Bezpečnosť dát, kryptografia

- ***Firewall. Kryptografia a šifrovanie dát. Digitálny podpis. Právne dôsledky.***

Ochrana dát
Postupy a metódy na ochranu dát:
- zabezpečenie počítača pomocou hesiel (windows, bios)
- hardvérový kľúč
- identifikácia užívateľa
- záložné zdroje energie
- ochrana dát pri komunikácii
- elektronický podpis
- šifrovanie dát
- biometria – identifikačné metódy založené na porovnávaní rysov osoby

Firewall
Slúži na obmedzenie prístupov na a z počítača. Pracuje na princípe preverovania paketov, prístupových portov, zdrojových a cieľových adries, ich vyhodnocovania a následného hlásenia alebo protiopatrenia.

Kryptografia
Slúži na zašifrovanie dát pri komunikácii. Zabezpečuje, aby sa správa nedostala do nepovolaných rúk.
Za dobré šifrovanie sa považuje to, ktorého prelomenie kľúča (-ov) trvá dlhšie, ako je doba, po ktorú má byť správa utajená.
Podľa toho, ako sa využíva kľúč rozlišujeme 2 druhy kryptografie:
- *symetrická*
- *asymetrická*

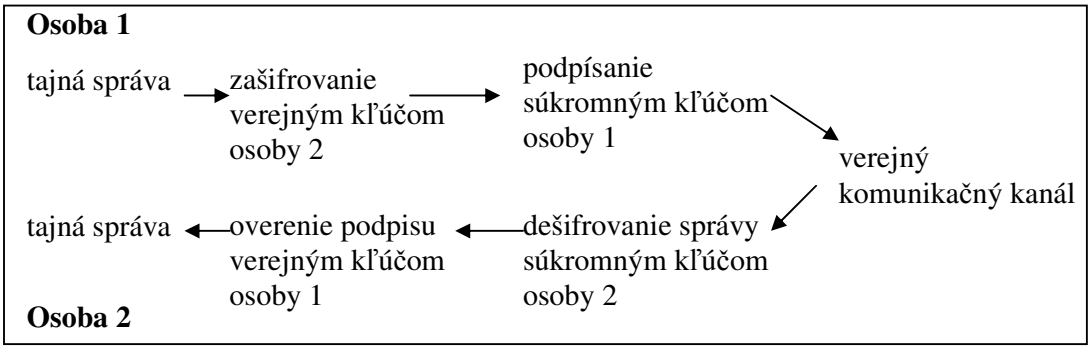
Symetrická
- na šifrovanie aj na dešifrovanie sa používa *jeden kľúč*
- medzi najjednoduchšie patrí zámena písmen za iné písmena
- ďalšia metóda je posun písmen o určitý počet v abecede
- zložitejšou metódou je rozdelenie písmen na jednotlivé časti a každé písmeno v časti je posunuté o iný počet znakov

  tajna sprava
  taj | na | spr | ava
  132 132 132 132

- šifrovanie a dešifrovanie dát je veľmi rýchle
- používa sa na šifrovanie dát, ktoré sa nikam neposielajú
- nevýhodou je, že ak poznáme pôvodnú a zašifrovanú správu, vieme kľúč jednoducho získať
- ďalším problémom je oboznámiť druhú stranu s kľúčom, bez toho, aby sa prezradil
- počet kľúčov pre každú dvojicu väčšej firmy je veľmi veľký (500 zamestnancov – 124750 kľúčov)

Asymetrická
- každý účastník má dva šifrovacie kľúče – **verejný a súkromný**

Schéma asymetricky šifrovanej komunikácie



Rôzne prípady pri asymetrickej kryptografii:

- osoba 1 poslala čistú správu – osoba 2 nemá istotu, či správa nebola cestou čítaná a či je od osoby 1
- osoba 1 podpísala správu - osoba 2 má istotu, že je od osoby 1, ale nemá istotu, či bola cestou čítaná
- osoba 1 zašifrovala správu – osoba 2 má istotu, že si cestou nikto správu neprečítal, ale nemá istotu, či je od osoby 1
- osoba 1 zašifrovala aj podpísala správu – osoba 2 má istotu, že správa je od osoby 1 a že si ju nikto neprečítal

Elektronický podpis

Podľa zákona č. 215/2002 Z.z o elektronickom podpise je elektronický podpis už na rovnakej úrovni ako podpis normálny. Vychádza zo smernice EU č. 1999/93/EC z decembra 1999.

Pre zaregistrovanie elektronického podpisu je potrebné podať žiadosť na *registračnú autoritu*, ktorá preverí údaje a pošle žiadosť *certifikačnej autorite*, ktorá vydá certifikát a zaradí verejný kľúč do „infraštruktúry verejného kľúča“ (PKI – Public Key Infrastructure). Tam je každý verejný kľúč podpísaný certifikačnou autoritou. Nad tým všetkým ja *Koreňová certifikačná autorita*, ktorá vydáva certifikáty nižším certifikačným autoritám. Koreňovú CA spravuje NBÚ.

Princíp práce elektronického predpisu:
Z pôvodnej správy sa hash funkciou vytvorí hash číslo, ktoré je zašifrované súkromným kľúčom osoby 1. Osoba 2 po prijatí správy a následným dešifrovaním si vytvorí taktiež hash číslo a dešifruje hash číslo, zašifrované osobou 1, jej verejným kľúčom. Ak sa čísla zhodujú je to správa od osoby 1. Nie je možné zmeniť správu cestou, lebo hash číslo sa zmení, no zašifrované ostáva pôvodné.

Autorské práva

- program vytvorený programátorom automaticky je chránený autorským zákonom, ktorý určuje práva a povinnosti
  autora
- podľa tohto zákona je právom autora ako sa bude jeho dielo používať, šíriť
- ak si kúpime počítačový program, jeho súčasťou je aj licenčná zmluva, ktorá stanovuje podmienky, za akých ho
  môžeme používať, táto zmluva sa vzťahuje na jedného používateľa a na jeden počítač

- ak chceme používať program na viacerých počítačoch musíme si zakúpiť multilicenciu, ktorá je určená konkrétnym
  číslom (10 počítačov) alebo miestom (škola)
- osobitú skupinu tvoria školské a študentské licencie, väčšinou sú lacnejšie

Počítačová etika (netiketa)

- zásady správania sa v počítačovom svete:
 - nikdy nepíšme druhému to , čo by sme nepovedali v miestnosti plnej ľudí
 - dávajme si pozor, čo píšeme o druhých, naše slová môžu čítať mnohí
 - uvedomme si, že naše slová hovoria za nás
 - buďme struční
 - rešpektujme autorské práva a licencie