Komprese a šifrování

Komprese

Komprese je proces při kterém se z velkého objemu dat získáme menší objem, ze kterého se dá však informace zpětně získat.

Kompresi můžeme dělit na:

- Ztrátovou
- Bezztrátovou

Ztrátová komprese

Při ztrátové kompresi dochází k nenávratné ztrátě některé části informace. Tato nevýhoda je ovšem kompenzována významným zmenšením objemu dat. Tento typ komprese se používá hlavně ke kompresi obrazu(videa) a hudby. U fotografií se například používá formát **JPEG**, u videa **MPEG** a u hudby **MP3** nebo **AAC**.

Bezztrátová komprese

Při bezztrátové komprese se dá komprimovaný soubor dá vyvolat do předchozí podoby, díky tomu se dají zachovat i textové informace. Bezztrátovní kompresní algoritmus je například **LZMA**, který používá program **7-Zip**. Pro bezztrátovou kompresi hudby se například používá formát **FLAC** a u obrázků **PNG** nebo **GIF**.

Šifrování

Šifrování je proces, při kterém se informace převede do podoby, která není čitelná bez znalosti procesu, který byl použit.

Šifry můžeme dělit podle možnosti zpětného získání informace na:

- Reversibilní - informace je možné zpětně vyvolat
- Ireversibilní - informace se uchovává ve formě hashe a není možné ji zpětně vyvolat

Reversibilní šifrování

Reversibilní šifrování můžeme dělit na:

- Symetrické - symetrické šifry mají stejný klič pro šifrování i dešifrování
- Asymetrické - asymetrické šifry mají dva klíče jeden pro šifrování a druhý pro dešifrování

Symetrické šifry

Jednoduchým příkladem symetrické šifry může být tzv. Caesarova šifra, kterou římský vojevůdce používal k šifrování vojenských zpráv. Šifra je založena na tom, že si na začátku určíme klíč (třeba číslo 2) a posuneme každé písmeno zprávy v abecedě o vybrané číslo.

Když vezmeme například slovo „Pascal“ a zašifrujeme ho Caesarovou šifrou s klíčem 2, tak dostaneme „Rctecn“.

Dalším příkladem je třeba Vernamova šifra

Asymetrické šifry

Díky tomu, že asymetrické šifry mají dva klíče, z nichž jeden z nich je ve většině případů veřejný a druhý soukromý.

Příklad komunikace za použití asymetrické kryptografie s veřejným klíčem pro zašifrování a privátním pro dešifrování: asymetricka_kryptografie_1_.svg

Asymetrická kryptografie se soukromým klíčem pro zašifrování a veřejným klíčem pro dešifrování se používá k ověření identity. Autor zprávy zašifruje zprávu soukromým klíčem a adresát ji po přijetí dešifruje a tím ověří identitu odesilatele.

Pro asymetrické šifrování se používá například algoritmus RSA.

http://cs.wikipedia.org/wiki/Elektronick%C3%BD_podpis#/media/File:Digital_Signature_diagram_cs.svg

Ireversibilní šifrování

Při ireversibilním zašifrování dostaneme ze zprávy tzv. hash. Z hashe už není možné získat původní informaci. Ireversibilní šifry se dají použít například k uložení hesla v aplikaci. Uživatel si zvolí své heslo a z toho se následně udělá hash. Při každém následném přihlášení se vezme zadané heslo a porovná se s hashem hesla uloženým v databázi.