Šifrování – základní pojmy

* Kryptografie -věda o tvorbě šifer
* Kryptoanalýza - věda o prolamování šifer
* Kryptologie – věda o šifrování, zahrnuje kryptografii a kryptoanalýzu
* Otevřený text (plaintext) - originální tvar dat ( to co má být zašifrováno)
* Šifrovaný text (ciphertext) – zašifrovaný tvar zprávy
* Šifrování (kryptování, enkryptování enciphering) – proces přeměny otevřeného textu na šifrovaný text
* Dešifrování (dekryptování, deciphering) – přeměna šifrovaného textu na otevřený text

Symetrické šifrování

* Je nejpoužívanějším typem šifrovacího algoritmu
* Používá stejný šifrovací klíč k šifrování i dešifrování  
  - což je jeho největší slabina
* Je velmi rychlý a používá se při velkém množství dat
* Klíč se musí dostat od odesilatele k adresátovi bezpečným kanálem (cestou), aby adresát mohl zprávu dešifrovat
* Pokud takový bezpečný kanál existuje, je často jednodušší zprávu nešifrovat a poslat ji rovnou tímto kanálem.

Asymetrické šifrování

* Používá jiný klíč k zašifrování a jiný klíč zpátky k dešifrování
* První z nich se nazývá veřejný, ostatní ho musejí znát. Druhý klíč se nazývá privátní
* Asymetrický šifrovací systém (systém s veřejným klíčem) je založen na principu jednocestné funkce, což jsou operace, které lze snadno provést pouze v jednom směru: ze vstupu lze snadno spočítat výstup, z výstupu však je velmi obtížné nalézt vstup.
* Nejběžnějším příkladem je například [násobení](http://cs.wikipedia.org/wiki/N%C3%A1soben%C3%AD): je velmi snadné vynásobit dvě i velmi velká čísla, avšak rozklad součinu na činitele (tzv. [faktorizace](http://cs.wikipedia.org/wiki/Faktorizace)) je velmi obtížný. (Na tomto problému je založen např. algoritmus [RSA](http://cs.wikipedia.org/wiki/RSA).)

**Princip:**

Bezpečnost RSA je postavena na předpokladu, že rozložit velké číslo na součin prvočísel (faktorizace) je velmi obtížná úloha. Z čísla *n* = *pq* je tedy v rozumném čase prakticky nemožné zjistit činitele *p* a *q*, neboť není znám žádný algoritmus faktorizace, který by pracoval v polynomiálním čase vůči velikosti binárního zápisu čísla *n*. Naproti tomu násobení dvou velkých čísel je elementární úloha.

Elektronický podpis

**Elektronický podpis** jsou elektronické identifikační údaje autora (odesílatele) elektronického dokumentu, připojené k tomuto dokumentu.

**Zaručený elektronický podpis** je elektronický podpis v takové formě, která zaručuje (zpravidla použitím kryptografických metod):

* autenticitu– lze ověřit původnost (identitu) subjektu, kterému
* patří elektronický podpis),
* integritu – lze prokázat, že po podepsání nedošlo k žádné
* změně, soubor není úmyslně či neúmyslně poškozen,
* nepopiratelnost – autor nemůže tvrdit, že podepsaný
* elektronický dokument nevytvořil (např. nemůže se zříct
* vytvoření a odeslaní výhružného dopisu),
* může obsahovat časové razítko, které prokazuje datum a čas podepsání dokumentu.

Elektronický popis – algoritmus

* Vybere se kryptografická hašovací funkce.
* Dále se rozhodne o parametrech *L* a *N*, které určují délku klíče. V původní verzi DSS (Digital Signature Standard) byla volba *L* omezena na násobky 64 v rozsahu 512 až 1024 včetně. Doporučují se dvojice *L* a *N* (1024,160), (2048,224), (2048,256) a (3072,256).
* Dále se vybere *N*-bitové prvočíslo *q*. Délka *N* musí být alespoň taková, jako délka výstupu použité hašovací funkce.
* Dále se vybere *L*-bitové prvočíslo *p* takové, že *p*-1 je násobek *q*.
* Nakonec se vybere *g* jako takové číslo, jehož multiplikativní řád modulo *p* je právě *q*. Toho lze dosáhnout dosazováním do vzorce ***g*=*h*(*p*-1)/*q* mod *p*** pro náhodná *h* (kde 1< *h* < *p*-1), dokud výsledek není různý od jedné. Většina náhodných voleb *h* uspěje, nejčastěji se používá *h*=2.
* Všechny výše zmíněné hodnoty mohou být sdílený více uživateli a nejsou tajné. Následuje vytvoření samotných klíčů.
* Nejdříve se náhodně vybere *x* v rozsahu 0<*x*<*q*.
* pak se spočítá *y*=*gx* mod *p*
* Veřejný klíč je pak dán jako čtveřice **(*p*,*q*,*g*,*y*),** soukromý klíč je dán jako *x*.