Časová osa Chipu: Šifrování

Dokážete **UDRŽET TAJEMSTVÍ**? Již více než 2 500 let se o to pokoušejí vládci, tajné služby a kryptologové.

MARKUS MANDAU

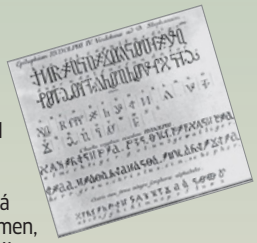
Dlouhá léta bylo šifrování doménou nejvyšších politiků, dnes je používáme všichni: při přístupu do banky, ale i k e-mailu nebo při surfování. Bez algoritmů, které znemožňují odposlech komunikace, by na internetu nebylo možné provozovat služby, které denně používáme.

Přitom principy, na kterých jsou založené dnešní metody, jsou staré tisíce let. Za Ceasara se šifrovala jednotlivá písmena, dnes jsou to bity. Římský vojevůdce chránil svou korespondenci tak, že písmena byla posunutá v abecedě o určitý počet. Místo A se použilo D, místo B se použilo E a tak dále. Tato jednoduchá substituční monoalfabetická šifra byla populární až do 9. století. Není divu – většina lidí stejně neuměla číst, takže i takto jednoduché zašifrování bylo bezpečné. Prolomení šifry je velmi jednoduché a lze k němu použít třeba frekvenční analýzu. Vysvětlení: Čeština je typická tím, že obsahuje velmi často znak E. Pokud by E bylo zakódováno jako H, text by obsahoval velmi mnoho těchto písmen, kterých se běžně vyskytuje jen málo. Z toho by bylo možné rychle vypočítat posun.

Dějiny šifrování

Skytale

Sparťané psali důležité zprávy na pergamen, který se musel natočit na tyč správné tloušťky. Pokud byla tloušťka jiná, zpráva nebyla čitelná.



Alphabetum Kaldeorum

Rudolf IV. vynalezl nejznámější šifrování používané ve středověku. Používá se nahrazování písmen, přičemž ta nejčastěji používaná měla několik náhrad – tím bylo možné obejít frekvenční analýzu.

Enigma

Nejznámější šifrovací stroj, který se proslavil ve 2. světové válce. Používal polyalfabetickou šifru a dlouhou dobu byl neprolomitelný.

Kerkhoffův princip

Bezpečné šifrování není otázkou utajení algoritmu, ale utajení klíče.

400 před Kristem | 50 před Kristem | 1360 | 1467 | 1585 | 1854 | 1881 | 1918

Caesarova šifra

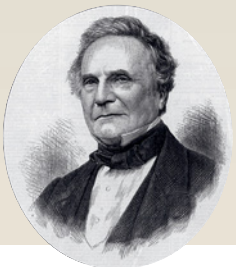
Římský vojevůdce posouval písmena v abecedě o tři pozice dozadu. Dnes je tento způsob označován jako monoalfabetické šifrování.

Vigenèrova šifra

Blaise de Vigenère přišel s polyalfabetickou šifrou, kdy každé písmeno mohlo být zakódováno různými znaky. Princip šifry nebyl prolomen 300 let.

Charles Babbage

Vynálezce programovatelného počítače. Prolomil Vigenèrovu šifru, ale nikomu to neprozradil. Zjistilo se to až po jeho smrti.



One-Time-Pad

Matematicky bezpečné: Pomocí malého číselníku se text zašifruje pokaždé jinak. Hlavní nástroj špionů v době studené války.

Šifrovací kolo

Pomůcka pro zašifrování a rozšifrování monoalfabetického šifrování.

FOTO: JÖRG BROBICK; ELECTRONIC FRONTIER FOUNDATION; MAGNUS MANSKE; NSA; WIKIPEDIA/ ANDREW BOSSI, LURINGEN, JOHN RAINERI

Mnohem účinnější substituční polyalfabetickou šifru vymyslel Francouz Blaire de Vigenère. Ten bojuje proti frekvenční analýze tím, že jednou by písmeno E bylo zašifrováno jako H, ale podruhé už jako U. Na podobném principu pracovaly šifrovací stroje ještě ve 20. století, třeba včetně známé Enigmy.

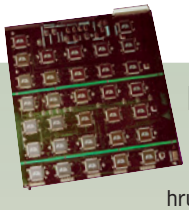
Každou šifru lze prolomit

S příchodem počítačů se všechno změnilo. Na jednu stranu roste náročnost algoritmů, takže bez počítače by i geniálnímu matematikovi trvalo velmi dlouho, než by zprávu rozkódoval, byť se znalostí hesla. Zároveň s tím ale roste výkon počítačů a útoky hrubou silou dokážou jednoduché algoritmy rozlousknout za několik sekund. Kryptologové vycházejí z Kerckhoffova principu: Metoda šifrování je bezpečná, pokud je kromě hesla známý celý algoritmus. Tento open-source koncept má tu výhodu, že kvalitu algoritmu může kdokoliv otestovat. Rovněž je možné zkoušet různé typy útoků, které jsou pro šifrování žádoucí – dokážou najít slabá místa. Díky tomuto principu bylo v roce 1998 prokázáno, že 56bitový klíč je pro šifrování DES (Data Encryption Standard) příliš krátký. Přitom se jedná o algoritmus používaný úřady USA. Nový, rychlý hardware dokáže takový klíč prolomit hrubou silou.

Následovník DES vzešel ze soutěže. Stal se jím algoritmus Rijndeal. Ten je spíše známý pod zkratkou AES a používá 128bitový klíč. Setkáváte se s ním denně: třeba při bezpečném přístupu k Wi-Fi síti nebo při přehrávání Blu-ray. Tento algoritmus má jednu nevýhodu: používá symetrický klíč – stejný klíč se používá jak pro zašifrování, tak pro dešifrování. Tím je nevhodný pro použití na internetu. Strany vyměňující si informace by musely mít stejný klíč. Ale jak jej získat? Musí jej poslat. Nešifrovaně?

V 70. letech se uvažuje o asymetrické šifře, jejíž model vypadá takto: Příjemce zprávy vygeneruje veřejný a soukromý klíč. Veřejný klíč dá k dispozici ideálně úplně každému. Odesílatel pak pomocí tohoto veřejného klíče zašifruje zprávu a tu odešle. Zašifrovanou zprávu lze dešifrovat jen pomocí soukromého klíče. Dvojce klíčů se počítá jako součin obrovských prvočísel. A jelikož není známý jednoduchý algoritmus pro rozklad čísla na prvočinitele, je časově velmi náročné odvodit z veřejného klíče klíč soukromý. Nevýhoda: Klíče jsou opravdu obrovské a šifrování je časově náročné. Proto se třeba při přístupu do banky postupuje tak, že se vygeneruje symetrická šifra, která je krátká. Ta se asymetricky zašifruje, pošle se druhé straně a další komunikace je pak šifrována symetrickou šifrou, která již není tak výpočetně náročná. Vzhledem k růstu výkonu počítačů však žádná z metod není neprolomitelná. Jistotu přinese až kvantové šifrování, při kterém se uplatňuje Heisenbergův princip neurčitosti. Je to stejné jako se Schrödingerovou kočkou. Kanálem se pošle symetrický klíč. A pokud se na něj někdo podívá – tedy někdo jej odposlechne ještě předtím, než se dostane k adresátovi, klíč se automaticky zneplatní. K šifrování bude použit až takový klíč, který nebyl odposlechnut.

AUTOR@CHIP.CZ

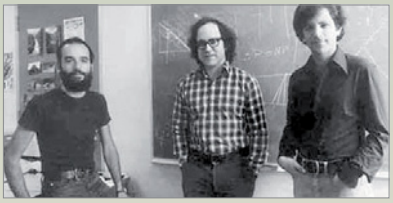


Fialka

Ruský šifrovací stroj z dob studené války. Byla to východní podoba Enigmy. Prolomena byla o dva roky později.

Deep Crack

Organizace Electronic Frontier Foundation postavila počítač s 1 800 procesory, který hrubou silou prolomil DES.



RSA

Rivest, Shamir a Adleman – tito tři lidé stojí za oblíbenou asymetrickou šifrou. Používá se pro šifrování e-mailů i digitální podpisy.

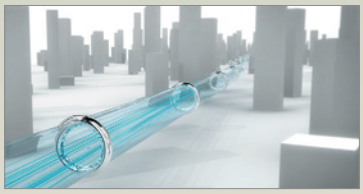
BUDOUCNOST

Trend: Kvantové počítače

Počítače jsou tak rychlé, že všechny šifrovací algoritmy jsou prolomeny během několika sekund. Jediné bezpečné šifrování poskytnou kvantové počítače.

Kvantová kryptografie

Ve Vídni se otevírá prezentační místo, které na optickém vlákně předvádí kvantové šifrování.



1940 · 1965 · 1973 · 1976 · 1977 · 1998 · 2000 · 2008 · 2030

Veřejný klíč

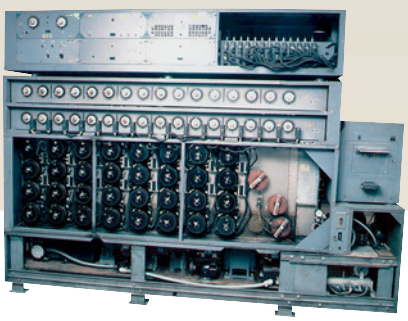
Tři zaměstnanci britské zpravodajské služby vymysleli první asymetrické šifrování. Tato skutečnost byla utajena až do roku 1997.

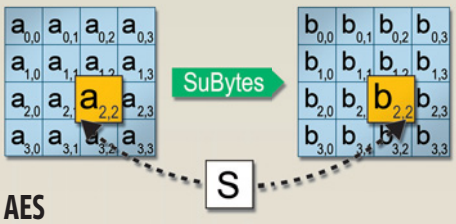
DES

Ze spolupráce NSA a IBM vzešel Data Encryption Standard, používaný všemi americkými úřady. Kritici si stěžují na zkrácení klíče ze 128 na 56 bitů.

Turingova bomba

Alan Turing přišel se strojem, který prolomil Enigmu. „Bomba" byla složena z mnoha samostatných strojů Enigma.





AES

V otevřeném výběrovém řízení byl jako nástupce DES vybrán algoritmus Rijndeal. Advanced Encryption Standard je nejpoužívanější šifrovací metoda současnosti.