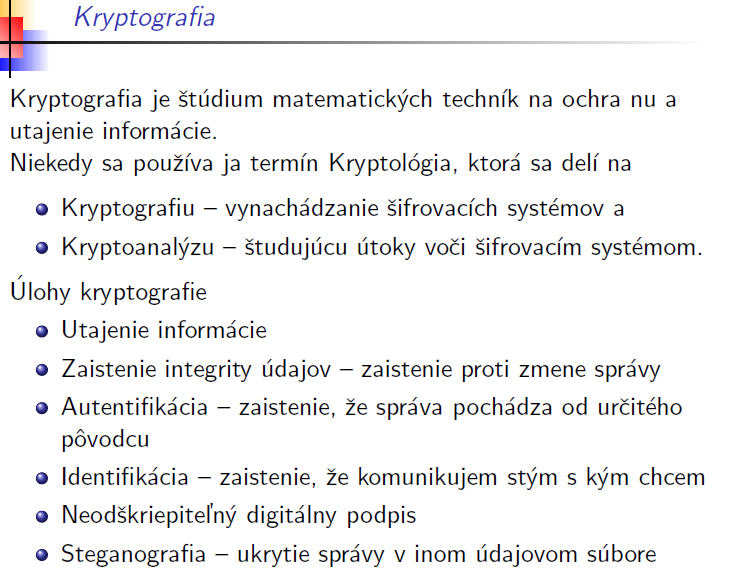
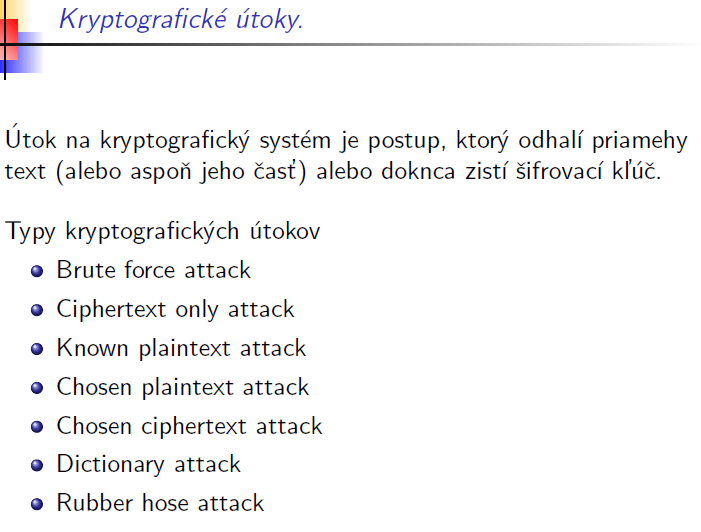
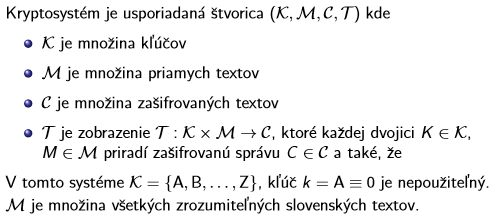
1. **Kryptografia**



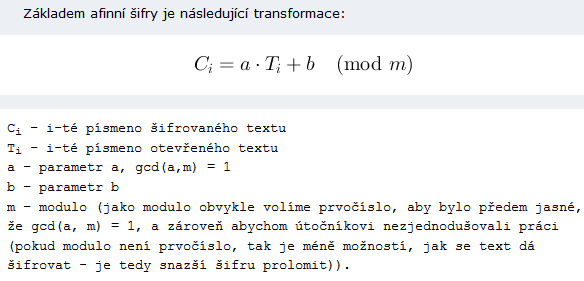
***Kryptografické útoky***

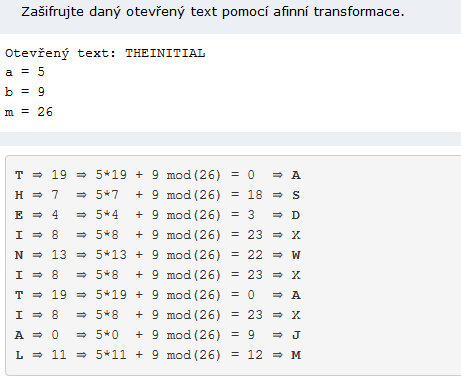


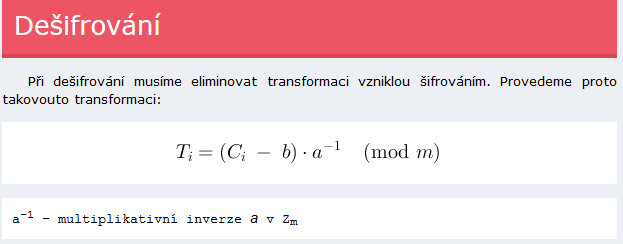
***Kryptosystém:***

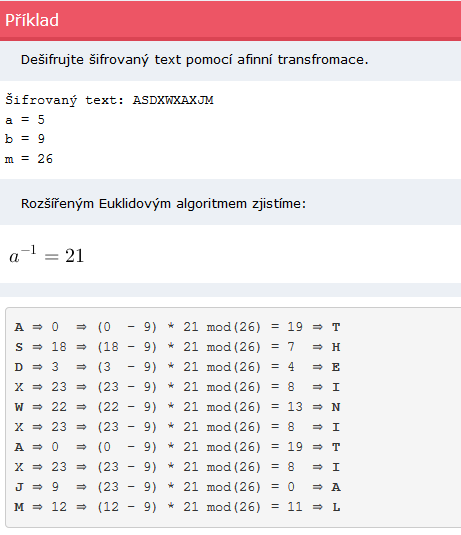


**2. Afinna sifra:**

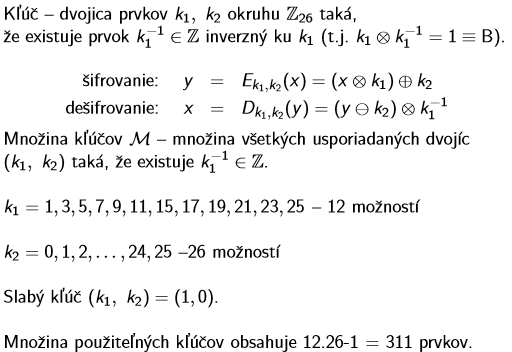


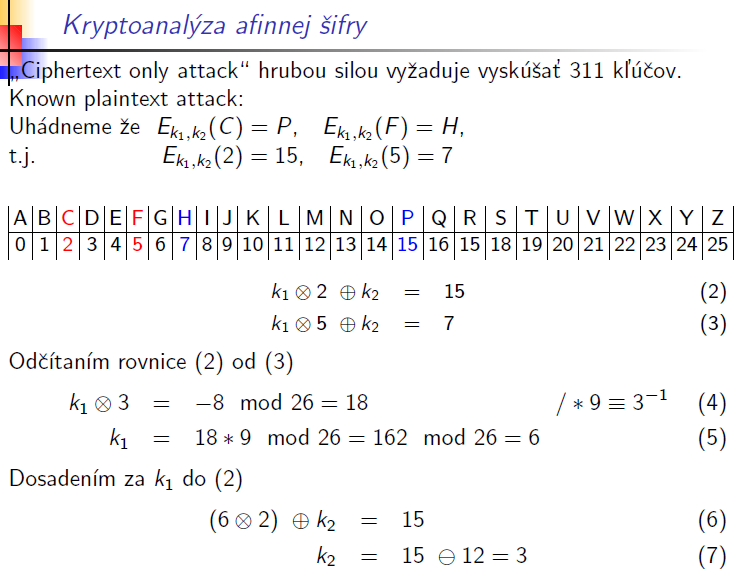




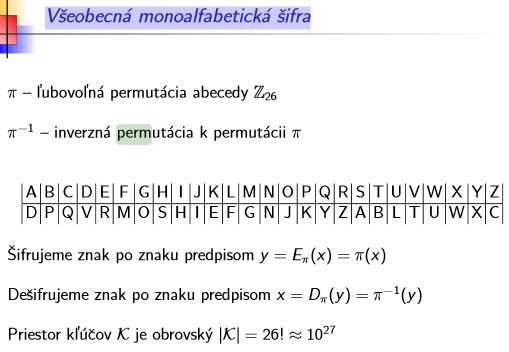


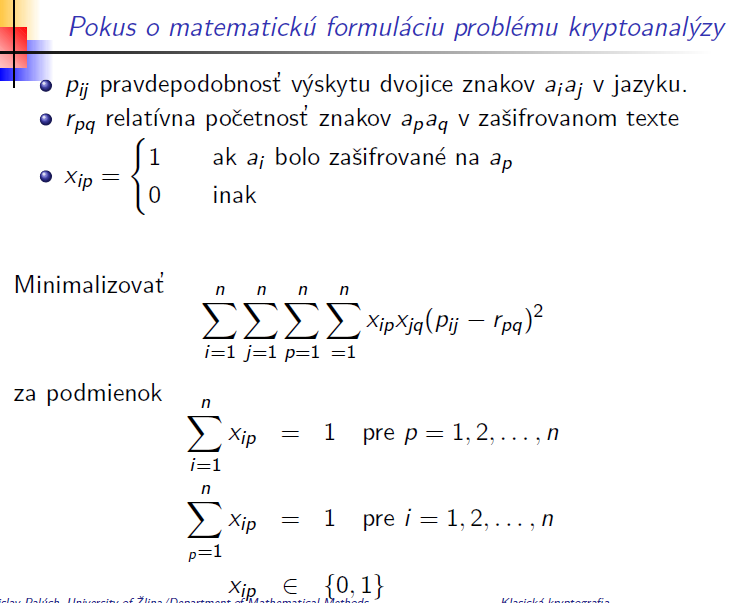


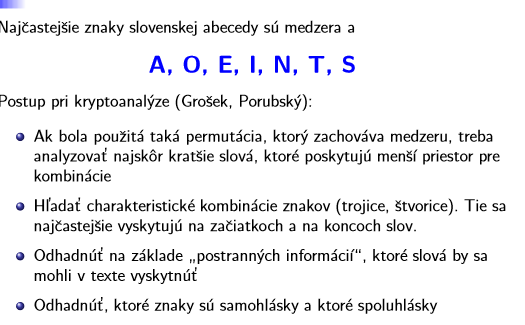


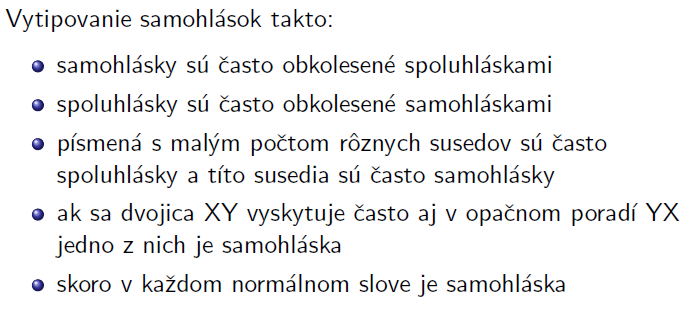


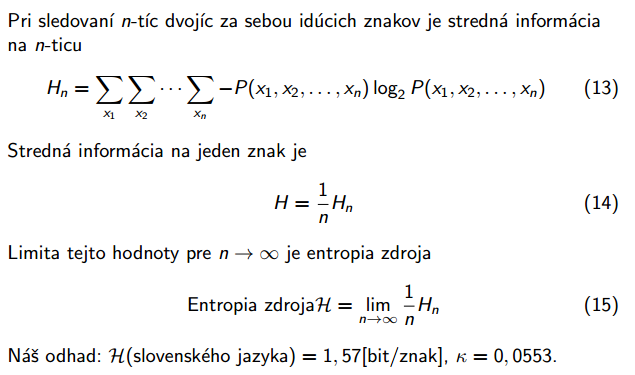
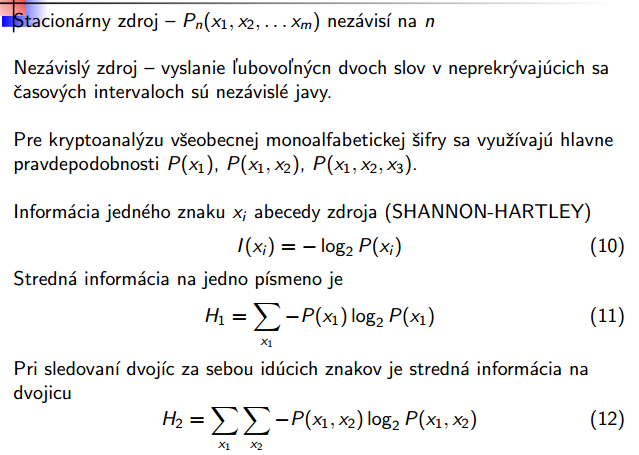
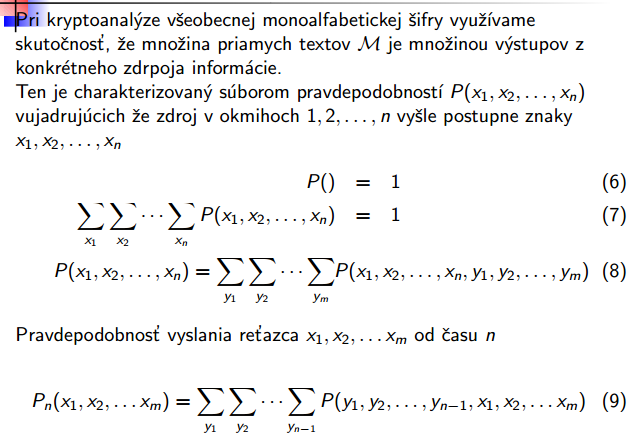
**3. Vseobecna monoalfabeticka sifra**



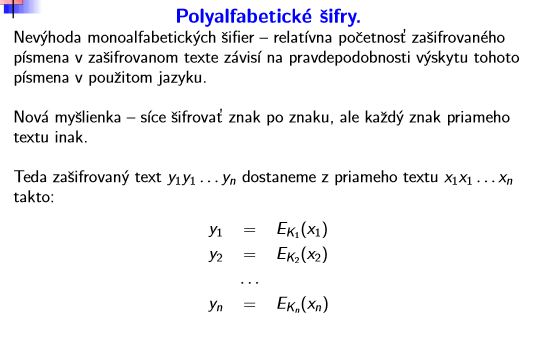


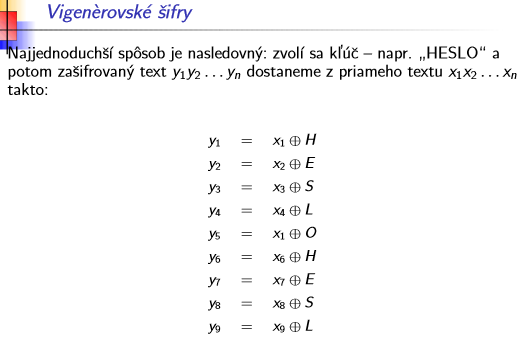


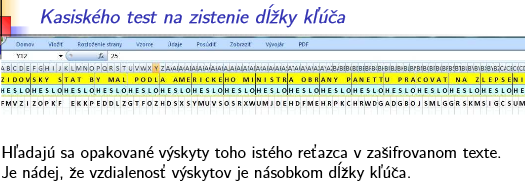


****

**4. Vigenerovska**

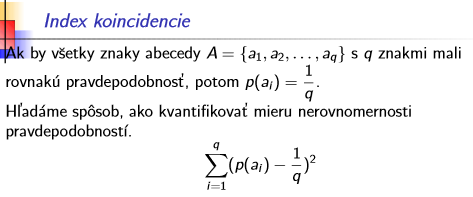


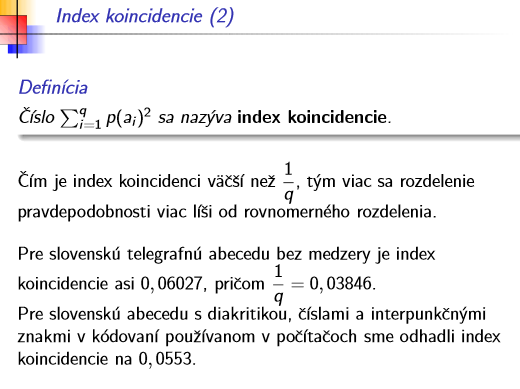


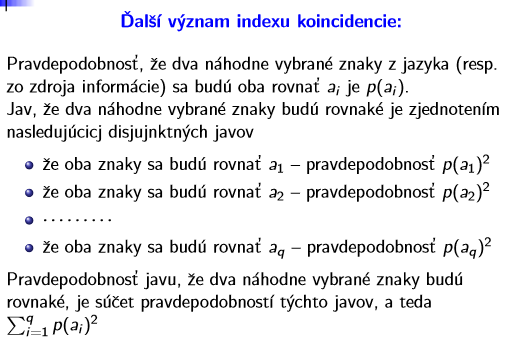


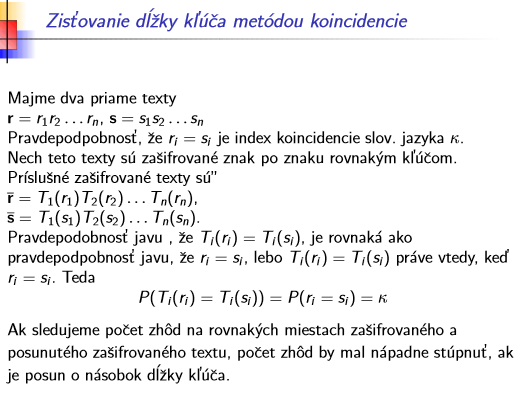


**5. Index koincidencie**

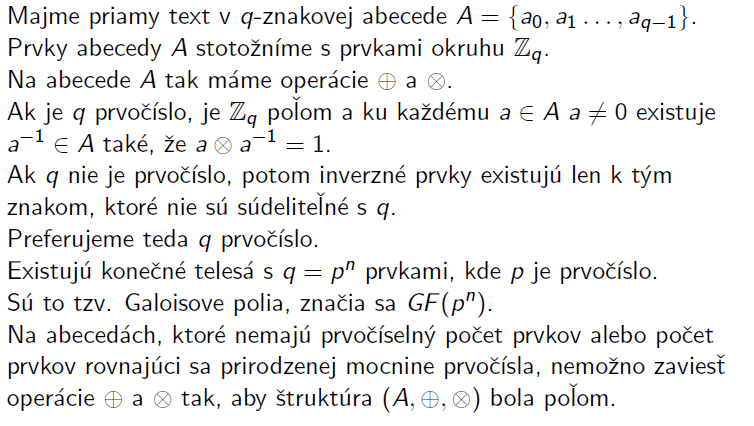


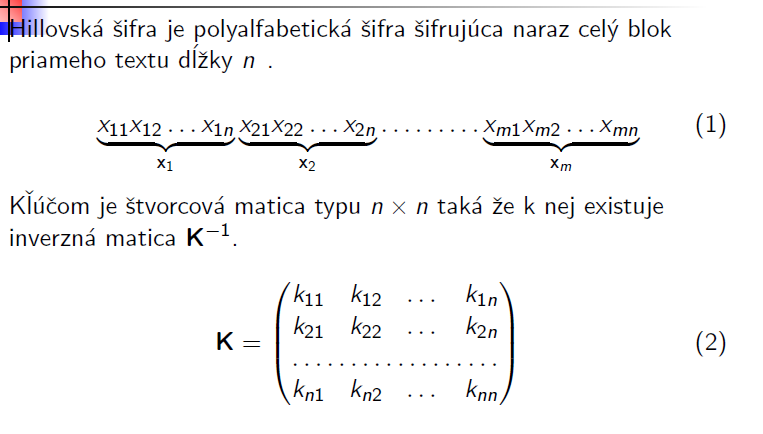


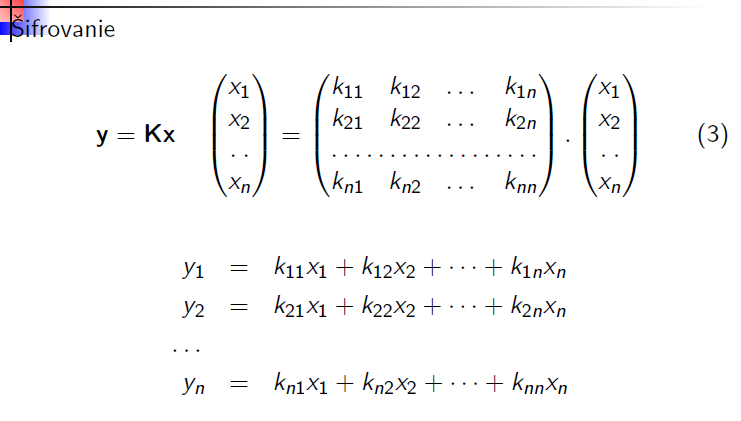


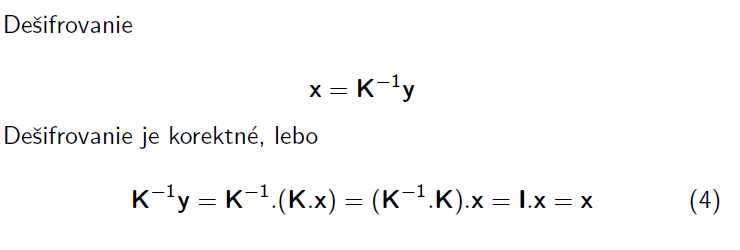


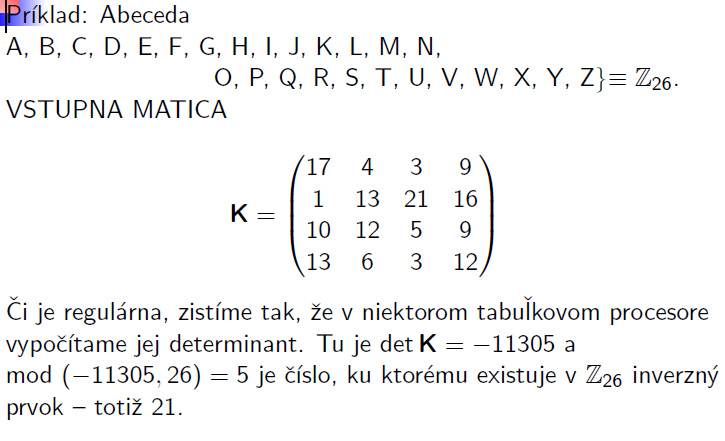
**6.Hillovska sifra**

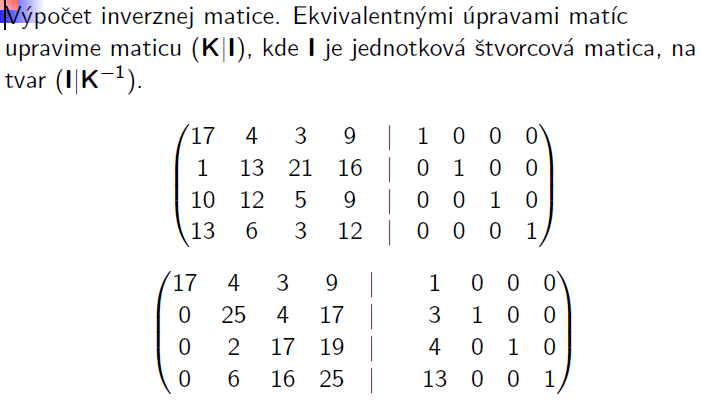


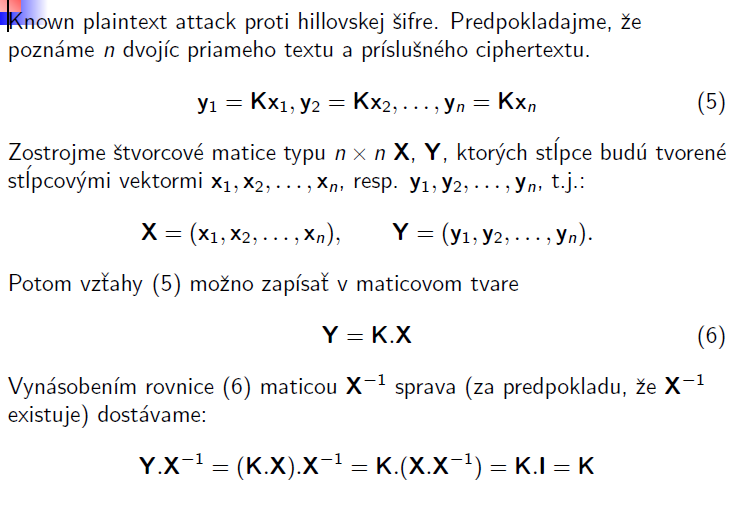




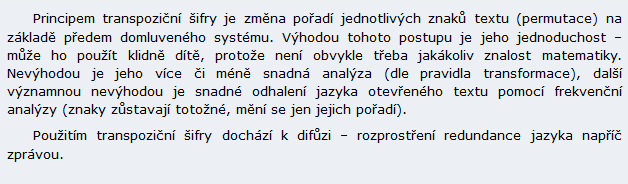


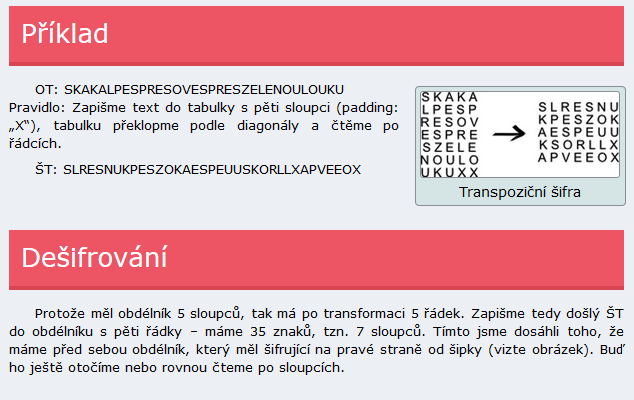


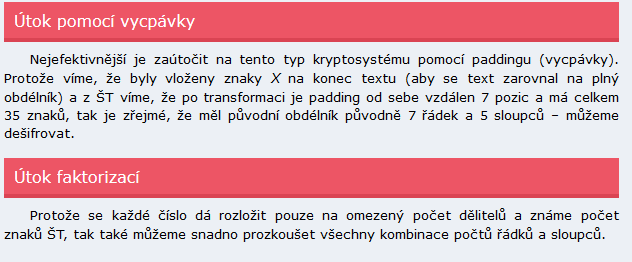




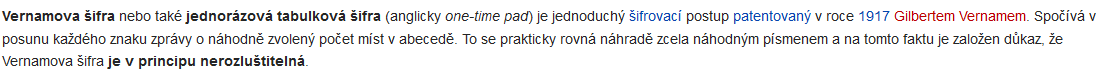
**7. Transpozicna – permutacna sifra**

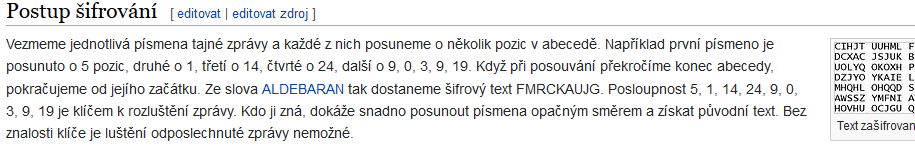


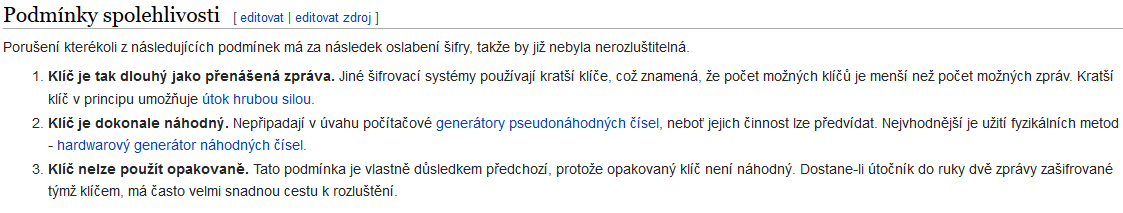


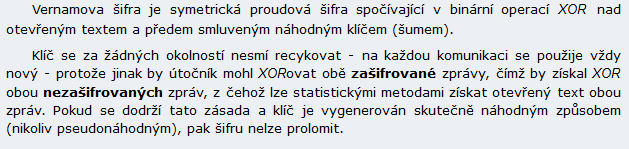


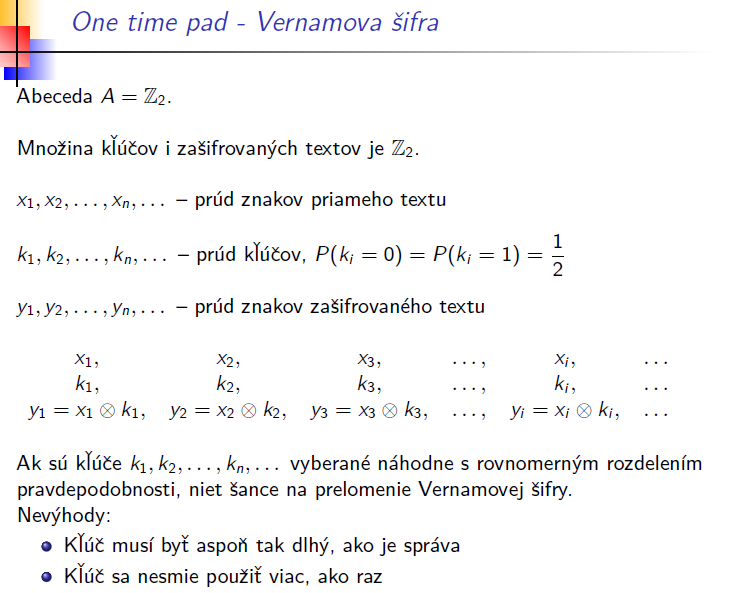
**8. One time Pad + utok (Vernamova šifra)**

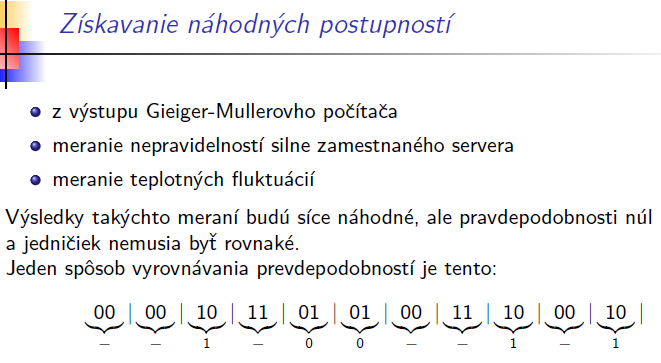




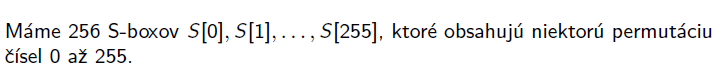


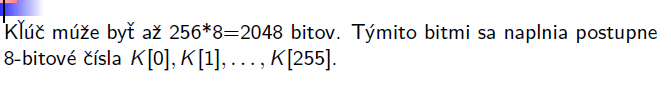


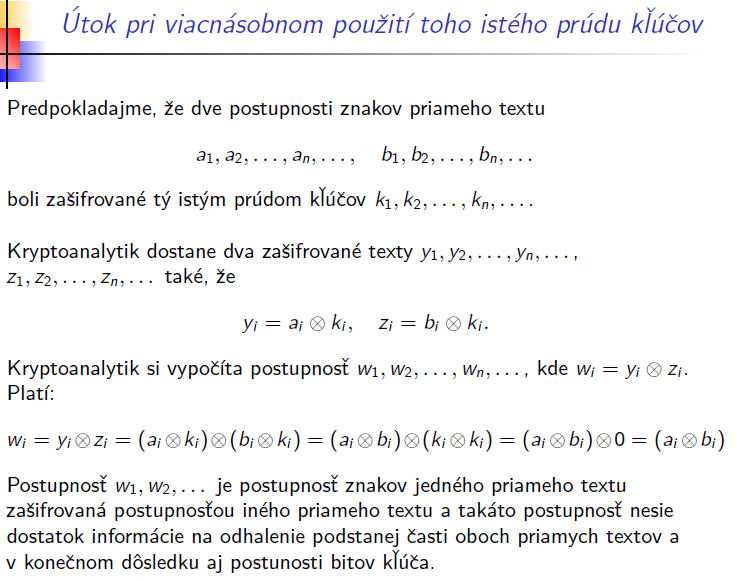


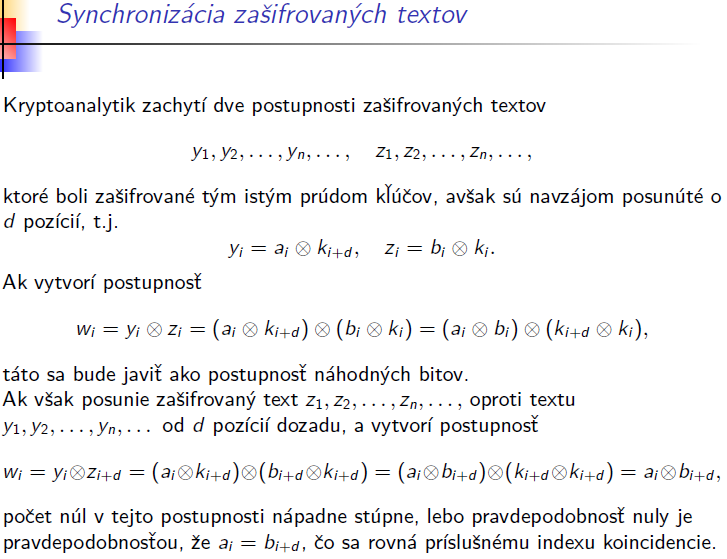


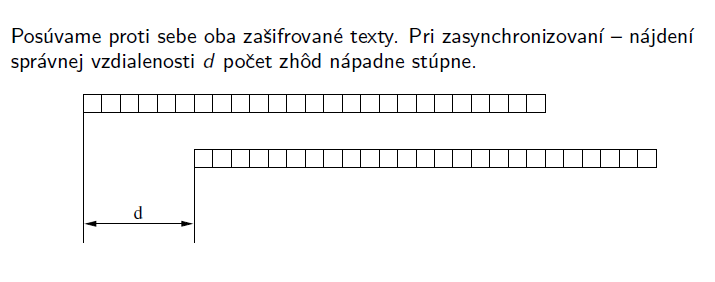






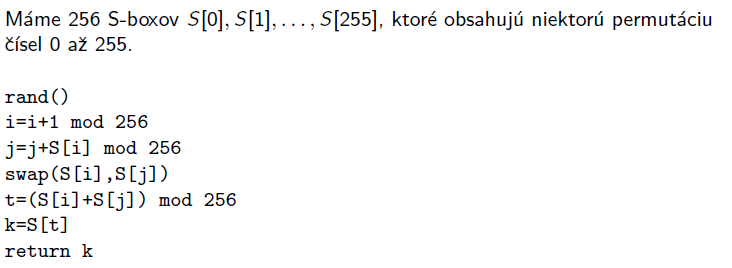


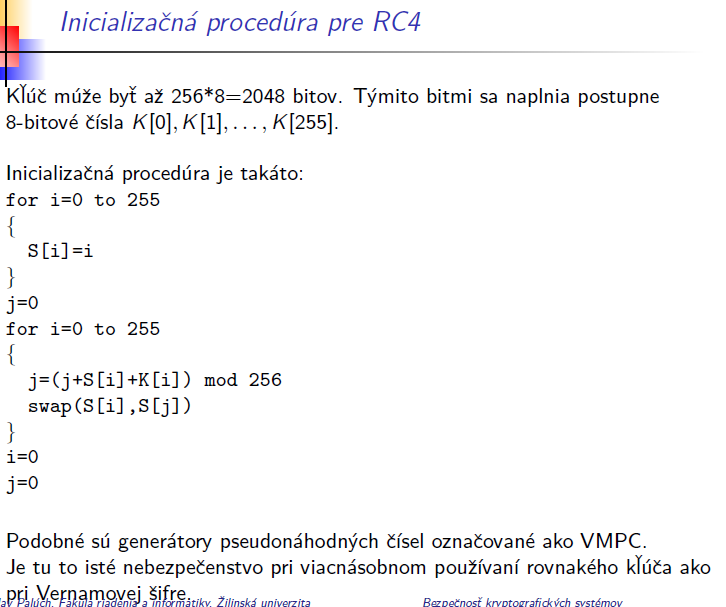




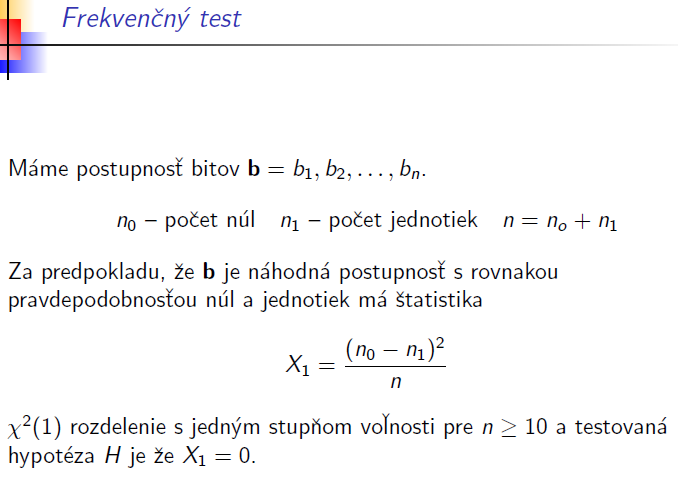
**9.Pseudogeneratory (linearny kongruencny, kvadraticky, kubicky, RC4)**

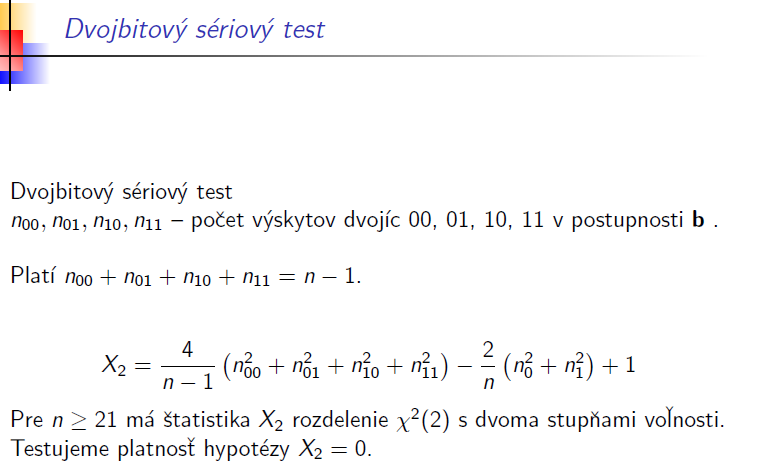




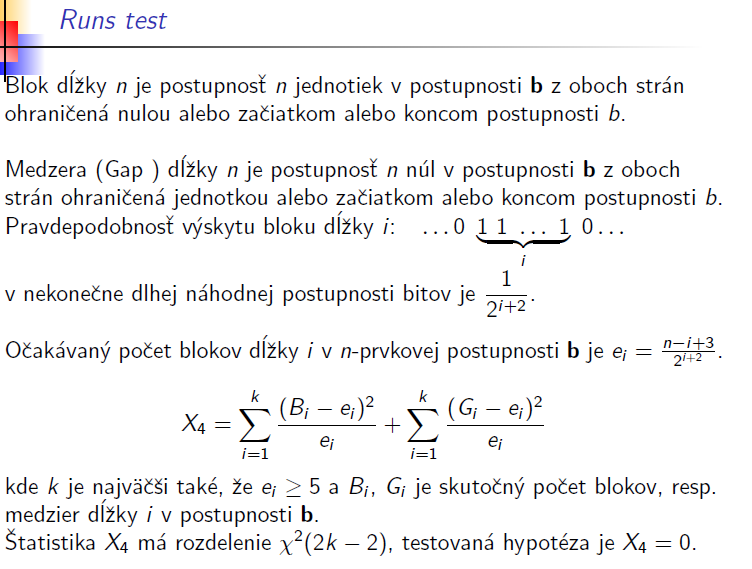


**10.Testy generatorov (frekvencny, TwoBits, Runs, Poker, FIPS 140-1, Autokorelacny)**

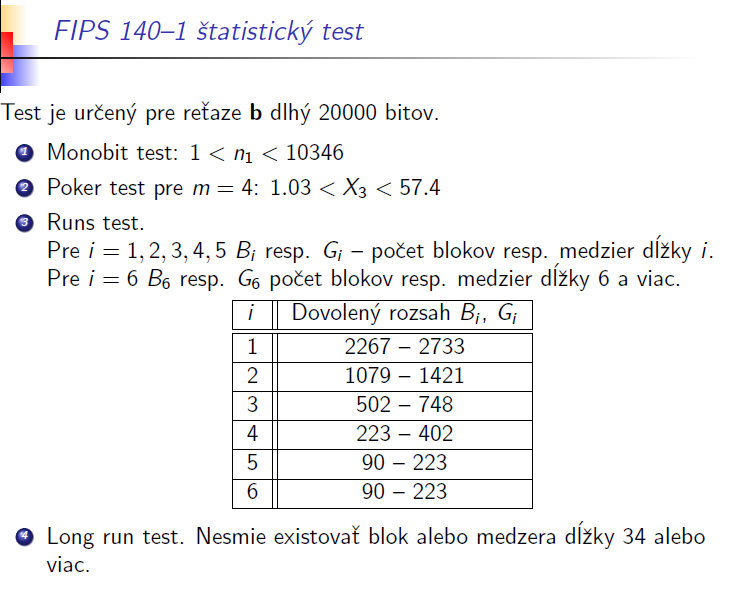




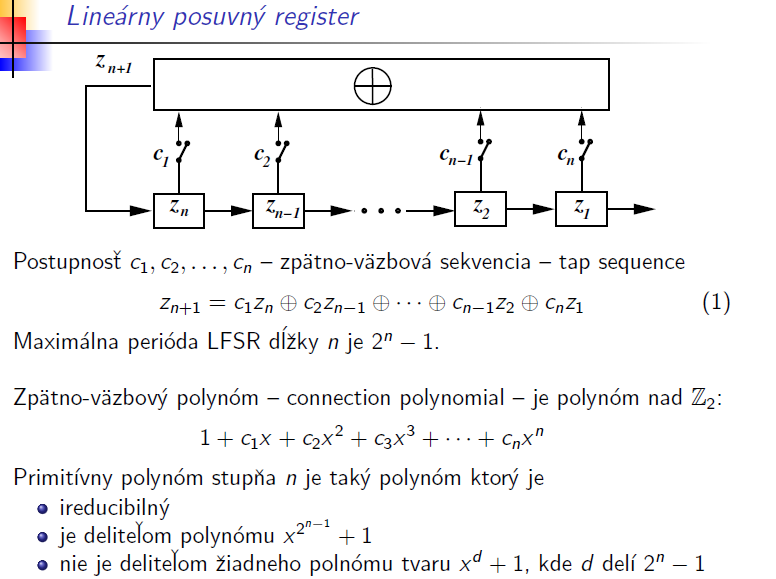


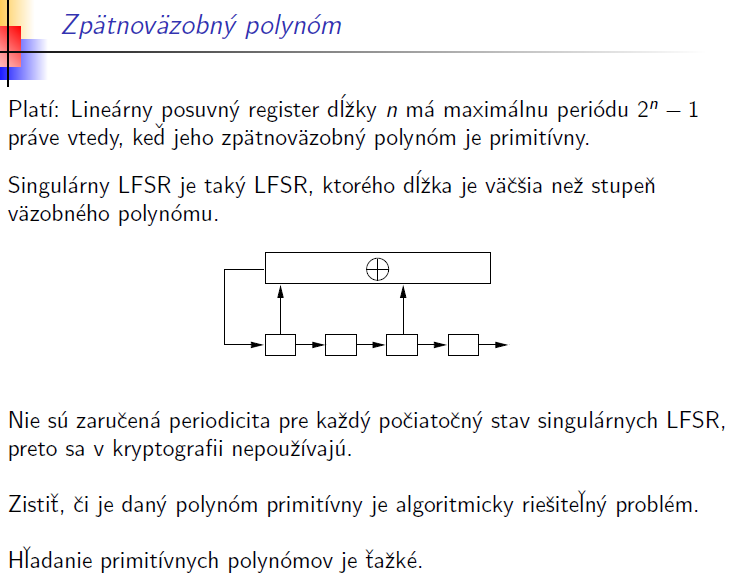




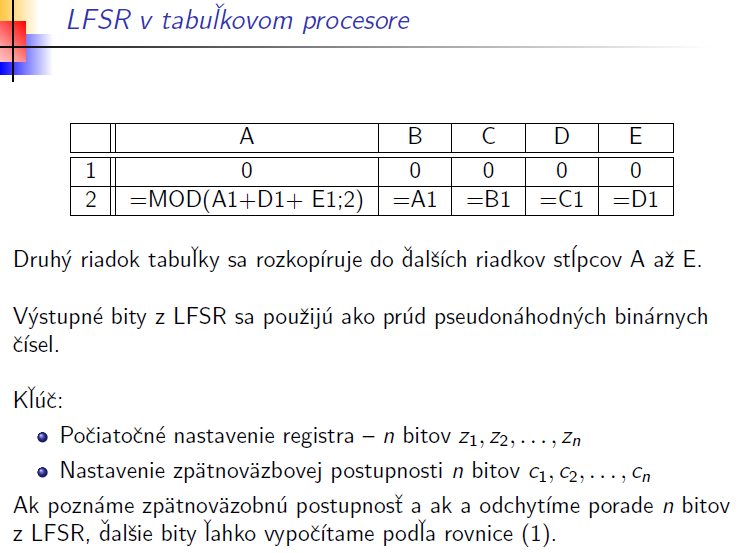


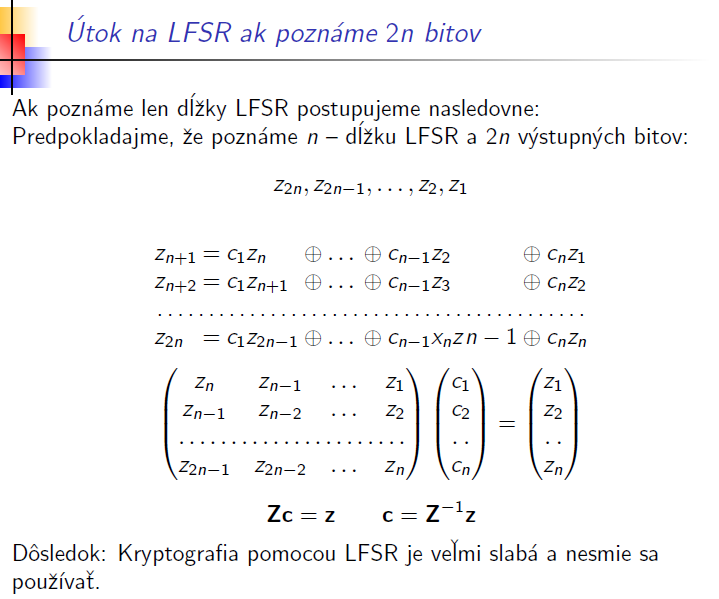
**11.LFSR**

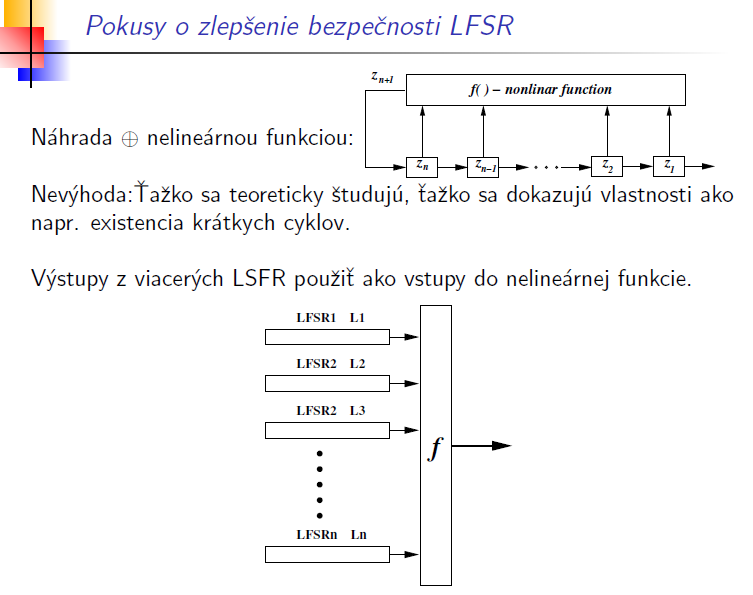


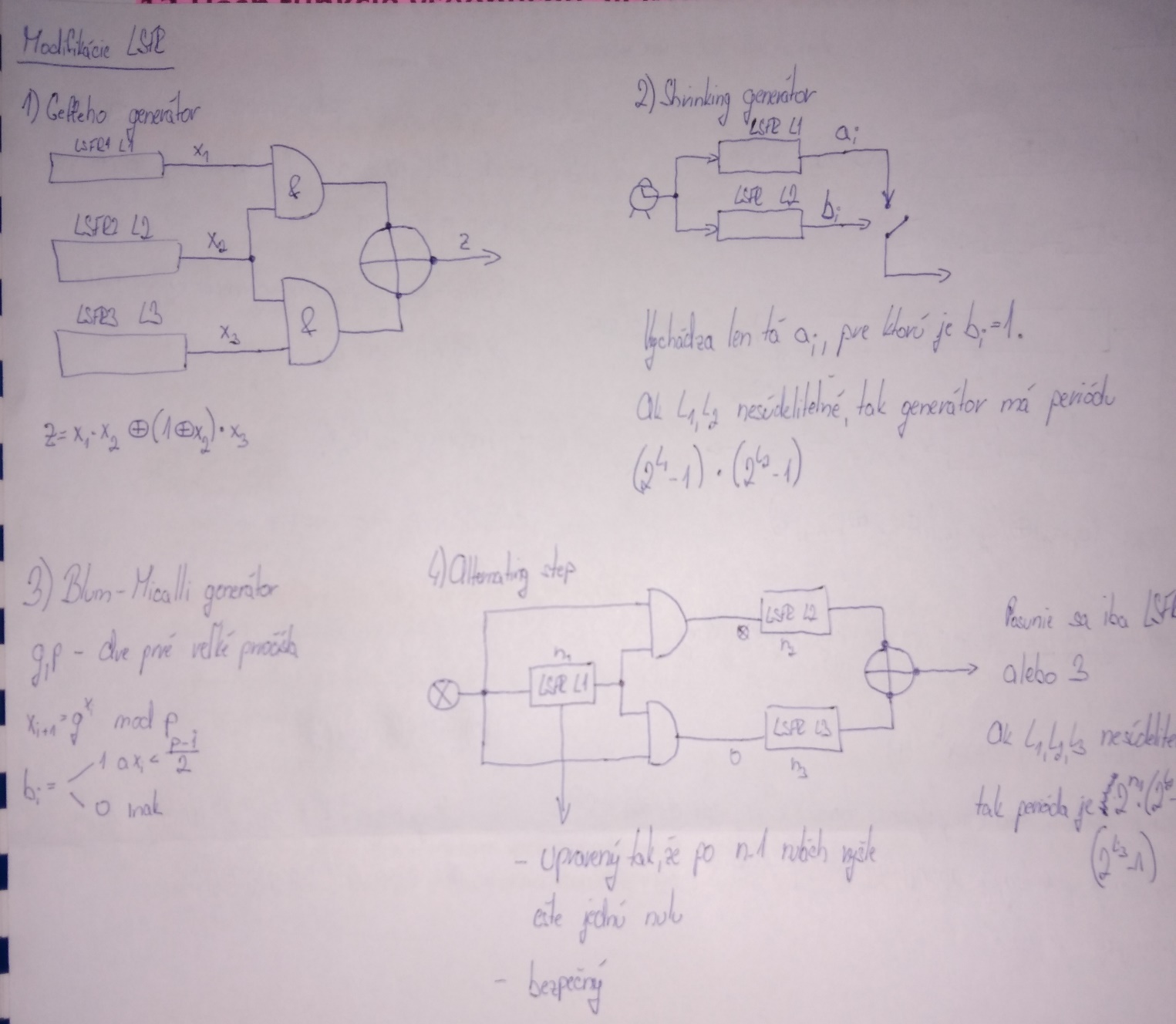






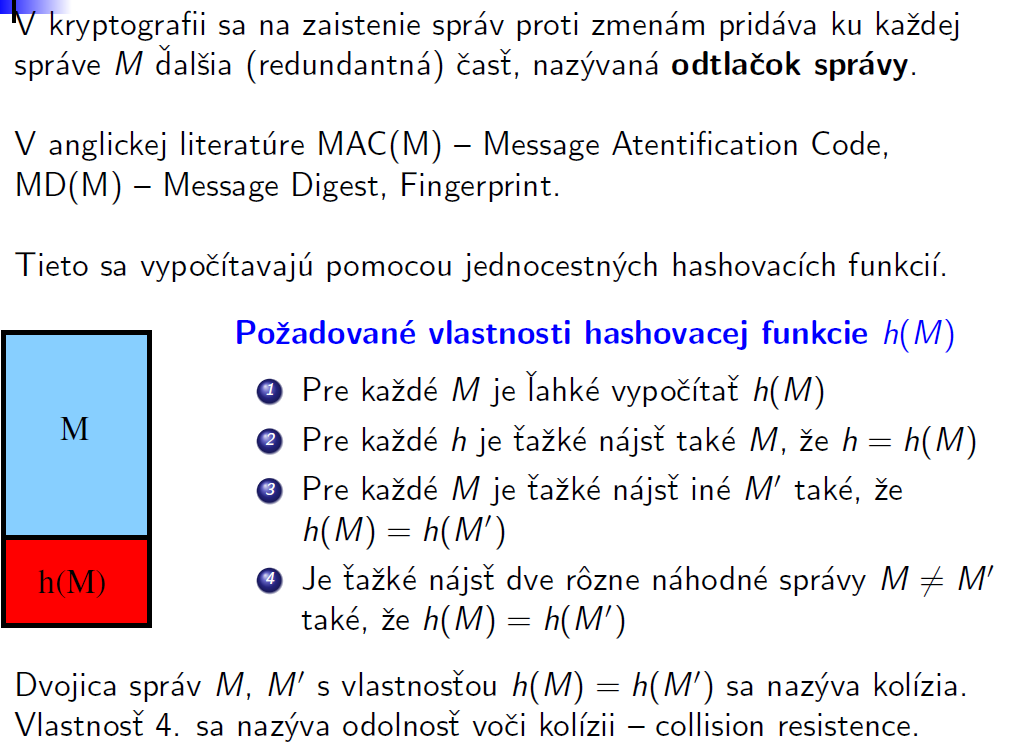




****

**12.Hash funkcie vseobecne, vlastnosti,(vseobecne, MD5, SHA)**

**Vlastnosti hashu by prednáška:**

****

**Medzi hlavné vlastnosti hashovacej funkcie patrí:**  
- Rýchlosť transformácie – zo vstupu sa rýchlo vyráta HASH

- Lavínovitosť - malou zmenou vstupných dát dosiahneme veľké zmeny na výstupe (odtlačok je odlišný od pôvodného na prvý pohľad)

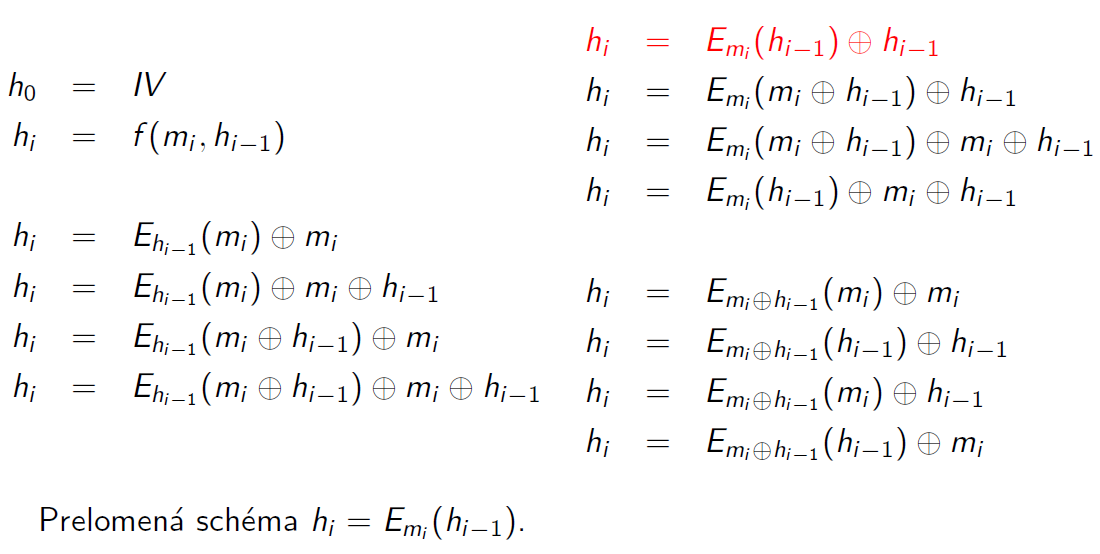
- Jednocestnosť - z hashu je prakticky nemožné rekonštruovať pôvodný text správy (rozdiel oproti klasickému šifrovaniu)

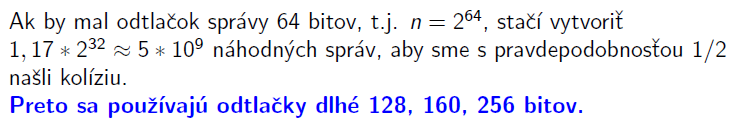
- Bezkolíznosť - odolnosť voči kolízii (dvom rôznym správam odpovedá rovnaký hash ... v praxi veľmi nepravdepodobné, pomocí hashu v praxi identifikovať práve jednu správu (overiť jej správnosť))

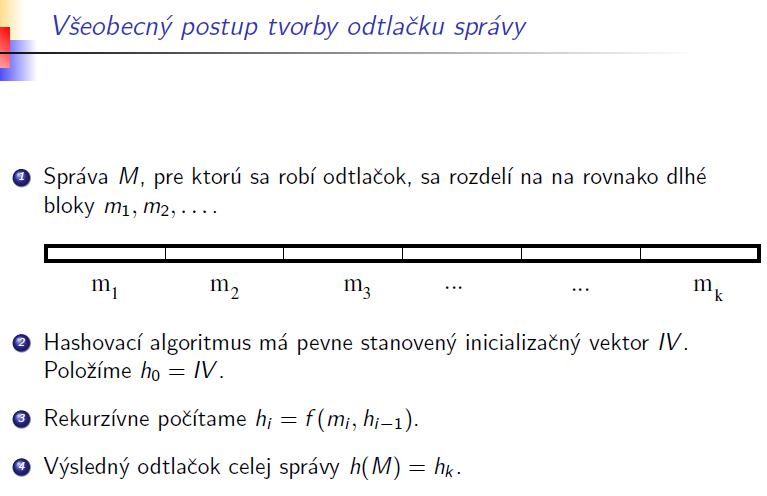
**Hash pomocou kryptosystému:**

hi = Ehi-1(mi) ⃝ (znamienko **+** v krúžku) mi

↑ bude budúci kľúč, takže dĺžka kľúča musí byť rovná dĺžke bloku.

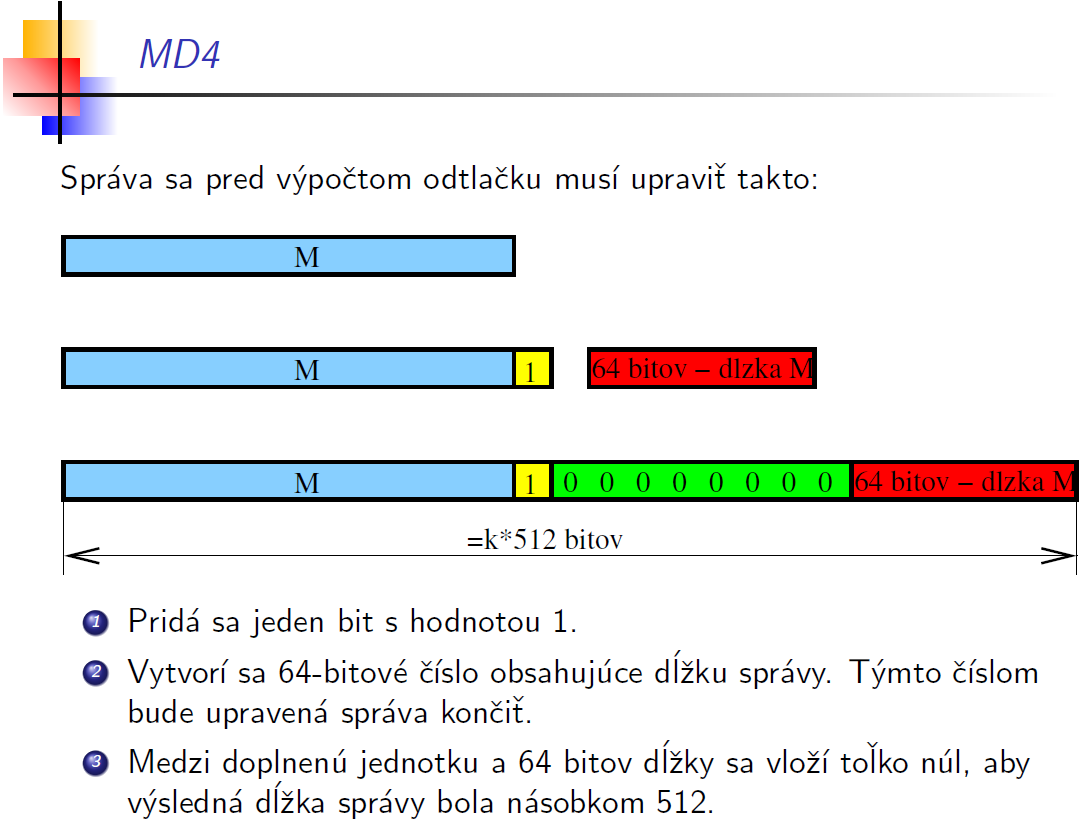


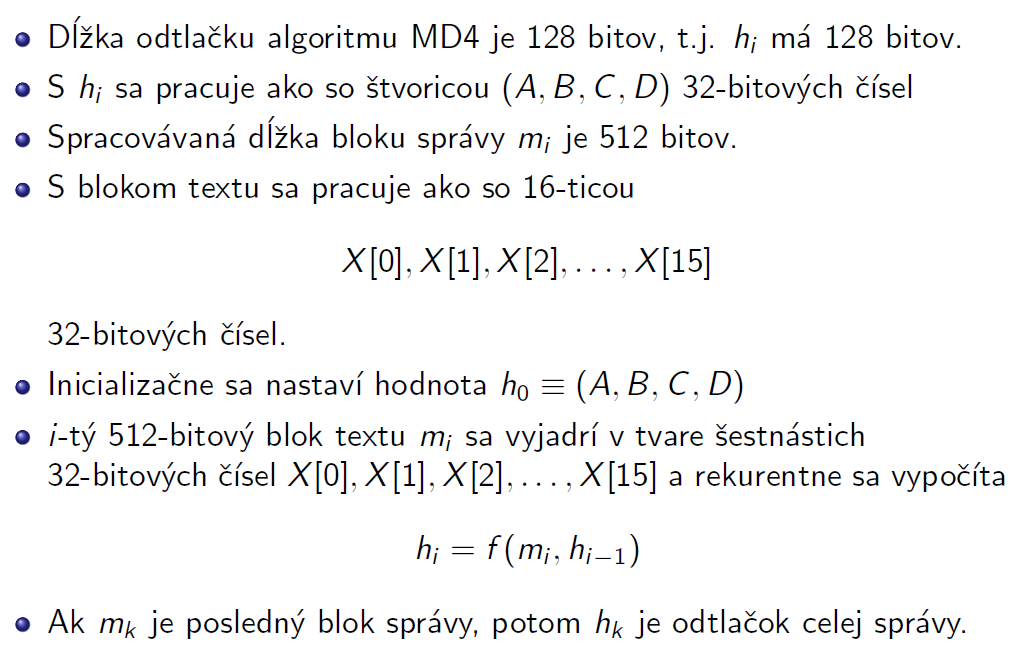




**dlzka odtlacku 3 kola**

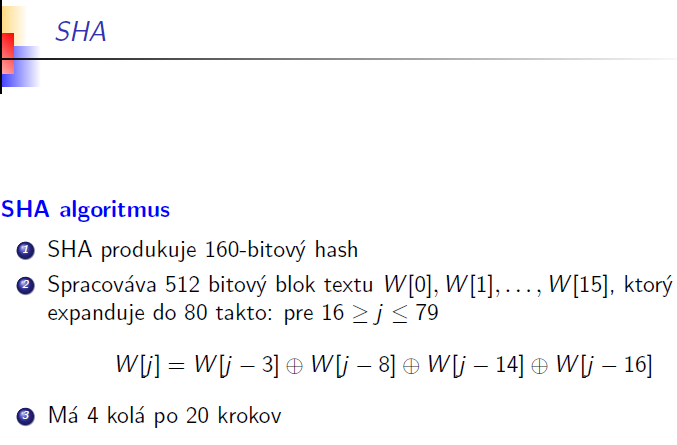
narodeninový paradox – v skupine 23 ľudí sa s pravdepodobnosťou p > ½ nájde dvojica ktorá má v ten istý deň narodeniny

****

****

**SHA:**

* Vyvinuli v NSA
* Náhrada MD5
* SHA-0 prelomený => použ. SHA-1 / SHA-2 / SHA-3

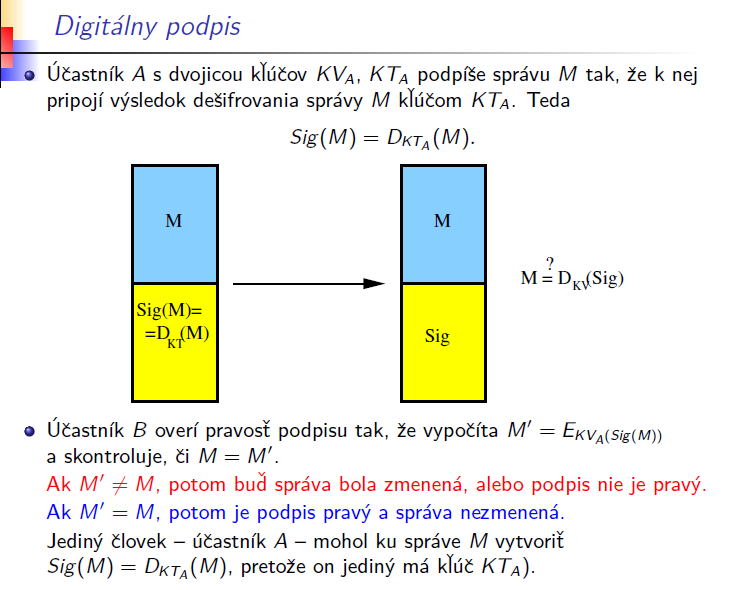


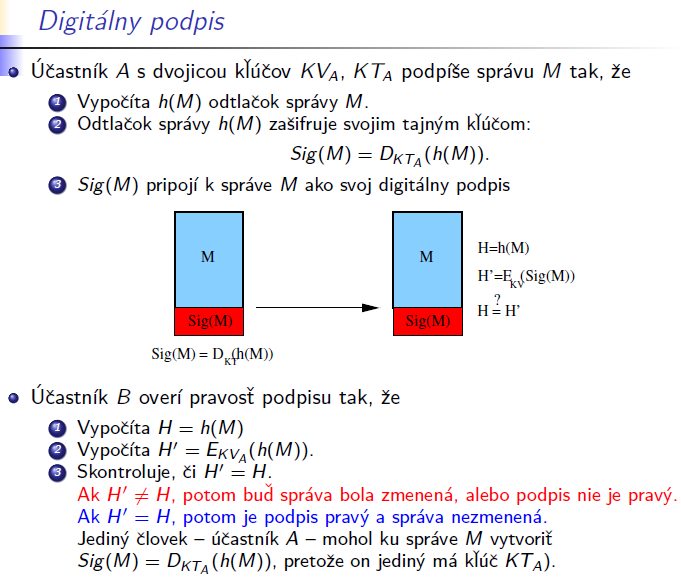
**SHA-256:**

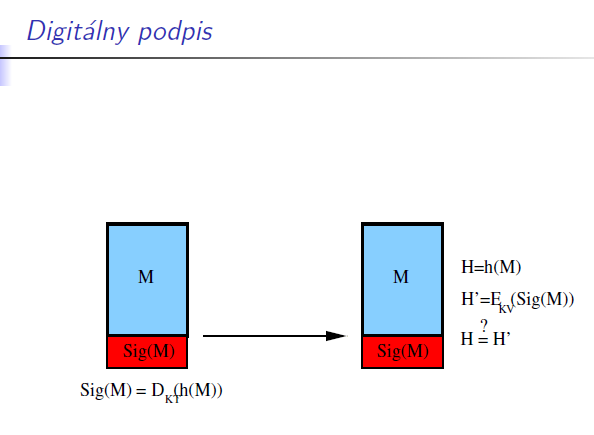
* dĺžka hashu 256
* patrí k najviac používaným
* prelomenie sa považuje za prakticky nemožné
* konštruovaná ako vysoko nelineárna
* patrí do „rodiny“ SHA-2

**13.Digitalny podpis - (plus Birdthday attack, zmenky)**

Používa sa na overenie integrity údajov, neumožňuje overiť pôvod údajov - autentifikáciu

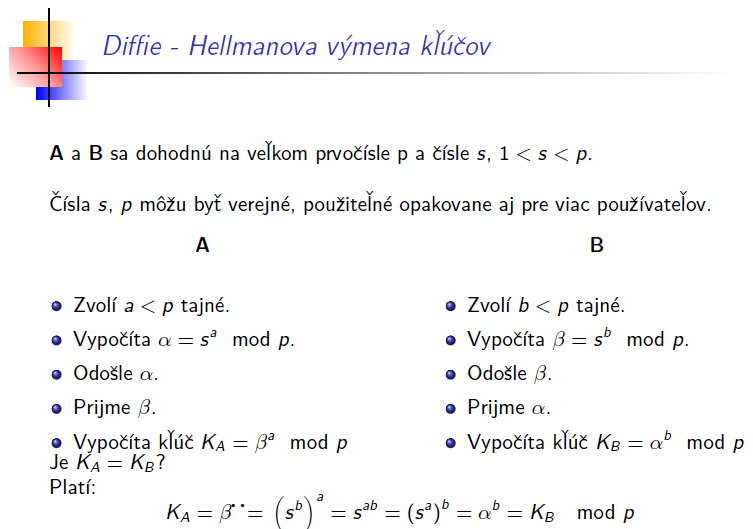


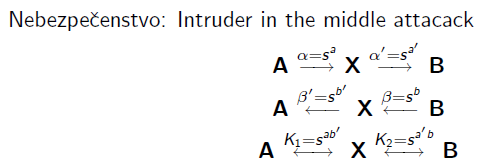






**Deffie – Hellmanova výmena kľúčov**

****

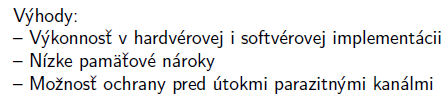
****

**14.AES**

- Symetrická bloková šifra (zrejme najviac použ. sym. blok. šifra súčasnosti)

- dĺžka bloku je 128 bitov

- dĺžka kľúča 128/192/256 – voliteľná



128-bit blok namiesto textu berieme ako postupnosť 16 bajtov:

a00 a10 a20 a30 | a01 a11 a21 a31 | a02 a12 a22 a32 | a03 a13 a23 a33

Tie sa usporiadajú do tabuľky, ktorá sa volá stav:

|  |  |  |  |
| --- | --- | --- | --- |
| a00 | a01 | a02 | a03 |
| a10 | a11 | a12 | a13 |
| a20 | a21 | a22 | a23 |
| a30 | a31 | a32 | a33 |

Stav

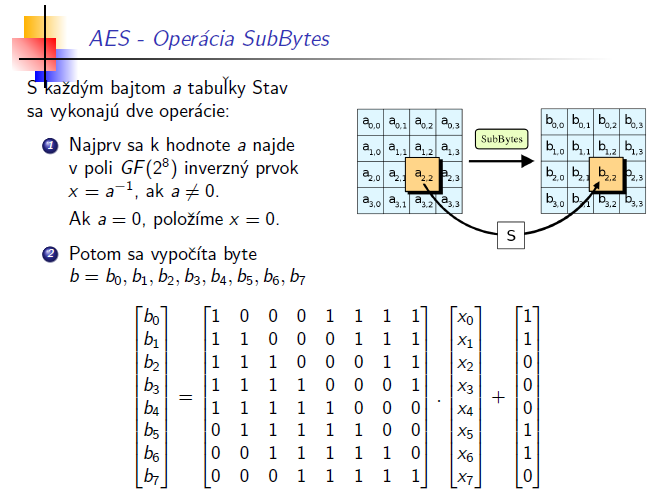
|  |  |  |  |
| --- | --- | --- | --- |
| k00 |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  | k33 |

Kolový kľúč

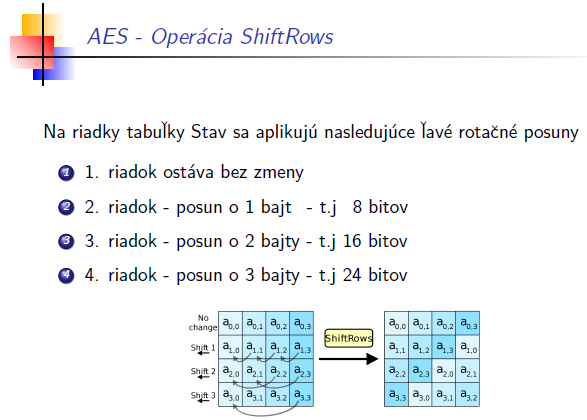
S týmto stavom sa iteračne vykonáva niekoľko kôl operácií (10,12,14 – podľa dĺžky kľúča), niektoré z nich závisia na kolovom kľúči reprezentovanom ako matica bajtov.  
  
AES je jediný verejne dostupný šifrovací algoritmus schválený NSA pre najtajnejšie informácie.

Pre stavovú maticu sú definované 4 elementárne operácie:  
- substitúcia bajtov (SubBytes)  
- rotácia riadkov (MixColumns)  
- substitúcia stĺpcov (ShiftRows)  
- pričítavanie iteračného kľúča (AddRoundKey)

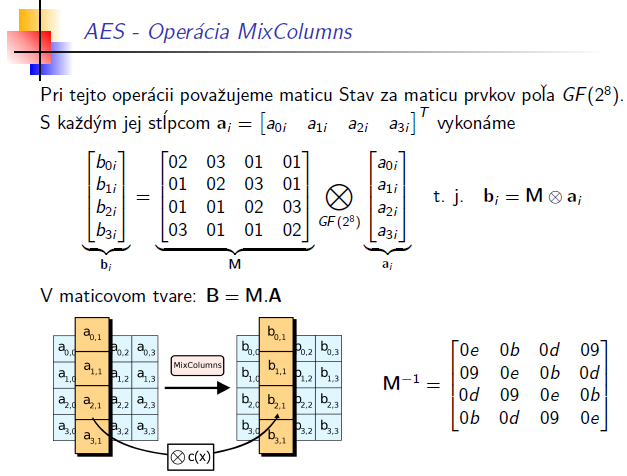
Operácia SubBytes: (Substitúcia bajtov)



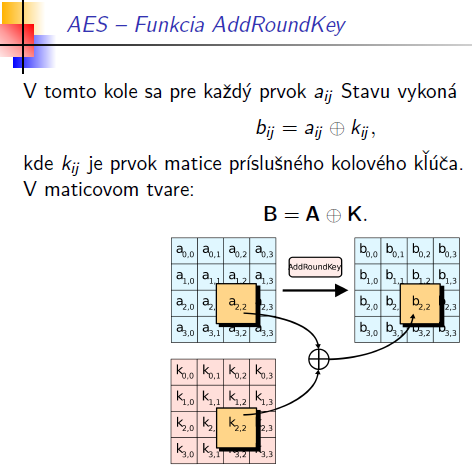
Operácia ShiftRows: (Rotácia riadkov)



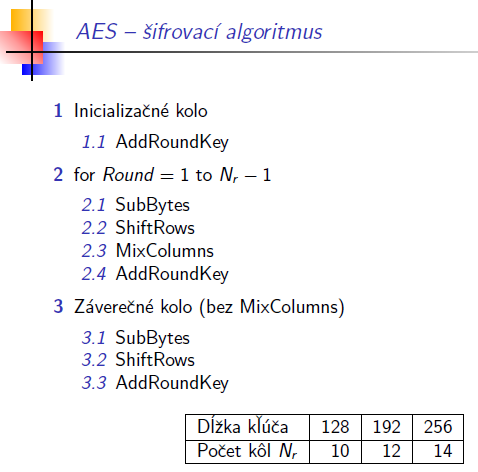
Operácia MixColumns: (Substitúcia stĺpcov)



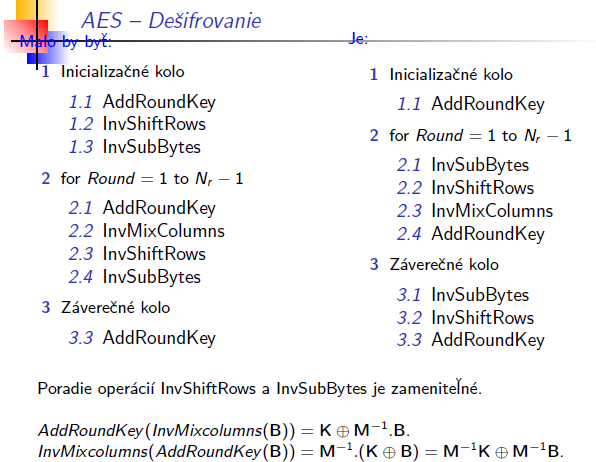
Operácia AddRoundKey: (Pričítavanie iteračného kľúča)



Šifrovanie:



Dešifrovanie:



**15.Asymetricka kryptografia (vseobecne principy, RSA)**

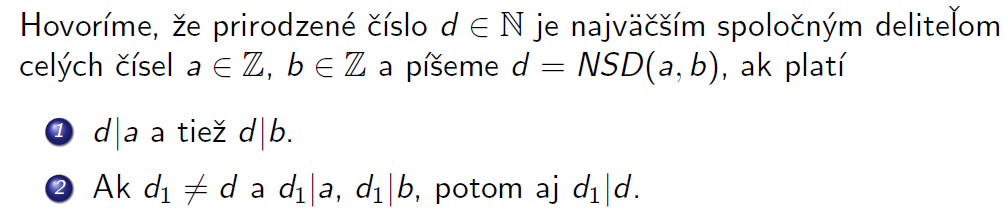
- Pre šifrovanie a dešifrovanie využíva dva odlišné kľúče

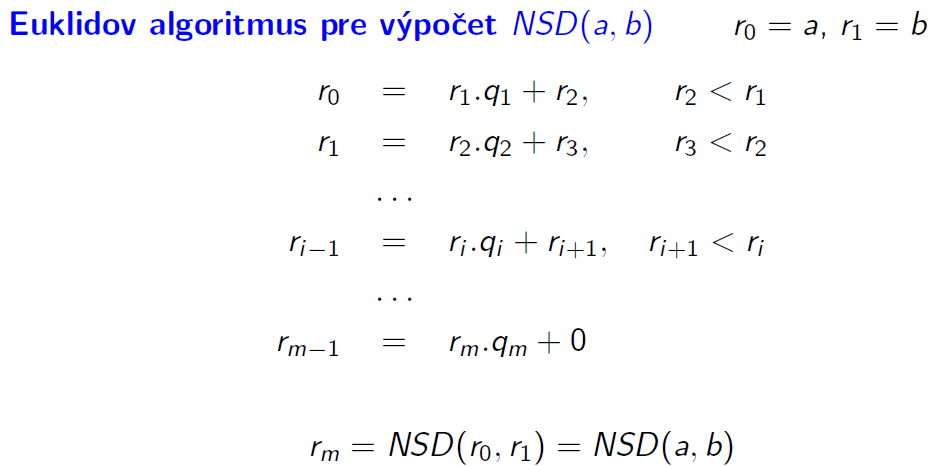
**Všeobecne:**

Základná veta aritmetiky hovorí, že každé prirodzené číslo m > 1 sa dá jednoznačne napísať ako m = p1α1 \* p2α2.... pkαk , kde

p1.... pk sú navzájom rôzne prvočísla a αi sú prirodzené čísla.

**Najväčší spoločný deliteľ:**



****

**Nevýhody symetrickej kryptografie:**  
- každá dvojica účastníkov musí udržiavať svoj kľúč a teda kľúčov je veľmi veľa a všetky sa musia držať v tajnosti.

**Princíp kryptografie s verejným kľúčom:**

-Každý účastník A ma jednu dvojicu kľúčov – verejný kľúč KV(A) a tajný kľúč KT(A). Verejný kľúč KV sa zverejní a tajný KT sa utají.

-Účastník A šifruje správu x účastníkovi B tak, že nájde verejný kľúč KV(B) a pošle správu y = EKV(B)(x)

-Účastník B dešifruje správu y predpisom x = DKT(B)(y).

**RSA algoritmus:**

1. Účastník A zvolí 2 veľké prvočísla p,q.
2. n = p \* q
3. Vypočítame Eulerovu funkciu ɸ(n) = (p-1)(q-1)
4. Ďalej zvolí 2 čísla 0 < e < ɸ(n), 0 < d < ɸ(n) také, že:

e\*d ≡ 1 mod ɸ(n)

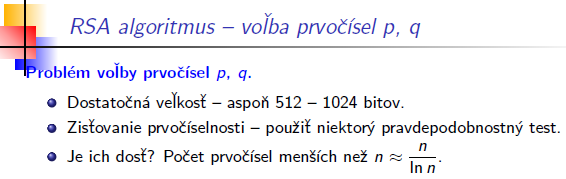
1. Verejný kľúč účastníka A je dvojica (e, n), jeho tajný kľúč je dvojica (d, n).
2. Účastník B bude správu x < n pre účastníka A šifrovať predpisom:

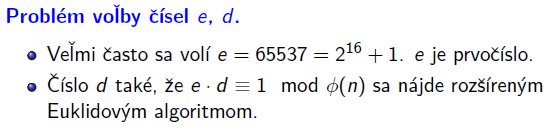
y = xe mod n

1. Účastník A dešifruje správu y predpisom:

x = yd mod n

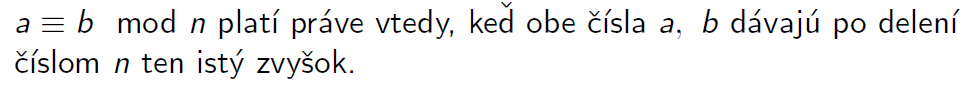
**Voľba prvočísel p,q v RSA:**

****

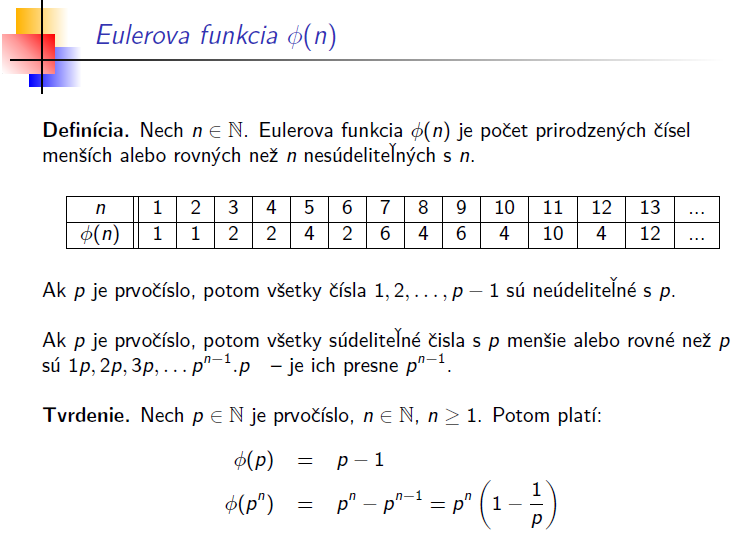
****

Bezpečnosť proti útokom je založená na tom, že rovnicu ***y = xe mod n*** nevieme vyriešiť ani keď poznáme c. Potrebujeme faktorizovať n (rozložiť na prvočísla).

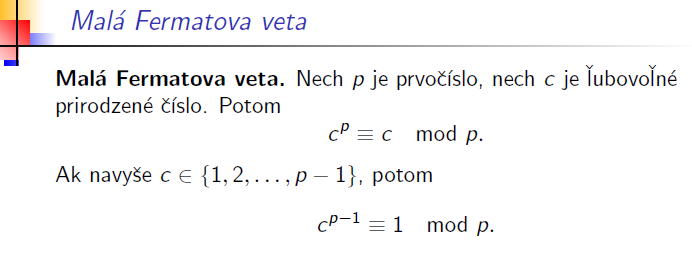
***Kongruencia:***



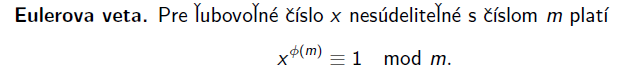
***Eulerova Funkcia:***

****

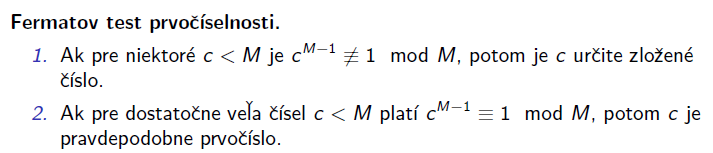
***Malá Fermatova veta:***



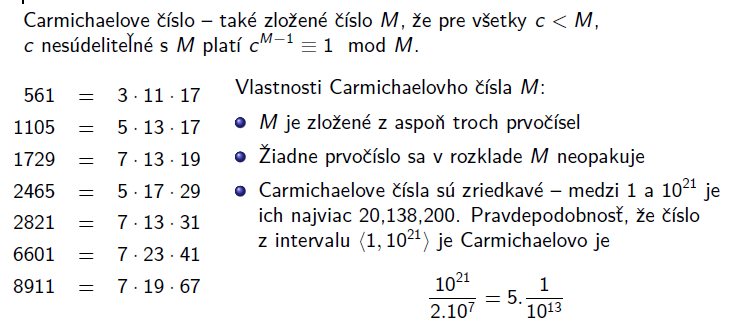
***Eulerova Veta:***



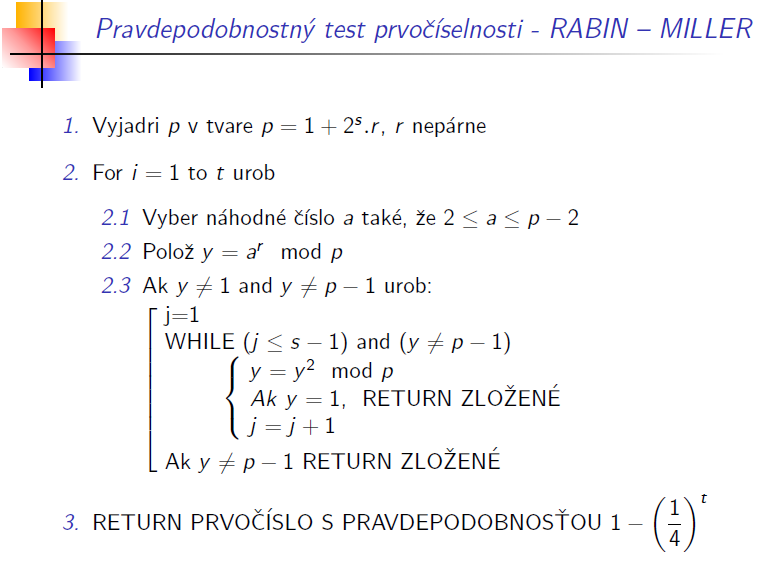
***Fermatov test prvočíselnosti:***



***Carmichaelove čísla:***



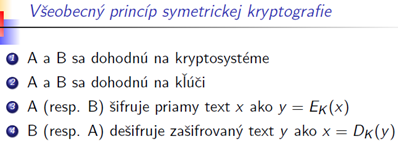
***Rabin Miller test prvočíselnosti:***

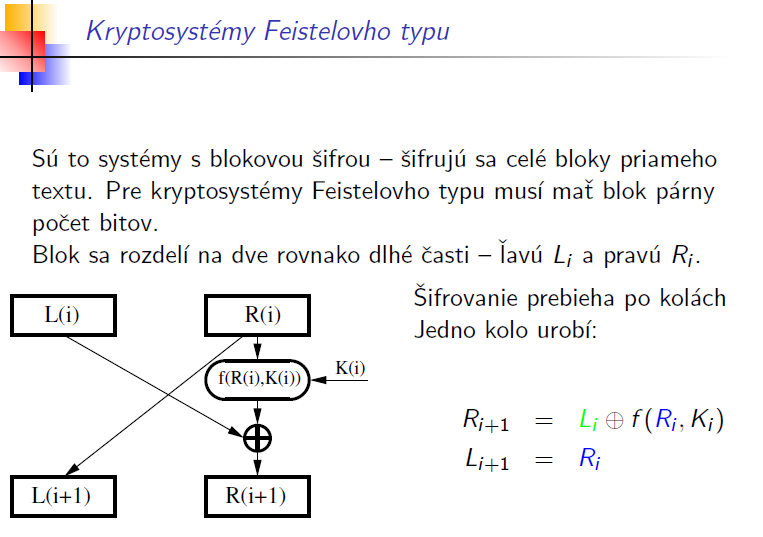


**Lehmannov test**

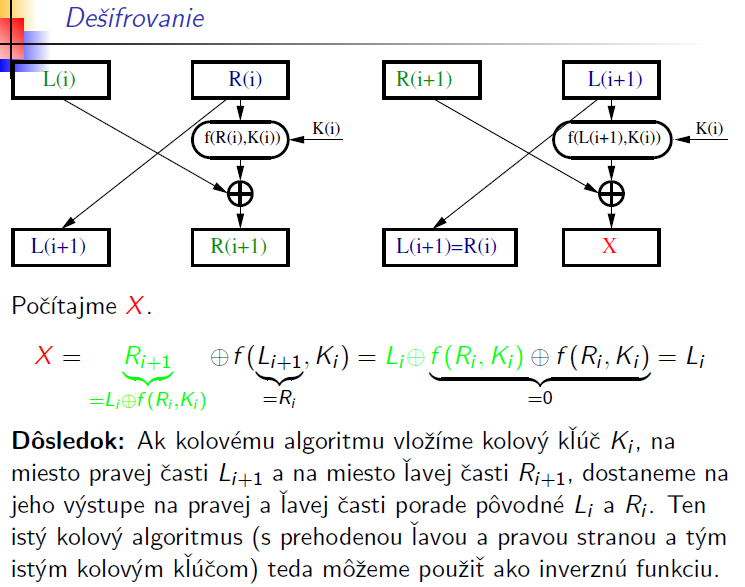
**16.Symetricku kryptografiu - Feistelove kola (hlavne DES - komplet, GOST, IDEA- posledne dve hlavne dlzka bloku a dlzka kluca plus omacka)**

Na šifrovanie aj dešifrovanie sa využíva jediný kľúč čož ma za následok nízku výpočtovú náročnosť avšak nutnosť zdieľania tajného kľúča.

****



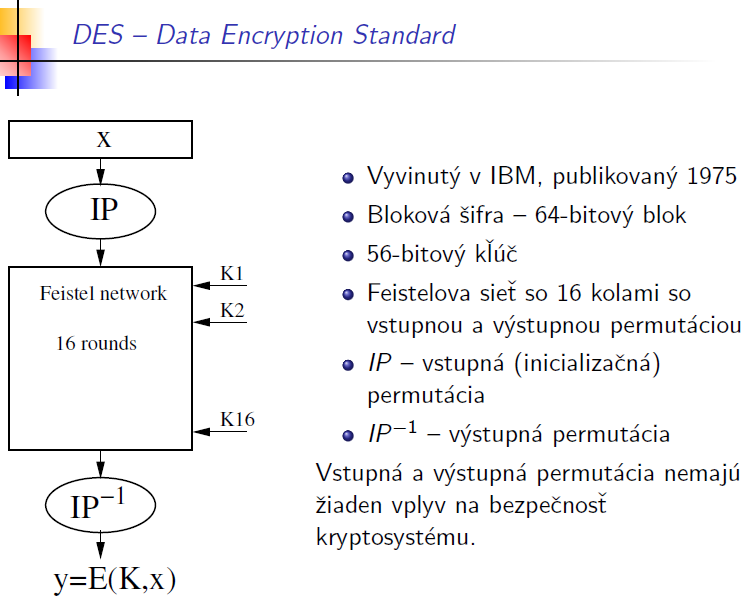
***Dešifrovanie:***

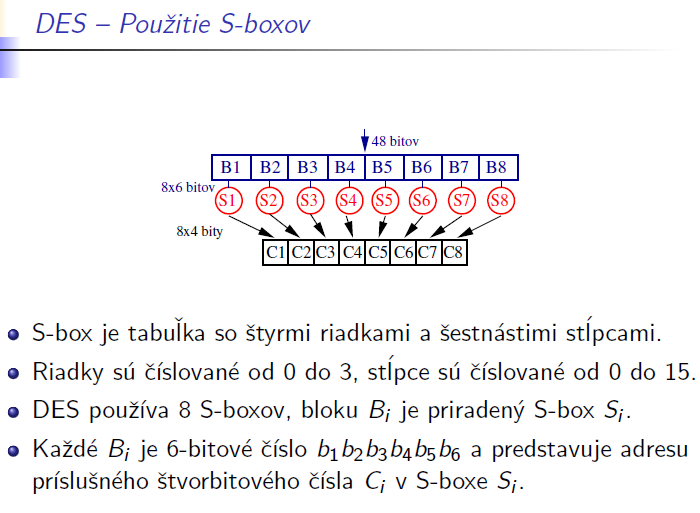


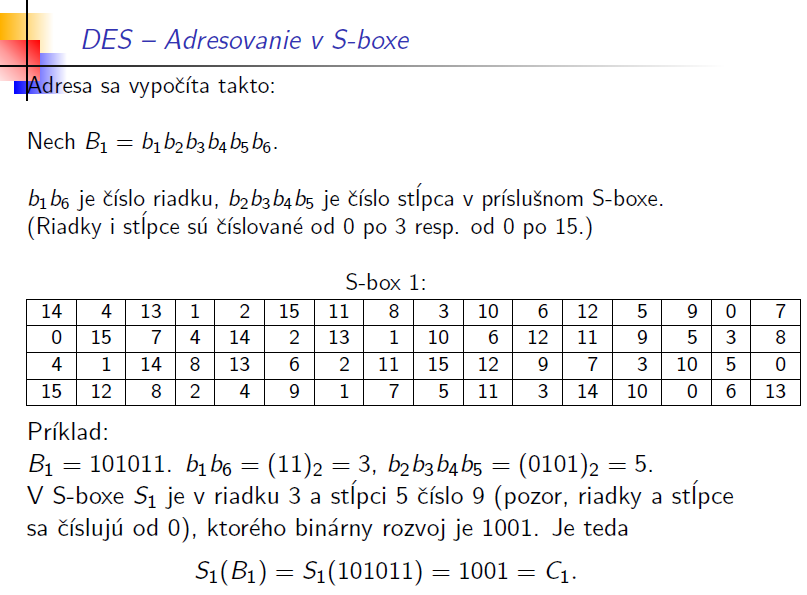
***Feistelová sieť:***

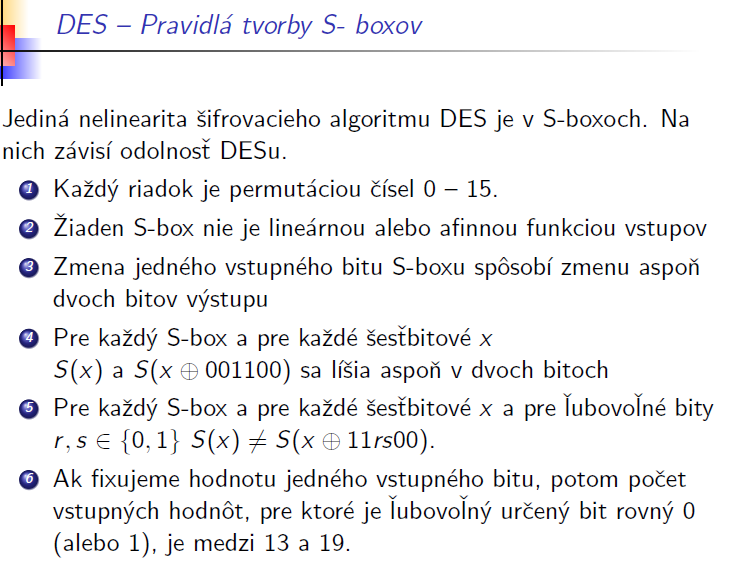
****

***DES:***

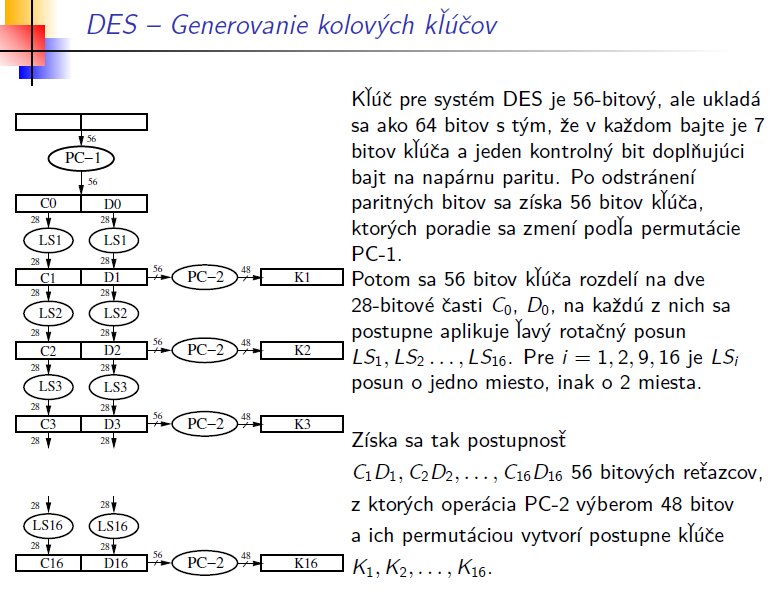




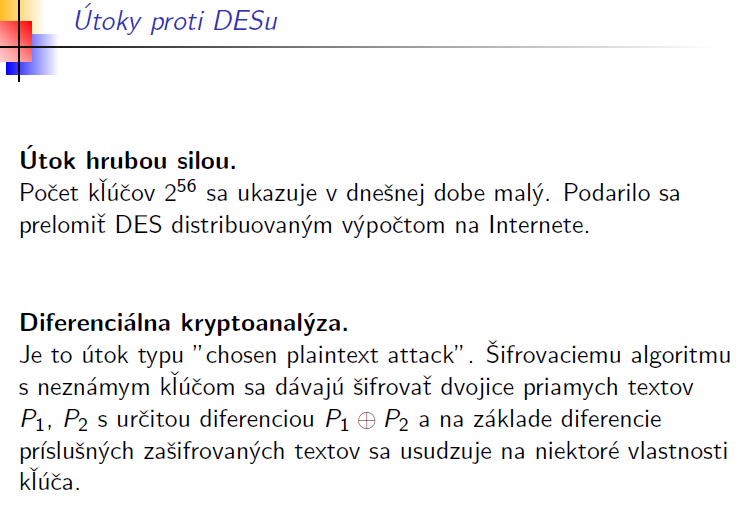




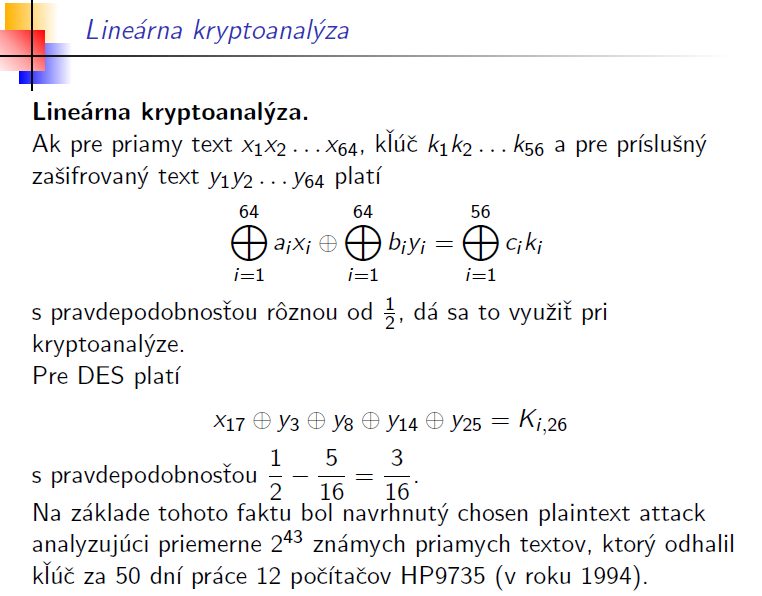
***DES – Generovanie kolových kľúčov:***



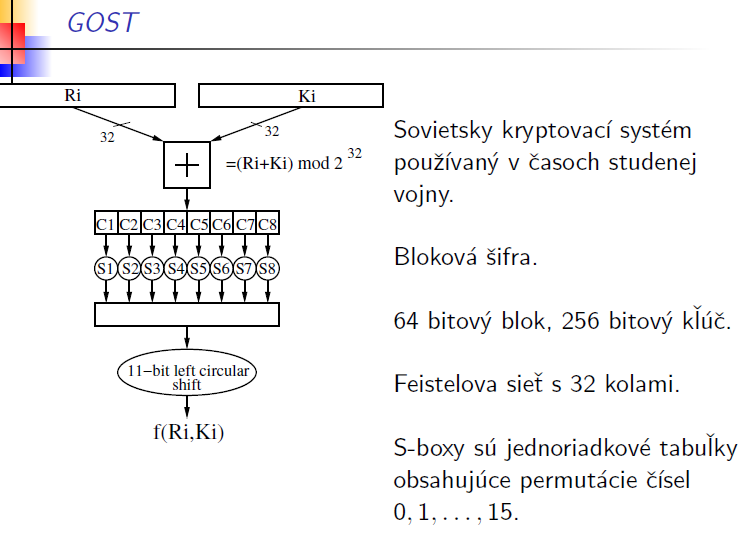
***Útoky proti DESu:***



***Lineárna kryptoanalýza:***



***Gost:***



***IDEA:***

