v šifrovém textu a jejich vzdáleností. Jsou-li to delší slova (aspoň čtyřpísmenná), je pravděpodobné, že odpovídají témuž otevřenému slovu a že byla zašifrována stejnou šifrovou abecedou.
  Jejich vzdálenosti v_i jsou násobkem délky klíčového slova, tipujeme délku klíčového slova $l = \gcd(v_1, \ldots, v_k)$.
- Rozdělíme text na l podtextů zašifrovaných vždy stejnou abecedou a použijeme frekvenční analýzu.

Substituční polyalfabetické šifry

Vývoj do 1. světové války

- Vynález rádia, Marconi, 1894 - snadná komunikace a také snadný odposlech. Velký tlak na rozvoj kryptografie.
- Během 1. světové války bylo vymyšleno mnoho šifer, ale všechno byly jen variace na staré téma a brzy byly prolomeny. (Zimmermannův telegram do Mexika o útoku Němců na USA)
- Jednorázová tabulková šifra (One-Time-Pad-Code)
  Navrhl Joseph Mauborgne, 1918, USA.
  Patentoval Gilbert Vernam, 1919, Bellovy laboratoře, USA.

Substituční polyalfabetické šifry

Jednorázová tabulková šifra

- Používá náhodný klíč stejné délky jako je otevřený text, klíč určuje výběr abecedy (=posun pro dané písmeno jako u Vigenèrovy šifry).
- Klíč musí být skutečně náhodný, pokud by obsahoval smysluplná slova, je tu prostor pro frekvenční analýzu.
- Odesílatel i příjemce musí mít stejnou knihu náhodných klíčů a každý klíč lze použít pouze jednou.

Substituční polyalfabetické šifry

Jednorázová tabulková šifra

- Vernam patentoval šifru pro binární slova. Posun o 0 či o 1 zařídí $\oplus$ (logické *XOR*), aneb součet modulo 2.
- Šifrování i dešifrování pomocí klíče k se provede stejně: $a \to a \oplus k = b;\ \ b \to b \oplus k = a$.
- Pokud bychom jeden klíč použili dvakrát, získáme z šifrových zpráv jistou informaci o otevřených zprávách: $(a_1 \oplus k) \oplus (a_2 \oplus k) = a_1 \oplus a_2$

Substituční polyalfabetické šifry

Jednorázová tabulková šifra

Jednorázová tabulková šifra je *nerozluštitelná!*

Kdybychom stihli vyzkoušet všechny klíče (je jich 26^d, kde d je délka zprávy), tak získáme i všechny smysluplné texty délky d. Nevíme ale, který z nich byl poslán!

Praktické potíže:

- výroba klíčů - musí být opravdu náhodné
- distribuce klíčů - musí být opravdu každý použit jen jednou

Používáno pro horkou linku mezi Washingtonem a Moskvou.

Šifrovací stroje

- Šifrovací disky se používaly pro šifrování od 15. století (Alberti, 1460, Itálie).
- Jedná se o dva disky umístěné na společné ose tak, aby se jimi dalo nezávisle otáčet. Na vnějším disku byla otevřená abeceda, na vnitřím šifrová abeceda.
- Vhodné pro Caesarovu posunovou šifru i pro Vigenèrovu šifru (po zašifrování jednoho písmene pootočíme disk tak, aby pod písmenem A otevřené abecedy bylo další písmeno hesla, které určuje šifrovou abecedu).

Enigma

- Nejslavnějším šifrovacím strojem je Enigma, kterou používalo Německo během 2. světové války.
- Enigmu vynalezl německý podnikatel Arthur Scherbius, 1918. Byl to jakýsi "psací stroj" o rozměrech 34x28x15 cm a váze 12 kg.
- Kvůli vysoké ceně o ni zpočátku neměla zájem ani armáda, ani obchodní sféra. Německá armáda ji začala používat až v roce 1926.

Enigma

Popis Enigmy

- Enigma se skládala z klávesnice pro otevřený text, tří otočných disků (scramblerů) a signální desky pro šifrový text.
- Vzadu byla umístěna deska (reflektor), která vracela signál zpět přes scramblery odlišnou cestou, což umožnilo umístit signální desku nad klávesnici.
- Propojení drátů od klávesnice skrze scramblery k žárovkám signální desky udává bijekci otevřené abecedy na šifrovou abecedu.
- Otevřený text se psal na klávesnici a to rozsvěcelo písmena šifrového textu na signální desce.

Enigma

Popis Enigmy

- Po napsání jednoho písmene se první scrambler otočí "o jedno písmeno", čímž se změní šifrová abeceda.
- Scramblery se používají jako "jednotkové, desítkové, stovkové" - poté, co se první scrambler otočí o 360°, otočí se druhý scrambler o 1/26 z 360°, pak se opět otáčí první scrambler, atd.
- Jedná se tedy o polyalfabetickou šifru s $26^3 = 17\ 576$ šifrovými abecedami. To zaručí odolnost vůči frekvenční analýze.

Enigma

Popis Enigmy

- Počáteční nastavení scramblerů (= jaké písmeno je nahoře) udává klíč k šifrování. Ovšem počet 17 576 klíčů je nízký.
- Scramblary jsou vyndavatelné a lze zaměnit jejich pořadí, pro tři scramblery je $3! = 6$ možností.
- Mezi klávesnicí a scramblery je pevná propojovací deska, která propojuje dvanáct písmen do šesti dvojic. To nezvětší počet šifrových abeced, neboť deska je pevná, ale počet klíčů vzroste $\frac{1}{6!}\prod_{i=0}^{5}\binom{26-2i}{2} = 100\ 391\ 791\ 500$-krát.
- Celkový počet klíčů je zhruba 10^{16}, což zaručuje odolnost vůči prolomení hrubou silou.

Enigma

Šifrovací a dešifrovací klíč

- Reflektor (odrazová deska) způsobí, že k šifrování i dešifrování se používá stejné nastavení = stejný klíč.
- Denní šifrovací klíč sestává z nastavení scramblerů (např. H-Q-L), pořadí scramblerů (např. 2-3-1) a propojení dvojic (např. A/L - P/R - T/D - B/W - K/F - Q/Y).
- Denním klíčem se zašifroval aktuální klíč pro danou zprávu (=jen nastavení scramblerů, např. D-Y-G). Pak se scramblery přenastavily a šifrovala se daná zpráva.
- Klíče se v německé armádě distribuovaly jednou za měsíc v tzv. měsíčních knihách.

Enigma

Enigma

Boj s Enigmou - Polsko

- Polsko cítilo ohrožení od Německa, proto usilovně pracovalo na prolomení Enigmy už před 2. světovou válkou (1932-39).
- Díky špionáži měli k dispozici přístroj i dokumenty k němu. Šlo o to prolomit klíč.
- Marian Rejewski využil faktu, že Němci opakovaly aktuální klíč před zprávou dvakrát (např. D-Y-G-D-Y-G). Zašifrován byl tímtéž denním klíčem. Opakování je díra pro šperhák.

Enigma

Boj s Enigmou - Polsko

- Rejewski zpracoval mnoho zpráv zašifrovaných stejným denním klíčem. Ze tří dvojic zopakovaných znaků na jejich začátcích vytvořil řetězce šifrových znaků (cykly v bijekci šifrových abeced pro 1. a 4. písmeno atd.) a všiml si, že jejich délky jsou určeny pouze pořadím a nastavením scramblerů.
- Na prozkoumání všech $6 \cdot 26^3 = 105\ 456$ možností pracoval celý rok a sestavil katalog "délek řetězců".
- S katalogem byl připraven na dešifrování. Sestavil řetězce znaků přítomného dne, v katalogu našel příslušné pořadí a nastavení scramblerů denního klíče. Vyzkoušel dešifrování textu bez propojovací desky a pak už bylo snadné uhodnout šest přehozených dvojic písmen.

Enigma

Boj s Enigmou - Polsko

- Rejewski později sestavil stroj, který mechanicky hledal nastavení scramblerů pro dané řetězce znaků. Šest strojů s různým pořadím disků pracovalo paralelně a našlo odpovídající nastavení cca za dvě hodiny.
- V roce 1938 zvýšili Němci bezpečnost Enigmy tím, že vyrobili dva nové typy scramblerů - vybíraly se pak 3 z 5 možných, což je $5 \cdot 4 \cdot 3 = 60$ možností - a propojili 20 písmen do 10 dvojic. Poláci neměli peníze na postavení tolika dešifrovacích strojů.
- 24.7.1939 předali Poláci svoje výsledky francouzským a anglickým kryptografům.

Enigma

Boj s Enigmou - Anglie

- Alan Turing hledal způsob dešifrování, který by nezávisel na faktu, že aktuální klíč je dvakrát opakován. Využil řetězce znaků sestavené z "taháků" (např. denně v 6:05 Němci odesílali zprávu o počasí začínající slovem WETTER).
- Práci dokončil v březnu 1940, ale dešifrování denního klíče trvalo týden. Němci přestali opakovat aktuální klíč v květnu. Turing zdokonalil dešifrovací stroje (tzv. bomby, neboť při dešifrování tikaly) a od srpna téhož roku trvalo nalezení denního klíče pouze jednu hodinu.
- Angličané dešifrovali Enigmu i po válce, v 50.letech ji používali i jiné státy, např. SSSR. Veřejně odhalila Anglie své výsledky až v roce 1974.

Šifrování za 2. světové války

- Němci používali kromě Enigmy šifru Lorenz pro komunikaci Hitlera s hlavními veliteli. Angličané ji též prolomili. Japonci používali šifru Purpur.
- Američané neměli vymyšlenou šifru, ale používali jazyk Navahů, domorodého indiánského kmene, jehož struktura se naprosto liší od jakéhokoliv evropského či asijského jazyka.
- Vojáky, mluvčími kódu byli Navahové. Byli schopni naučit se nazpaměť obrovské množství nových slov (např. bojové letadlo = kolibřík, válečná loď = velryba, bomby = vejce). Šifrování a dešifrování pak probíhalo v reálném čase telefonického hovoru.
- Jazyk Navahů byl jeden z mála kódů v historii, který nebyl nikdy prolomen. Byl odtajněn vládou USA až v roce 1968.

Šifrování pomocí počítačů

- Dešifrovací stroje byly předchůdci počítačů (stroj Colossus na dešifrování šifry Lorenz, postavený z elektronek, 1943, Anglie).
- Vynález tranzistoru 1947 umožnil výrobu počítačů na zakázku. Firma IBM začala vyrábět počítače v roce 1953. V roce 1959 byl vynalezen integrovaný obvod. V 60. letech mělo počítače stále více firem a použílaly je i pro šifrování.
- Písmena jsou v počítači kódována v ASCII kódu jako binární slova (American Standard Code for Information Interchange, 1960-67, IBM, USA).
- Pro šifrování lze použít klasické šifry na úrovni bitů, tedy uvnitř písmene. Např. transpoziční šifra přehazující vždy dva sousední bity, Vernamova šifra atd. Lze také provádět různé číselné operace s binárními slovy.

Šifrování pomocí počítačů

Standardní šifrovací protokoly

- V roce 1973 vyhlásil Americký standardizační úřad soutěž o standardní šifrovací protokol pro USA. Hlavním kandidátem byl protokol Lucifer, jehož autorem byl Horts Feistel z IBM.
- NSA (=National Security Agency) tento protokol oslabila na 56-bitové klíče a tato verze byla oficiálně přijata v roce 1976 pod názvem DES (=Data Encryption Standard).
- DES pracuje s binárními slovy délky 64, rozdělí je na dvě části poloviční délky, jednu část prožene jistou funkcí a přičte druhou část, toto opakuje šestnáctkrát.

Šifrování pomocí počítačů

Standardní šifrovací protokoly

- Od roku 2002 se používá AES (=Advanced Encryption Standard). AES pracuje se slovy délky 128, která chápe jako matici bytů velikosti 4×4. Tuto matici posloupností několika operací s použitím 128−bitového klíče "prohněte".
- DES i AES jsou symetrické šifrovací protokoly, které používají k šifrování a dešifrování stejný klíč. Hlavním problémem používání těchto protokolů je distribuce klíčů. Dříve než nastane tajná komunikace, musí si obě strany jednu tajnou informaci sdělit, a to klíč.

Šifrování pomocí počítačů

Problém distribuce klíčů

- Whitfield Diffie, Martin Hellman, Ralph Merkle, USA, se snažili vyřešit problém distribuce klíčů.
- Diffie předpovídal vznik internetu a potřebu šifrovat, která zahrnovala širokou veřejnost. Distribuování klíčů pomocí agentů s kufříky by pak bylo nemožné.
- Trezor se dvěma zámky ("můj - můj a tvůj - tvůj") dokazuje, že tajná informace se dá vyměnit bez předchozí výměny klíčů. Ale šifrovací funkce nekomutují s dešifrovacími funkcemi!
- Hellman, 1976, navrhl protokol veřejné domluvy na tajném klíči používající diskrétní logaritmus. Diskrétní exponenciální funkce je jednosměrná funkce, skládání dvou exponenciálních funkcí komutuje ("míchání barev").

Šifrování pomocí počítačů

Problém distribuce klíčů

- Diffie, 1975, vymyslel šifrování s veřejným klíčem. Asymetrické klíče - veřejný klíč pro šifrování a tajný klíč pro dešifrování. K šifrování se použije jednosměrná funkce se zadními vrátky. (Rozešlu své zámky na všechny pošty a jen já si nechám klíč. Kdo mi chce poslat trezor, zamkne ho mým zámkem.)
- Výhody - není nutná synchronní komunikace při domlouvání klíče. Veřejný klíč je stále dostupný v "telefonním seznamu". Každý má jediný klíč pro komunikaci se všemi ostatními. Soukromý klíč je možné použít k digitálnímu podpisu zpráv.
- Článek byl převratem v kryptologii, ale konkrétní návrh protokolu s veřejným klíčem Diffie neměl.

Problém distribuce klíčů

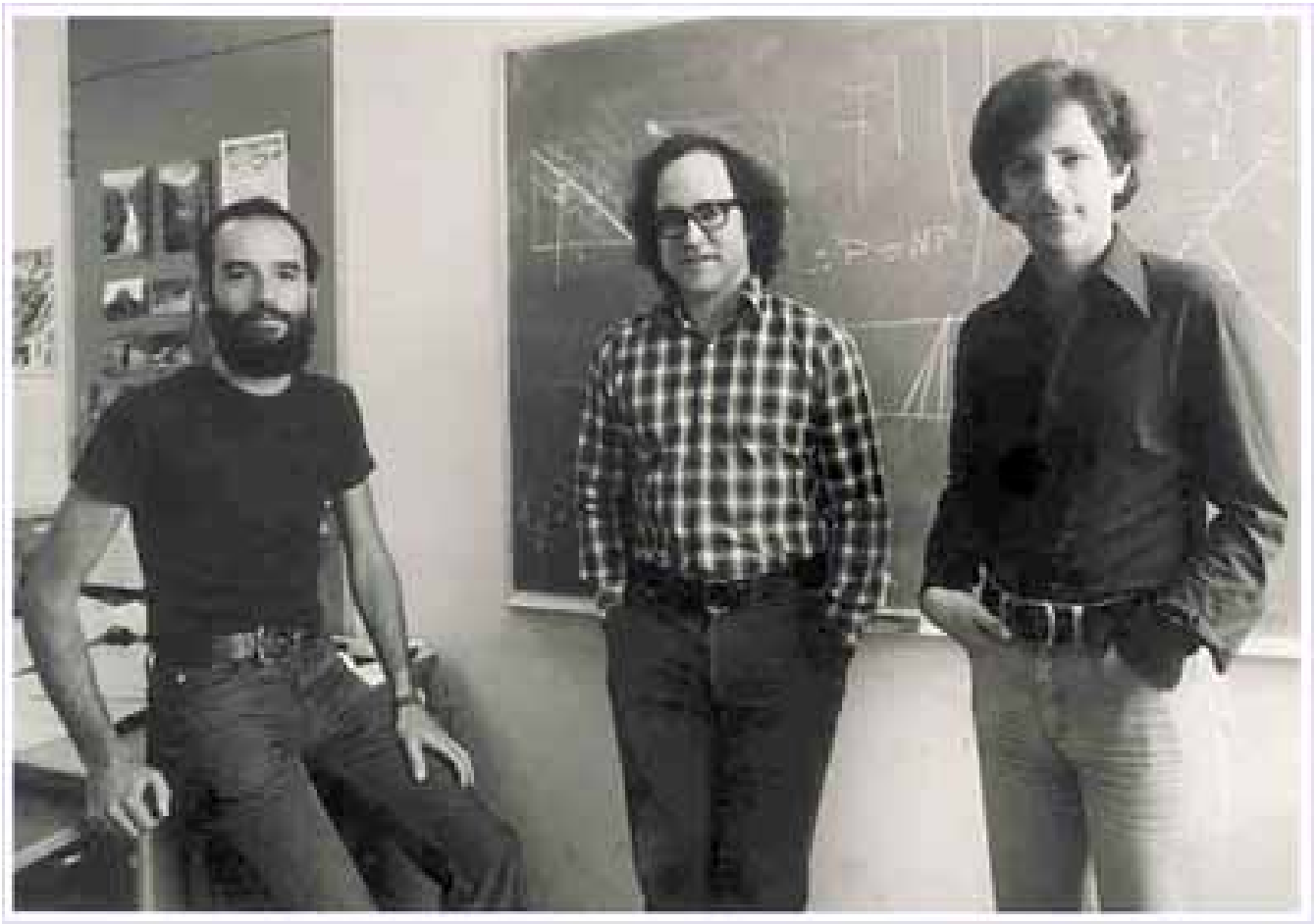
Ralph Merkle, Martin Hellman, Whitfield Diffie

Šifrování pomocí počítačů

Šifrování s veřejným klíčem

- Ronald Rivest, Adi Shamir, Leonard Adleman, USA, patentovali první šifrovací protokol s veřejným klíčem.
- Protokol RSA využívá problém faktorizace. Jednosměrnou funkcí je diskrétní mocnina a zadní vrátka otvírá Euler-Fermatova věta.
- Článek byl zveřejněn v časopise Scientific American v r. 1977 spolu se soutěží na dešifrování s modulem $n = pq \doteq 10^{129}$ za odměnu 100 dolarů. Modul n byl faktorizovám po sedmnácti letech společným úsilím mnoha počítačů.

Šifrování s veřejným klíčem



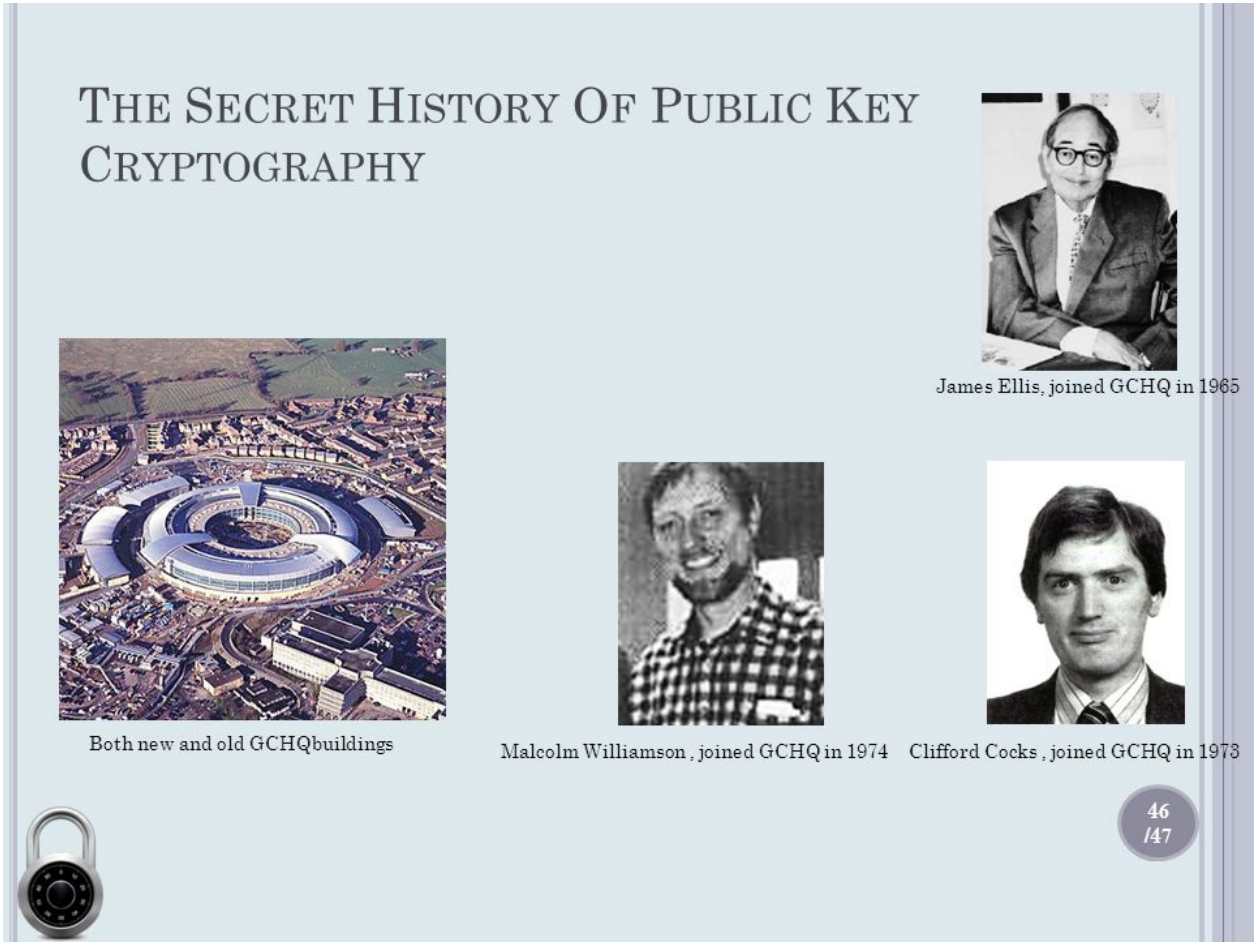
Adi Shamir, Ronald Rivest, Leonard Adleman

Šifrování pomocí počítačů

Šifrování s veřejným klíčem

- James Ellis, Clifford Cocks, Malcolm Williamson, Anglie, členové GCHQ (=Goverment Communication Headquater), vymysleli totéž, ale jejich výzkumy byly přísně tajné.
- Ellis, 1969 - myšlenka šifrování s veřejným klíčem (tzv. šifrování bez utajení).
- Cocks, 1973 - našel jednosměrnou funkci opírající se o problém faktorizace (protokol RSA).
- Williamson, 1975 - našel veřejnou domluvu na tajném klíči opírající se o problém diskrétního logaritmu (protokol Diffie-Hellmanův).
- Tyto výsledky byly zveřejněny až v roce 1997.

Šifrování s veřejným klíčem



James Ellis, Malcolm Williamson, Clifford Cocks

Šifrování pomocí počítačů

Docela dobré soukromí

- Phil Zimmermann, USA, 1991, zveřejnil software pro PC nazvaný PGP (=Pretty Good Privacy), který používá RSA šifrování k výměně symetrického klíče a vlastní zprávy pak šifruje rychleji symetrickou šifrou IDEA.
- Software PGP umí také generovat klíče pro RSA a umí připojit digitální podpis zpráv.
- Zimmermann umístil PGP na web k volnému stažení a byl za to obžalován z ilegálního vývozu zbraní. Později byl obžaloby zproštěn.
- Otázka zní: Má občan právo na soukromí nebo má stát právo na odposlech kvůli zajištění bezpečnosti?

Kvantové šifrování

Kvantové počítače

- Pokud se podaří vyrábět kvantové počítače, tak bezpečnost známých šifrovacích protokolů padá.
- David Deutsch, 1984 - první myšlenka kvantového počítače.
- Peter Shor, 1994 - kvantová faktorizace v polynomiálním čase (konec bezpečnosti RSA).
- Lov Grover, 1996 - kvantové prohledávání seznamů v polynomiálním čase (prohledá všechny klíče pro AES).

Kvantové šifrování

Kvantová distribuce klíčů

- Stephen Wiesner, Charles Bennett, Gilles Brassard, 1984, USA, vymysleli kvantovou domluvu klíče.
- Pomocí měření polarizace fotonů se dá domluvit na libovolně dlouhém tajném klíči. Navíc jakýkoliv odposlech se pozná, neboť změní polarizaci fotonů.
- Klíč se pak může použít pro jednorázovou tabulkovou šifru, která je (v případě náhodného klíče) nerozluštitelná.
- V roce 1995 se podařilo implementovat kvantovou domluvu klíče pomocí optického vlákna v Ženevě na vzdálenost 23 km.

Dějiny kryptografie

Literatura

- Simon Singh: Kniha kódů a šifer. Nakladatelství Dokořán a Argo. Praha 2009.