ZABEZPEČENIE INFORMÁCIÍ/ INFORMAČNÁ BEZPEČNOSŤ

Vzťahuje sa k informácii ako procesu spracovania, uchovania, prenosu a prezentácie informačného obsahu.

Riešenie sa rozlišuje podľa typu siete na:

Bezpečnosť LAN

- Oranžová kniha – kritériá bezpečnosti OS
- Červená kniha – kritériá hodnotenia bezpečnosti počítačových sietí

!!! 80% narušenia bezpečnosti majú na svedomí vlastní zamestnanci

LAN produkty:

- Servery
- Pracovné stanice
- Sieťový OS
- Stanicový OS
- Aplikačný SW
- Tlačiarne

Bezpečnosť v LAN odpovedá bezpečnosti jej najslabšieho článku.

OS- výrobca zaručuje určitú úroveň bezpečnosti

Kritické miesto – pracovné stanice:

- **Kontrolovaný prístup**
- **Identifikácia obsluhy**
- **Kontrola nad SW vybavením**

BEZPEČNOSŤ WAN

- **Siete verejné**
- **Zdieľanie technických prostriedkov rôznymi používateľmi**
- **Poskytujú služby prvých troch úrovní OSI**
  - **fyzické rozhranie**
  - **linkový protokol**
  - **protokol sieťovej vrstvy**
- **Prvky zabezpečujúce službu prenosu:**
  - **komunikačné dátové rozhranie**
  - **transportný systém**
  - **smerovacie zariadenie**

RIZIKÁ V JEDNOTLIVÝCH PRVKOCH:

- **ROUTER (smerovanie, diagnostika)**
  ohrozenie:
  - **možnosť monitorovania**
  - **zmeny dát**
  - **kopírovanie**
  - **zdržiavanie**

- **KOMUNIKAČNÝ KANÁL (komutované okruhy, pevné spoje, otické, rádiové kanály)**
  ohrozenie:
  - **odpočúvanie**
  - **zmena informácie**
  - **rušenie prenosu**

- **ROZHRANIA (normalizované body prepojenia) ohrozenie:**
  - **monitorovanie dát**
  - **modifikácia obsahu**
  - **zadržanie dát**
  - **falošné správy**

VŠEOBECNÉ MOŽNOSTI OHROZENIA:

- **Získanie informácie**
- **Modifikácia informácie**
- **Vytvorenie falošnej informácie**
- **Zabránenie komunikácie**
- **Zdržanie, alebo spozdenie informácie**

OCHRANA PROTI ÚTOKOM – poskytovanie služieb:

- **Autentizácia**
- **Integrita**
- **Utajenie**

K vytvoreniu týchto služieb slúži kryptografia

BEZPEČNOSŤ A KRYPTOGRAFIA

Kryptogtrafia sa používa na:

- **utajenie informácie**
- **na ochranu pred modifikáciou**
- **overenie pravosti, identity**
- **overenie autorstva**

Informácia je v elektronickom tvare bezpečne uchovaná, prenesená a prezentovaná ak sú zachované nasledovné **funkcie**:

Dôvernosť – informácia je dostupná len autorizovaným subjektom, pre iných je utajená

Celistvosť– ochrana proti neautorizovanej zmene dát alebo ochrana proti nasadeniu vírov

Totožnosť– preukázanie totožnosti/ auteticity subjektu – používateľa, procesu, správy

Autorizácia - nepopierateľnosť zodpovednosti, preukazovanie pôvodu správy

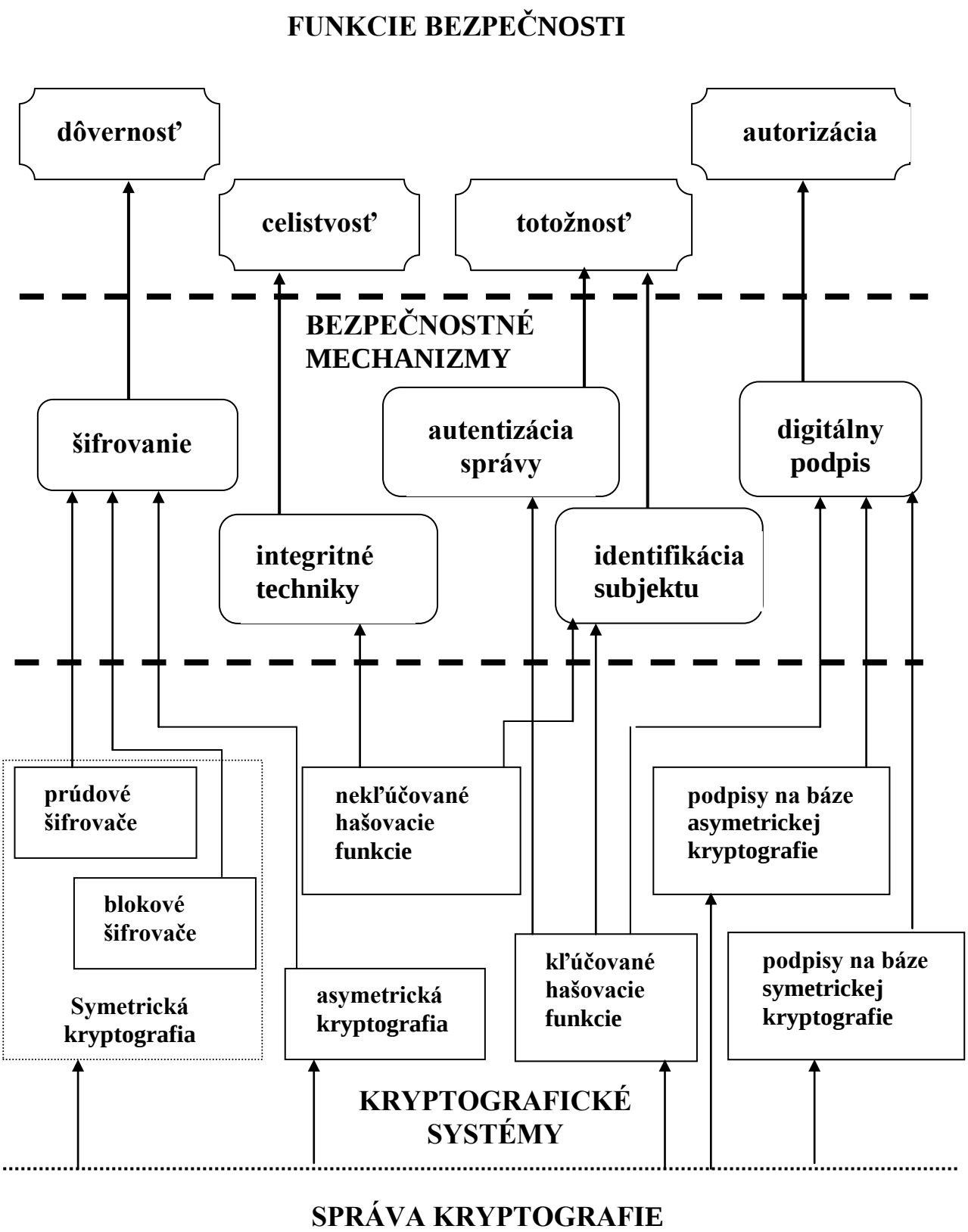
Bezpečnosť kryptosystému sa rozumie jeho odolnosť proti porušeniu zrozumiteľného textu neautorizovaným subjektom.

KRYPTOGRAFIA je teoretická a technologická báza bezpečnostných mechanizmov

KRYPTOANALÝZA je odhalenie zabezpečenej informácie

KRYPTOLÓGIA je matematika pre kryptografiu a kryptoanalýzu

POJMOVÉ SÚVISLOSTI



KRYPTOGRAFIA - VEDA O ŠIFRÁCH

História šifrovania

1. Pred n.l.

Egypt - hieroglify
India – tajné písmo
Čína - znalosť písma
Sparta – drevený šifrátor
Caesarova šifra

2. Novovek

Vigenerov (Baconov) šifrovací systém (1586) – periodicky opakujúci sa kľúč

3. 20. storočie

Vernamov systém – systém jednorázového hesla
Enigma – nemecké šifrovacie zariadenie 2. svetovej vojny
Shanon – základy kryptológie na matematickom základe

4. 60 –te roky

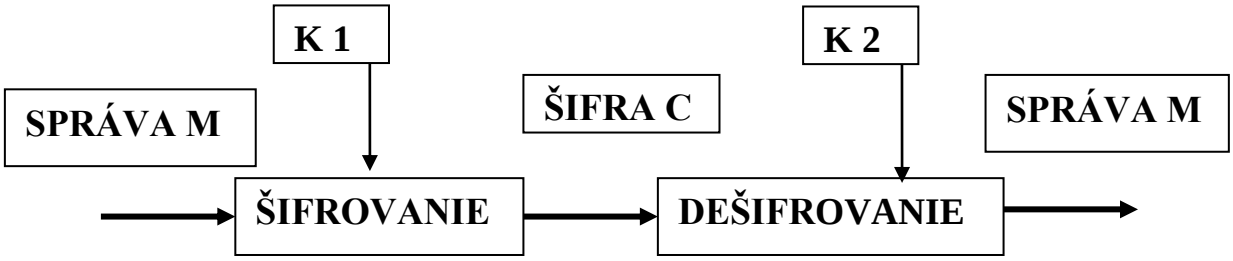
Realizácia Shanonových myšlienok

5. 70 – 80-te roky

Štandard DES
Kryptografia s verejným kľúčom
RSA

ZÁKLADY KRYPTOGRAFIE

MODEL KRYPTOGRAFICKÉHO SYSTÉMU



Kryptografický systém sa skladá z:

- **šifrovacieho algoritmu**
- **dešifrovacieho algoritmu**
- **kľúča**

Algoritmy sa neutajujú – (iba z obchodného dôvodu), utajuje sa kľúč

Ak K1 = K2 SYMETRICKÁ KRYPTOGRAFIA

Ak K1 = K2 ASYMETRICKÁ KRYPROGARFIA

SYMETRICKÁ KRYPTOGRAFIA

(používa pre dešifrovanie tajný kľúč)

A/ KLASICKÁ, KONVENČNÁ KRYPTOGRAFIA

DRUHY ŠIFROVANIA

1. Transpozícia – mení sa poloha
2. Steganografia – utajenie správy
3. Substitúcia - kód – verejná tabuľka
- šifra – tajná tabuľka

MONOALFABETICKÁ SUBSTITÚCIA

Tajná abeceda, ktorou sa šifrujú všetky písmená

Cézarova šifra
Nomenklátory

POLYALFABETICKÁ SUBSTITÚCIA

Prvé písmeno sa šifruje poľa jednej substitúcie, druhé podľa inej substitúcie

Albertiho šifrovací disk
Cardanova mriežka

VIGENEROV SYSTÉM

Základom je tajný kľúč K

ŠT = OT + K mod 26

VERNAMOV ŠIFRÁTOR

Kľúč je rovnako dlhý ako text, načítavanie v mod 2, po každom použití sa kľúč mení

B/ NA MATEMATICKOM ZÁKLADE

Nástroje:
Teória informácie
Teória zložitosti

(Nie je dosť informácie k rozbitiu šifry,
nie je dosť času, pamäti a techniky vyriešiť výpočtovo zložitú metódu)

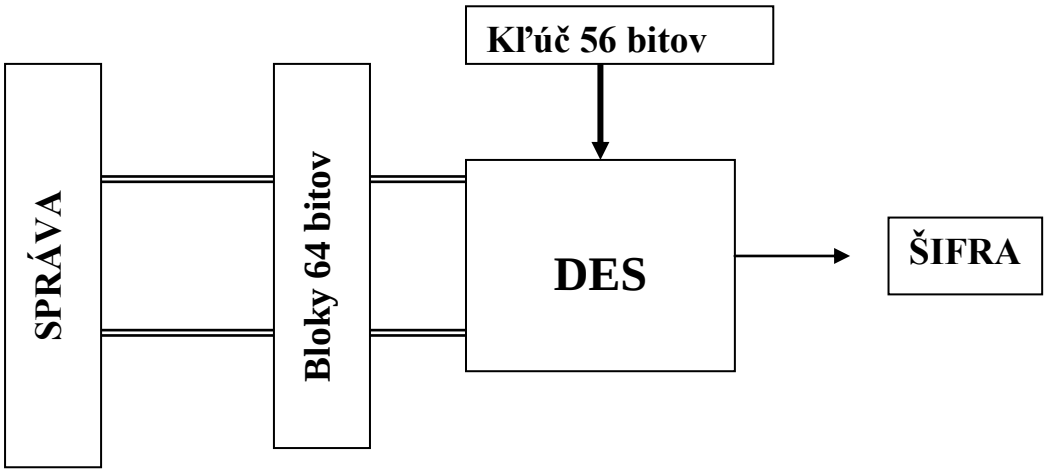
KRYPTOGRAFICKÉ SYSTÉMY

Najznámejší mechanizmus symetrickej kryptografie:

DES - DATA ENCRYPTION STANDARD (1977)

Vlastnosti:

- **Vyhlásený v roku 1977**
- **Zverejnený v roku 1997**
- **Najpoužívanejší algoritmus na svete**
- **Použitie vo finančnom sektore**



POPIS

- **Patrí do skupiny symetrických blokových šifier**
- **Symbolický zápis**

$$ŠT = E_k(OT) \qquad OT = D_k(ŠT)$$

- **OT rozdelený do 64 bitov**
- **Dĺžka kľúča K = 56 bitov**
- **Má 2 vstupy OT a K**
  a 2 výstup ŠT
- **Spracovanie prebieha v 16 krokoch, v každom kroku je z kľúča vyberaný pracovný kľúč K_i = 48 bitov**

VLASTNOSTI

- **Permutácia – rozprestrenie vplyvu bitov OT**

- **Transformácia v S- boxoch – každý výstup je nelineárna funkcia vstupu (kritériá návrhu sú prísne tajné)**

- **Lavínovitosť – zmena bitu v OT vyvolá lavínu zmien v ŠT**

- **Konfúzia a difúzia – každý bit OT a K má vplyv na ŠT a ten musí byť komplikovaný**

DOSTUPNOSŤ

- **Čipy**
- **Zásuvkové moduly do počítačov**
- **Šifrovacie jednotky**

NEDOSTAKY

- **1990 rozlúštenie DES**

Dnes je používané

2 násobné $ŠT = E_{k2}\ E_{k1}\ (OT)$

3 násobné $ŠT = E_{k1}\ D_{k2}\ E_{k2}\ (OT)$

BUDÚCNOSŤ DES

- **???náhrady novým štandardom**
  - $\Rightarrow$ **Skipjak**
  - $\Rightarrow$ **IDEA – International Data Encryption**
  - $\Rightarrow$ **RC4 – Rivest Cipher**
- **asymetrické kryptosystémy**

ASYMETRICKÉ KRYPTOSYSTÉMY

(Asymetrická kryptografia)

Používa dva princípy:

1. PROBLÉM DISKRÉTNYCH ALGORITMOV

Základom je jednocestná (hašovacia) funkcia $y = f(x)$

Ak poznáme x, je jednoduché vypočítať y, ale nie je jednoduché vypočítať x ak poznáme y.

Príklad:

$X = a^x \ . \mod n$

Je jednoduché vypočítať X ak máme a,x,n aj 200 ciferné. Umožňuje to rozklad exponentu a postupné násobenie.

$X = a^{41} = a^{(32 + 8+1)} = (([((a^2)^2)^2)^2)^2 \ . \ ((a^2)^2)^2 \ . \ a$

(7 násobení namiesto 41)

Výpočet a z X vyžaduje násobení mnoho, lebo nie je známy výpočet diskrétneho algoritmu.

Ak a,x,n sú 655 bit pre výpočet X stačí 1330 násobení,
pre výpočet x 10^{100} násobení

VEREJNÁ KRYPTOGRAFIA

PKC – Public Key Cryptography - Kryptografia s verejným kľúčom , tvorcovia Diffie a Hellman

PROTOKOL VEREJNÉHO KĽÚČA

A, B si dohovoria s certifikačnou autoritou n, a n

Každý si zvolí exponent A → x, B → y

Zverejnia čísla, ktoré sú verejné kľúče

A → $X = a^x \bmod n$

B → $Y = a^y \bmod n$

Hodnotu partnera umocnia na vlastný exponent a obdržia spoločný tajný kľúč

A → $K = X^y \bmod n$

B → $L = Y^x \bmod n$

$K = L = a^{xy} \bmod n$

2. PROBLÉM FAKTORIZÁCIE SÚČINU DVOCH VEĽKÝCH PRVOČÍSIEL A EULEROVEJ VETY

RSA – Rivest, Shamir, Adleman
(prvý konkrétny kryptosystém s verejným kľúčom)

Volia sa dve náhodné veľké prvočísla p a q rovnakej dĺžky a určí sa súčin n =p.q

Verejný kľúč je e nesúdeliteľné s m= (p-1)(q-1)

Vypočíta sa dešifrovací kľúč d tak, aby platilo

$$e.d = 1 (\mathrm{mod}\ (p-1)(q-1))$$

$$d = e^{-1} \mathrm{mod}\ ((p-1)(q-1))$$

Platí, že d a n sú nesúdeliteľné.
Verejný kľúč je e, n.
Súkromný kľúč číslo d

Pre šifrovanie sa rozdelí správa do celočíselných blokov M po bitoch alebo bytoch menších ako n

$$\text{Šifra C sa vypočíta } C = M^e \mathrm{mod}\ n$$

$$\text{Dešifrovanie } M = M^d \mathrm{mod}\ n$$

SYSTÉMY DIGITÁLNEHO PODPISU

- **Sú na báze asymetrickej kryptografie**
- **Zaručujú autenticitu a integrity správy**
- **Vyjadrujú pravosť podpisu**

DDS – Digital Signatur Standard štandard NIST 1991

ISO/ IEC 9796 – vyhovuje RSA algoritmus

PGP - Pretty Good Privacy – kombinovaný systém, v ČR prevádzkuje SkyNet - www.pgp.cz

POROVNANIE SYMETRICKÝCH A ASYMETRICKÝCH KRYPTOSYSTÉMOV

Asymetrické sú:

⇒pomalšie – zložité výpočty
⇒dohľad nad kľúčmi – certifikačná autorita
⇒nie je potrebné dohovárať si tajné kľúče, nemusia sa poznať

Digitálny podpis