# Historie Kryptografie

***Co je kryptografie?***

*Kryptografie* je věda o šifrování dat za pomoci matematických metod. S tímto pojmem musíme ještě zavést pojem *kryptoanalýza*. Kryptoanalýza se snaží bez znalosti klíče dojít k utajovaným datům. Ke kryptoanalýze je třeba mnoho analytického myšlení, aplikace matematických metod, hledání cestiček, trpělivosti a štěstí.

Kryptografie a kryptoanalýza spolu tvoří jeden obor nazývaný *kryptologie*.

***Důvody pro šifrování komunikačních kanálů***

Důvodem pro šifrování je nutnost přenosu citlivých či tajných dat přes nezabezpečené prostředí. Takovým prostředím může být např. Internet, či jiná veřejná datová síť. Příkladem může být šifrování e-mailů s důvěrnými informacemi nebo elektronické platby

V zásadě rozeznáváme dva druhy šifrování. A to šifrování s tajným klíčem a šifrování s veřejným klíčem. Oba dva jsou pro bezpečnost důležité. Šifrování s veřejným klíčem je výpočetně a matematicky náročnější.

***Kryptoanalýza a útoky***

Kryptoanalýza je stará jako kryptografie sama. Existuje velké množství kryptoanalytických metod. Kerckhoffův princip zní: *Spolehlivost šifrovacího systému nesmí záviset na utajení algoritmu. Spolehlivost je založena pouze na utajení klíče.*

Vyjmenuji zde alespoň některé metody.

*Útok hrubou silou* – nejuniversálnější princip, kdy jsou zkoušeny všechny možné klíče. Metoda je tím méně efektivní, čím delší je klíč.

*Lineární kryptoanalýza* - šifrovací text aproximujeme vhodnou lineární funkcí otevřeného textu.

*Diferenciální kryptoanalýza* - je založená na tom, že cíleně zkoumáme určité páry šifrovacích textů a to těch, jejichž otevřené protějšky vykazují určité diference (rozdíly). Pak se postupně zkoumá, jakým způsobem se tyto diference v průběhu šifrovacího algoritmu mění a na tomto zjištění se různým klíčům přiřadí různé pravděpodobnosti. Pokud analyzujeme dostatečně velký počet dvojic, "otevřený text – šifrovaný text", obdržíme jeden klíč jako nejpravděpodobnější. Tento klíč je pak hledaný správný klíč.

*Diferenciálně-lineární kryptoanalýza* - ta je kombinací diferenciální a lineární analýzy. Pro tento typ útoku stačí podstatně menší počet dvojic otevřený text – šifrovací text, nevýhoda je v tom, že je omezena na malý počet kol.

*Timing attack* – je založený na přesném změření času potřebném pro operace se soukromým klíčem.

### *Export šifer*

S šiframi je zacházeno v mnoha zemích jako se zbraněmi. Vláda USA zakazuje export šifrovacích algoritmů, které nemají "zadní vrátka". Stanovila hranici 40 bitů klíče u symetrických algoritmů a 512 bitů klíče u asymetrických.

Například SSL s 40 bitovým algoritmem již bylo rozlousknuto za 31 hodin. Proto mnohé firmy vyvíjejí své algoritmy mimo území USA, aby nezapadali do regulované části trhu. Na tato vývozní opatření lze vyzrát tak, že budou programy vyvezeny jako literární dílo a pak přepsány, slinkovány s knihovnami v zahraničí. Takto bylo vyvezeno např. PGP.

"Silné" šifry jsou takové, které dokážou odolat všem kryptoanalytickým metodám kromě útoku hrubou silou. Obranou proti útoku hrubou silou je zvětšení délky klíče, aby se vyčerpávající prohledávání uskutečnilo v čase, který není realizovatelný, neboli je "výpočetně neproveditelný".

Obecně jsou za silné považovány kvalitní symetrické šifry s délkou klíče nad 70 bitů a u asymetrických šifer typu RSA s délkou klíče nad 700 bitů.

Vůbec žádné šifry (resp. software šifry užívající) se nesmí vyvážet do tzv. teroristických zemí.

### *1. Symetrické šifrování*

Symetrické, též konvenční šifrování je založeno na principu jednoho klíče, kterým lze zprávu jak zašifrovat, tak i odšifrovat. Příkladem symetrického klíče je DES (Data Encryption Standard) vyvinutý v 70. letech v USA a americkou vládou také hojně používaný. Symetrické kódy mají jako hlavní výhodu rychlost algoritmu. Na druhou stranu je nutné aby se příjemce i odesílatel dohodli na jednom klíči, který budou znát *pouze* oni dva. Problémem je tedy distribuce klíče - jak dostat klíč k příjemci aniž by se ho chopil někdo nepovolaný?

Velmi jednoduchou a známou aplikací symetrického klíče je tzv. *Ceasarova šifra.* Její princip je v tom, že je provedeno abecední posunutí po písmenech a klíčem je číslo, o kolik se písmeno posune.

Např.: Klíč = 3
ABCDEFGHIJKLMNOPQRSTUVWXYZ
DEFGHIJKLMNOPQRSTUVWXYZABC
Tedy AHOJ = DKRM

### *Blowfish*

Autorem algoritmu Blowfish je B. Schneier, který jej publikoval v roce 1993. Tento algoritmus není patentován a je volně šiřitelný. Jde o velmi rychlý, jednoduchý algoritmus, který je možno efektivně implementovat i na malých procesorech, nebo dokonce čipových kartách. Při pečlivém naprogramování se to všechno včetně všech svých datových struktur vejde do interní cache procesoru i486.

*Jde o blokovou šifru s délkou bloku 64 bitů a klíči dlouhými maximálně 448 bitů.*

Algoritmus je použitelný ve všech běžných pracovních modech vhodných pro blokové šifry. Míru dosažené bezpečnosti lze regulovat délkou použitého klíče. Rovněž lze omezit počet kol šifrovacího procesu. Snížení počtu kol vede k jistému snížení odolnosti vůči lineární a diferenciální kryptoanalýze, výhodou je ovšem vyšší rychlost šifrování. Naopak se nezdá, že by další zvyšování počtu kol mělo zásadní vliv na zvýšení bezpečnosti algoritmu.

***CAST***

Vývoj CASTu reagoval na neutěšenou situaci na poli šifrovacích algoritmů v polovině 90. let. DES měl v té době už svá nejlepší léta za sebou, a ostatní kvalitní šifry byly patentovány a tudíž drahé (např. IDEA, RC2, RC4). Na internetu byl publikován v květnu 1997 jako *RFC 2144.* CAST se tak stal kanadskou alternativou k americkému algoritmu Blowfish. Oproti Blowfishi měl CAST výhodu,že dostal certifikát kvality od oficiálního kanadského úřadu pro komunikaci CSE (Communication Security Establishment), používá ho Microsoft ve svých produktech a také je začleněn do PGP (Pretty Good Privacy).

*CAST umí pracovat s klíči od 40 do 128 bitů a bloky o 64 bitech.* Algoritmus pracuje na Feistelově principu, tzn. že algoritmus pracuje v cyklech totožných operací, které se nazývají rundy (rounds). Algoritmus má buď 12 rund (pro 80-bitový klíč) nebo 16 rund (pro 128-bitový klíč). Dalším principem CAST je substitučně-permutační síť. Znamená to, že jsou bity jak posouvány, tak nahrazovány jiným sledem bitů. CAST má 4 substituční boxy (S-boxy), které převádějí 8 bitů na 32 bitů. Toto rozšíření je kryptografická vymoženost 90. let a objevuje se v mnoha algoritmech.

CAST nyní představuje standard, který je velmi rozšířen a akceptován mnoha společnostmi. Akceptuje jak silné, tak slabé klíče a je velmi bezpečný. Prozatím vyplňuje mezeru, než bude vybrán nový šifrovací standard.

***DES***

V roce 1974 byl vyvinut algoritmus LUCIFER firmou IBM a stal se kandidátem na americký standard šifrování dat. Posléze v roce 1977 byl jako federální standard přijat a pojmenován DES – Data Encryption Standard.

*Algoritmus je blokový a šifruje 64 bitů otevřeného textu na 64 bitů šifry. Klíč je 64 bitový*, ale každý osmý bit je kontrolní, tedy efektivní délka klíče je 56. Kvůli vyšší bezpečnosti byl přijat standard Triple DES (též TDES, 3DES), který jedna data protáhne algoritmem 3x. Potom je efektivní délka klíče 128 bitů. DES je jednou z nejnapadanějších šifer.

***IDEA***

Autory algoritmu publikovaného v roce 1991 původně pod názvem IPES byli X. Lai a J. Massey. Současný název je akronymem za International Data Encryption Algorithm. IDEA vznikla jako vylepšená verze svého předchůdce, algoritmu PES poté, co byla publikována metoda jeho zlomení. Je implementována v rámci protokolu SSL nebo jako součást PGP.

*Jde o blokovou šifru s délkou bloku 64 bitů, pracující s klíčem o délce 128 bitů.*

***MARS***

Vytvořen byl stejně jako DES firmou IBM. Podle tvůrců MARS nabízí větší bezpečnost než Triple-DES s neporovnatelnou rychlostí.

*Mars je šifra s délkou bloku 128 bitů a proměnlivou délkou klíče.* MARS pracuje s 32 bitovými slovy – kvůli optimalizaci registrů. Používá principy Feistelovy sítě, kdy 4 části bloku podrobuje opakovaně jednotlivým operacím. Substituční S-box je o 512 položkách dlouhých 32 bitů. Dalším důležitým bezpečnostním prvkem jsou datově závislé rotace. Ty jsou velice odolné kryptoanalýze a velmi dobře hardwarově a sofwarově implementovatelné.

***RC4 – Rivest Cipher 4***

Autorem je Donald Rivest.

RC4 je jednou z nejpoužívanějších proudových šifer pro internet a komerční využití. Po celých 7 let se RSA dařilo utajit algoritmus RC4. Poté její popis nějaký hacker a umístil na internetu (v diskusní skupině *cyberpunks*). RSA dostala strach o zneužití jejich šifry konkurencí, jelikož nebyla patentována. Tato šifra je řádově 10x rychlejší než DES.

RC4 je využita v SSL 3.0 společnosti Netscape, v Microsoft Office, ORACLE Secure SQL nebo v Microsoft Windows 2000.

*Klíč pro RC4 může mít maximálně 256 bytů (2048 bitů).* Pro funkčnost se uvažuje o klíčích zarovnaných na byty. V praxi se využívá 128bitový klíč na území USA a 40bitový. Vstupem je klíč o volitelné délce. Princip šifry je míchání bytů klíče spojené s permutací klíče.

RC4 je velmi zajímavá a neobyčejná a analytickou metodou zatím nenapadnutá šifra. Ani teoretický základ šifry není doposud řádně prozkoumán.

***RC5 – Rivest Cipher 5***

Druhý algoritmus z dílny Ronalda Rivesta z roku 1994. RC5 přinesl do kryptografie novou myšlenku o použití rotací závislých na datech. Jedná se o velmi pružný algoritmus s mnoha parametry.

*Šifrovací klíč má 0-255 bytů, počet kol šifrovacího procesu (0-255) a délka slova z hodnot 16, 32, 64, 128 a 256 přičemž algoritmus zpracovává bloky o dvojnásobné délce slova.*

***RC6 – Rivest Cipher 6***

Algoritmus RC6 je vylepšená verze RC5. Byly přidány některé funkce, celočíselné násobení v klíči a čtyři pracovní registry místo dvou.

***SKIPJACK***

23. června 1988 NSA (National Security Agency) velmi překvapivě odtajnilo dva kryptografické algoritmy ze své dílny jež do té doby velmi pečlivě střežila. Tím prvním je Skipjack, druhým je asymetrický KEA (Key Exchange Algorithm). Původně tyto algoritmy měly být realizovány pouze chráněným hardwarem. Velké požadavky na bezpečnost pro

americký vojenský DMS (Defense Message System) však splnila pouze PC karta Fortezza™ a její varianta Fortezza™ Plus. Protože výroba těchto karet pouze na zakázku by byla drahá i pro US ministerstvo obrany, vypustila NSA Skipjacka a KEA na konkurenční prostředí.

*Skipjack je 64bitová symetrická šifra s 80bitovým klíčem.* Celkem 64 bitů otevřeného textu projde 32 šifrovacími rundami.

### *TWOFISH*

*Twofish pracuje s blokem o délce 128 bitů a proměnlivou délkou klíče až do 256 bitů.* Základními stavebními kameny této šifry jsou Feistelova síť, S-boxy, MDS matice (zajišťují bezpečné transformace klíčů), pseudo-Hardamanovy transformace (jednoduché mixovací operace převádějící dva vstupy na 32-bitový výstup).

## *2.ASYMETRICKÉ KRYPTOVACÍ ALGORITMY*

Asymetrické algoritmy nazýváme též algoritmy s veřejným klíčem. Princip těchto algoritmů je v tom, že pro každého uživatele existuje dvojice klíčů: ***veřejný a tajný.***

*Veřejný klíč* je všeobecně komukoliv dostupný. Tímto klíčem lze pouze zašifrovat zprávu pro určitého uživatele.

*Tajný klíč* má každý u sebe schovaný a určitým způsobem chráněný proti ukradení (heslem, na čipové kartě, na magnetické kartě). Tímto tajným klíčem lze provádět odkódování přijatých zpráv. Tedy, je-li zpráva pouze pro mě, tak pouze já svým tajným klíčem ji mohu odšifrovat.

Z hlediska bezpečnosti je nutné podotknout, že teoreticky je možné z veřejného klíče u všech algoritmů vypočítat klíč tajný. Ale dosud je to výpočetně neproveditelné. Se současným výkonem počítačů by se jednalo o tisíciletí. Existují návrhy na zefektivnění kryptoanalýzy – např. TWINKLE pro RSA, ale pro rozumný počet bitů klíče jsou algoritmy stále bezpečné.

### *RSA*

RSA byl objeven roku 1977 a jeho autoři jsou Ron Rivest, Adi Shamir a Joe Adleman – odtud RSA. Systém je založen na teoreticky jednoduché úvaze: *Je snadné vynásobit dvě dlouhá (100-místná) prvočísla, ale bez jejich znalosti je prakticky nemožné zpětně provést rozklad výsledku na původní prvočísla.* Součin těchto čísel je tedy veřejný klíč. Přitom obě prvočísla potřebujeme pro dešifrování. Algoritmus RSA je též používán k digitálním podpisům.

### *Diffie-Hellmanova funkce*

Na počátku 70 let uveřejnili pánové Diffie a Hellman svou představu o možnostech šifrování veřejným klíčem.Výsledkem jejich snažení je DH funkce, která je stále v kryptosystémech používána.

### *El Gamal*

Tato šifra je v případě systémů založených na diskrétním logaritmu v podstatě analogií RSA.

### *Eliptické křivky*

Eliptické křivky byly zkoumány algebraickou geometrií a teorií čísel více než 150 let, avšak až v roce 1985 přišli nezávisle na sobě Victor Miller (tehdy IBM) a Neal Koblitz (University of Washington) na jejich použití v rámci systému veřejného klíče. Je třeba si uvědomit, že éra masivního zkoumání algoritmů veřejného klíče začala až v roce 1976. V nejbližších letech po objevu možností využití problému diskrétního logaritmu v kryptografii se zdálo vše vyřešené a použití eliptických křivek se proto jevilo jako nepraktické. Postupem času se ukázalo, že metody veřejného klíče typu RSA jsou relativně pomalé a těžkopádné a z tohoto hlediska, že jsou eliptické křivky výhodnější.

Požadavky praxe kladou na kryptografické algoritmy rozporuplné požadavky: kryptografická síla, rychlost a jednoduchost. Rychlost je potřebná např. u linkových šifrovacích systémů při vysokých rychlostech dnešních sítí LAN i WAN – např. díky technologii ATM. Jednoduchost (a tedy i nízká cena zařízení) je potřebná zvláště u čipových karet.

Eliptické křivky jsou tedy výhodné především kvůli

- vysoké kryptografické síle ve vztahu k velikosti klíče,
- nízkým nárokům na výpočty, šířku pásma i paměť ze všech algoritmů veřejného klíče,
- rychlosti šifrování i podepisování, a to jak u hardwarové, tak i u softwarové realizace.

Vhodnými oblastmi použití jsou čipové karty, PC-karty, vysokorychlostní linky, zařízení pro bezdrátové přenosy příručními zařízeními a vůbec pro aplikace s častým podepisováním, verifikováním nebo autentizováním.

### *Hashovací funkce*

Vzorkovací, neboli hashovací, funkce jsou velmi důležité pro kryptografii a tvorbu digitálních podpisů. Jsou to funkce, které umí udělat vzorek jakéhokoli souboru, aby byl závislý na všech bitech původního souboru. Výstupem funkce je vzorek (též nazývaný hash, figerprint, otisk) o pevné délce.

### *MD5 – Message Digest Algorithm 5*

Výstupem funkce je 128-bitový vzorek. MD5 je jednocestná hešovací funkce vytvořená profesorem Ronaldem L. Rivestem v roce 1991. Algoritmus MD5 vytváří z libovolně dlouhého vstupu 128 bitů dlouhý výtah.

### *SHA-1 – Secure Hash Algorithm 1*

SHA (Secure Hash Algorithm) je jednocestná hešovací funkce vyvinutá institucí National Institute of Standards and Technology (NIST).

Algoritmus vytváří ze zprávy 160bitů dlouhý řetězec nazývaný message digest. Ten je používán jako digitální podpis zprávy a slouží zejména pro ověření její pravosti. Příjemce provede pro přijatou zprávu stejný výpočet a nesouhlasí-li doručený message digest s tím, který příjemce spočítal, zpráva byla cestou upravena.

### *DSA - Digital signature algorithm*

DSA se stal americkým vládním standardem roku 1994.. DSA je asymetrický kryptografický algoritmus. Byl navržen NSA (National Security Agency) pouze k digitálnímu podpisu. Narozdíl od RSA či eliptických křivek jím nelze šifrovat (dle přijatého standardu). Původní standard DSS uznával pro digitální podpis pouze algoritmus DSA spolu s vzorkovací funkcí SHA (Secure Hash Algorithm). Později byl do standardu zahrnut i RSA a SHA byla upravena na SHA-1. RSA byla zahrnuta do standardu díky tlaku amerických bank, které mají RSA v ANSI standardu bezpečnosti X9.31.

DSA využívá tajný 160bitový klíč a veřejný 1024bitový klíč. Tajný klíč je velmi krátký, což je výborné pro užití v čipových kartách.

Výhodou DSA je jeho volná šiřitelnost a bezpečnost, která je založena na problému diskrétního logaritmu. Podle odborníků je bezpečný v horizontu mnoha desítek let.

## Aplikace šifrovacích algoritmů

### *PGP*

PGP je zkratkou pro Pretty Good Privacy, což lze přeložit jako “celkem slušné soukromí”. Tvůrcem tohoto světově rozšířeného programu (nyní balíku programů) je Phill Zimmermann. Ačkoli bylo PGP napsáno v USA a používá silnou kryptografii, je používáno všude ve světě. PGP bylo vyvezeno jako literární dílo a mimo území USA přepsáno a zkompilováno. PGP je freeware, ale existuje i komerční verze. Nyní aktuální (20.10.1999) je verze 6.5.1. Do verze 5.0 používalo PGP asymetrickou RSA, symetrickou šifru IDEA, hash MD5 a podpis RSA. Od verze 5.0 je implementována Diffie-Hellmanova asymetrická funkce, symetrický T-DES, IDEA a ČAST, hash SHA1 a podpis DSS.

PGP funguje jako hybridní kryptosystém používající jak symetrickou, tak asymetrickou kryptografii a systém digitálních podpisů. Funguje to tak, že otevřený text je zkomprimován freeware rutinou PKZIP od fy PKLITE. Poté je zakódován konvenčním (symetrickým) klíčem (náhodným – vytvořeným pouze pro tento proces). Tento konvenční klíč je zakódován veřejným klíčem. Konečný “kryptobalíček” obsahuje tedy text zašifrovaný symetricky a symetrický klíč zakódovaný asymetricky. Tento princip je optimalizací kvůli rychlosti. Symetrické šifry jsou totiž mnohem rychlejší než asymetrické na velkých datech. Takto probíhá asymetrickou šifrou pouze x-bitový klíč podle typu šifry.

Proces dekódování je inverzní k procesu zakódování. Prvně je privátním klíčem odkódován symetrický klíč a potom teprve odkódován samotný text (dosud zazipovaný) a nakonec je právě ten odzipován.

PGP má implementován i systém digitálního podpisu. Na internetu existuje tzv. *síť serverů veřejných klíčů*. Fungují podobně jako vyhledávače www stránek, ale výsledkem hledání je veřejný klíč určité osoby. Freeware verze PGP a server veřejných klíčů lze nalézt na http://www.pgp.cz

***SSL – Secure Socket Layer***

SSL je norma vytvořená společností NETSCAPE. Používá se jako tzv. *bezpečný protokol* https. Obecně je používán k přenosu informací, které nesmí být odposlechnuty jako např. číslo kreditní karty při platbě přes Internet. Opět tu však je nevýhoda exportních nařízení USA.

Aby mohl uživatel (myšlen klient) ověřit totožnost serveru je nutné mít platný certifikát. Certifikát je něco jako elektronický průkaz totožnosti. Vydává jej třetí osoba – tzv. *certifikační autorita* serveru. Tím ověřuje důvěryhodnost. Certifikát je vlastně identita serveru s veřejným klíčem. Certifikační autoritou v ČR je 1. Certifikační autorita (http://www.ica.cz ). Nebo Verisign (http://www.verisign.com).

SSL používá asymetrickou RSA a symetrickou šifru RC4. A to 128-bitový klíč v USA a 40-bitový klíč mimo území USA. Protokol SSL při komunikaci serveru z USA a klientem mimo území USA sníží uměle délku klíče na 40 bitů. Těchto 40 bitů je doplněno náhodnou posloupností, která je vyměněna mezi serverem a klientem na počátku komunikace protokolu SSL. Na tento řetezec je aplikována hash funkce MD5. Z vytvořeného vzorku je 88 bitů použito k doplnění původního klíče, čímž dostáváme 128 bitů pro RC4. Efektivní délka klíče však je pouze 40 bitů. Pro RSA používá 512-bitový klíč.