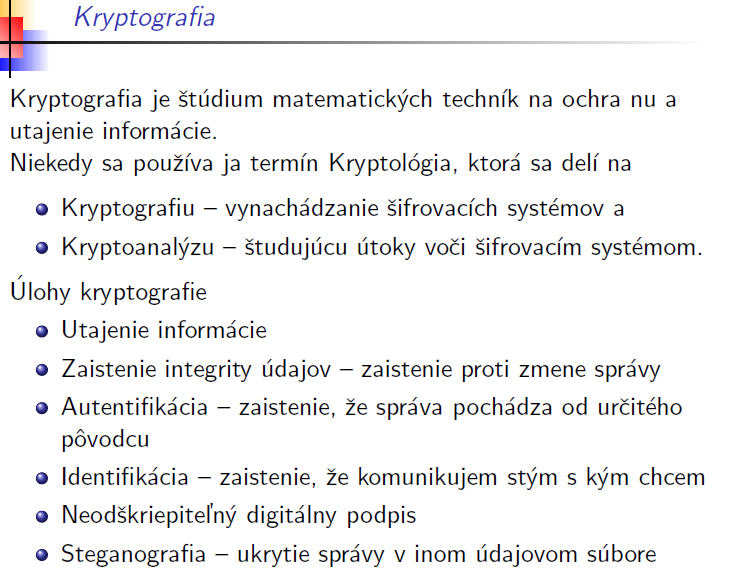
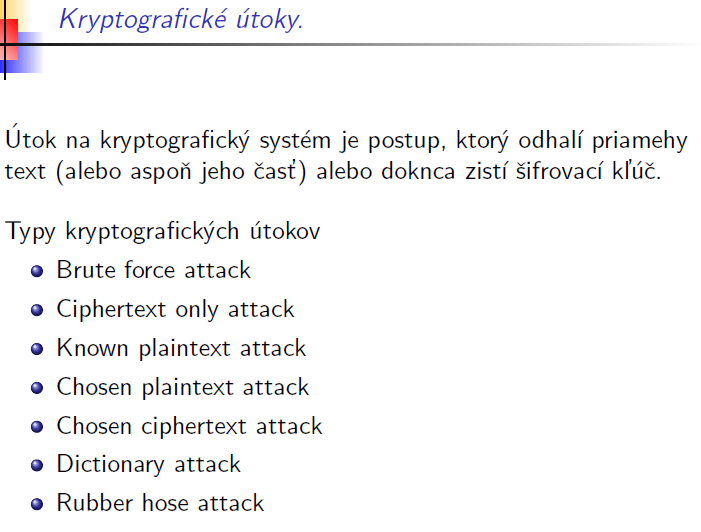
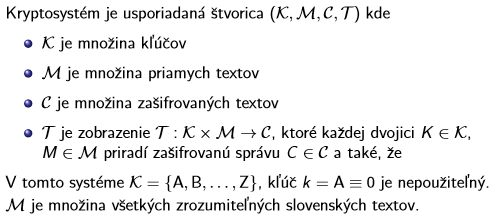
1. **Kryptografia**

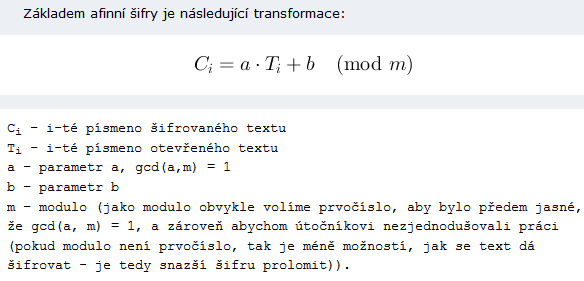


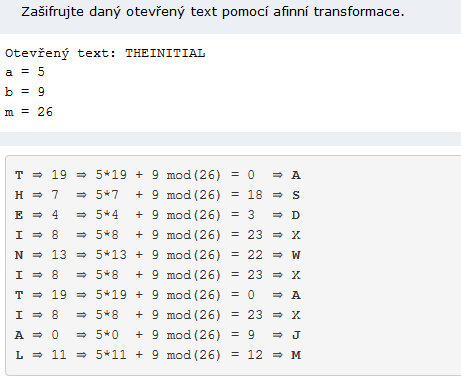
**Kryptografické útoky**

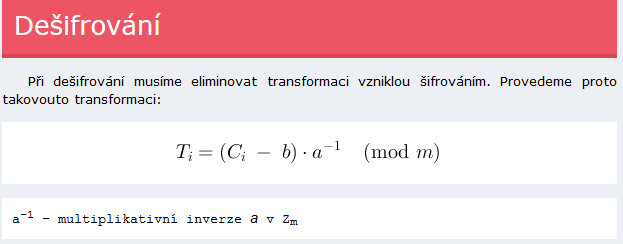


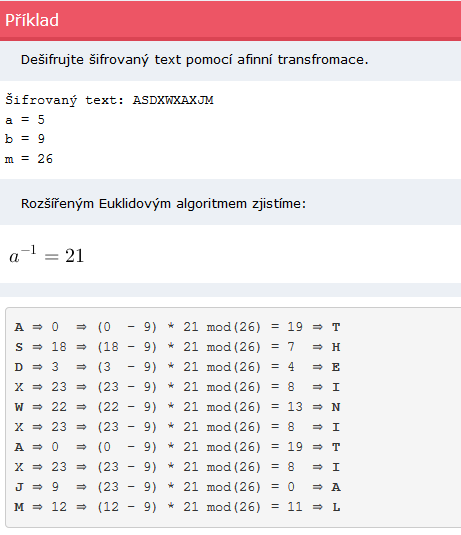


**2. Afinna sifra:**

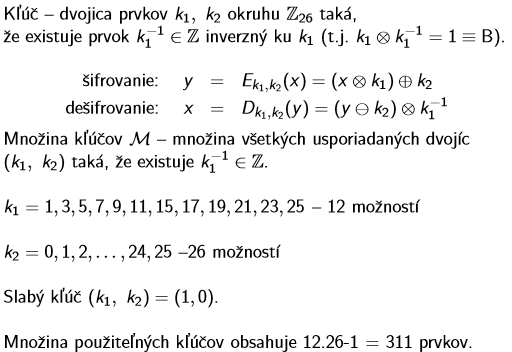


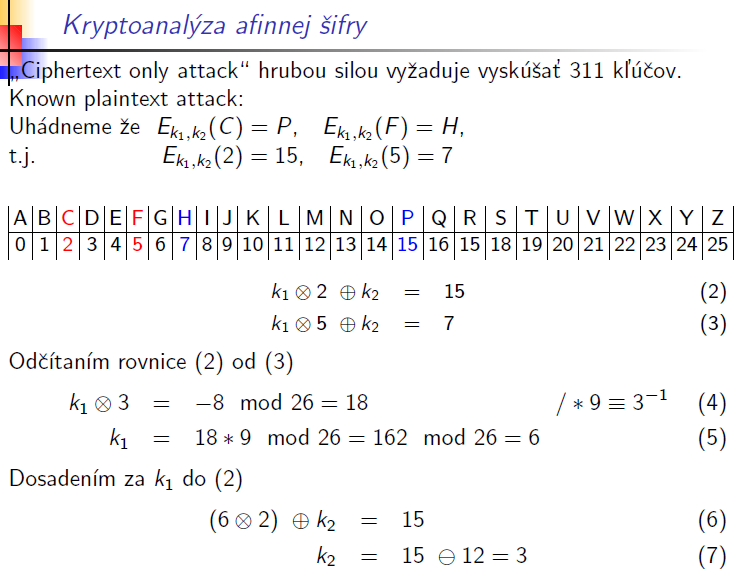




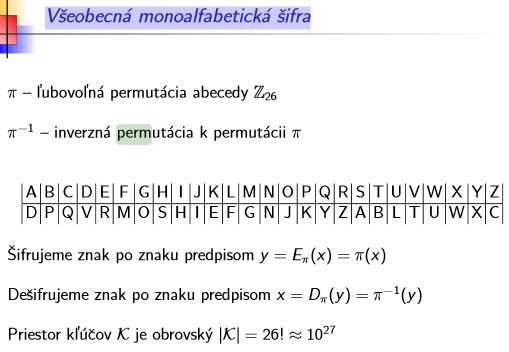


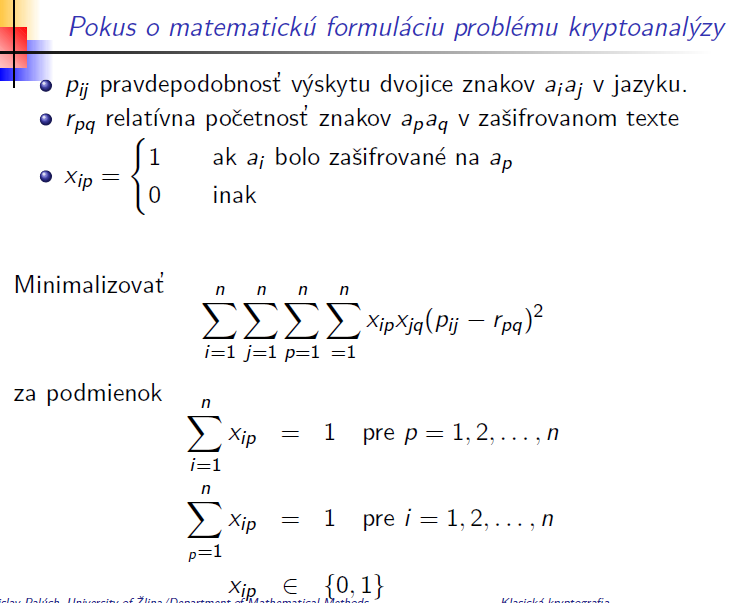


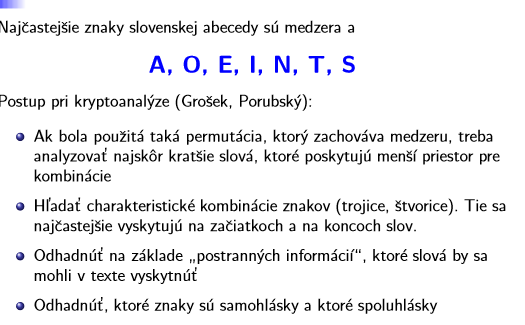


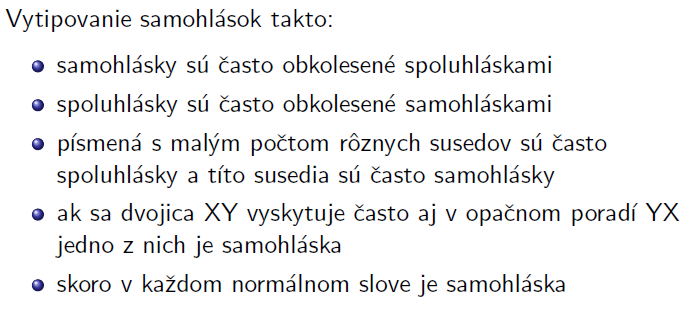


**3. Vseobecna monoalfabeticka sifra**

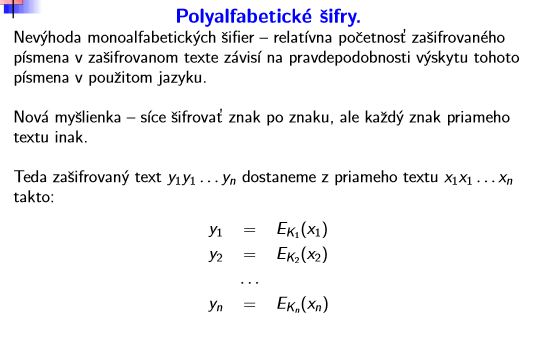


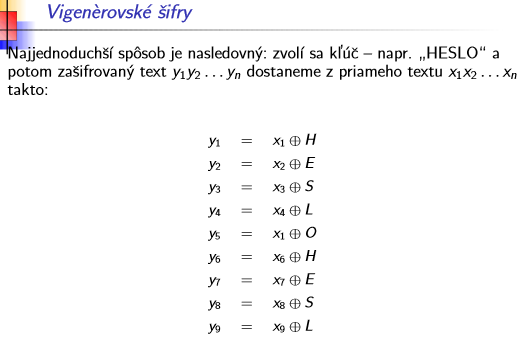


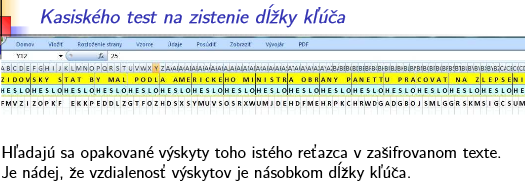




**4. Vigenerovska**

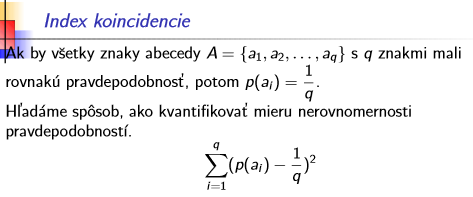


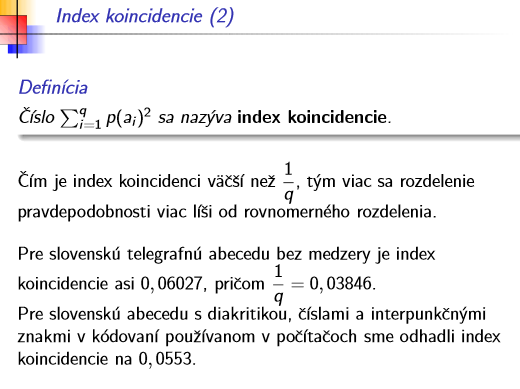


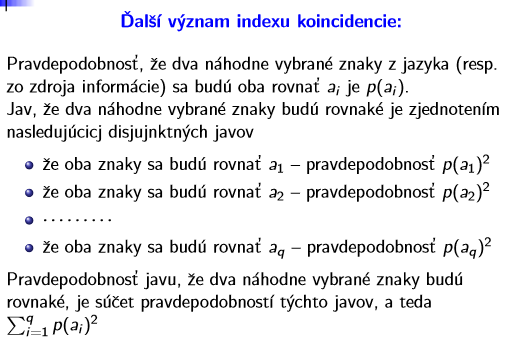


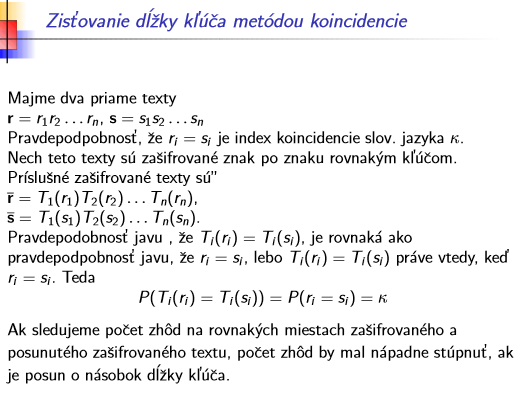


**5. Index koincidencie**

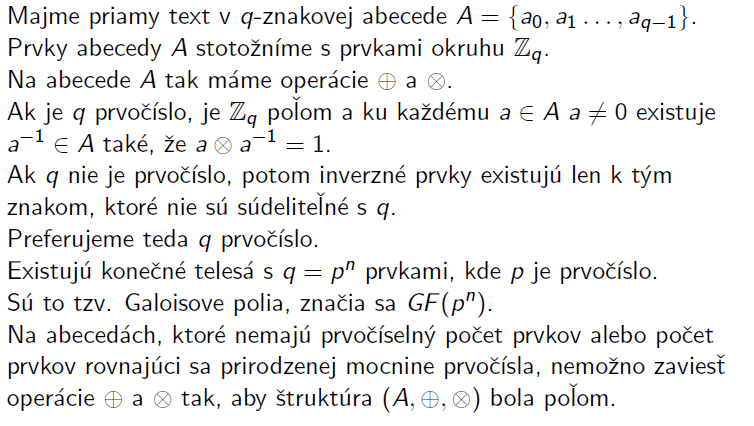


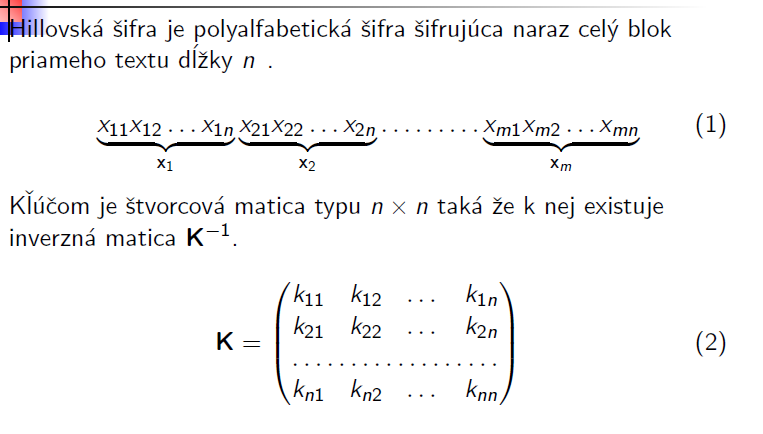


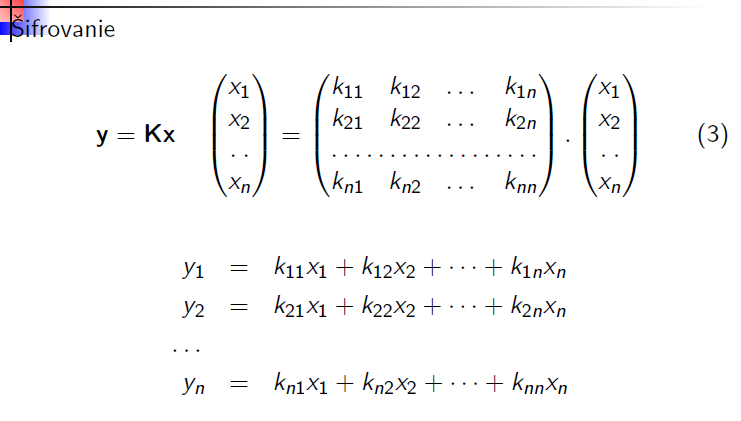


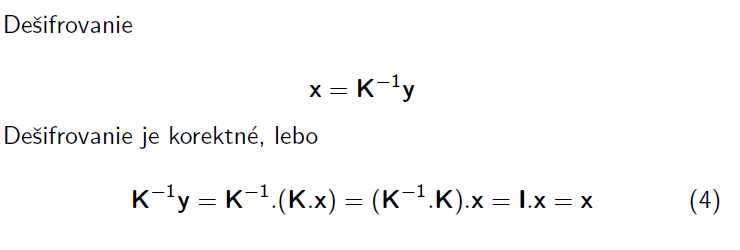


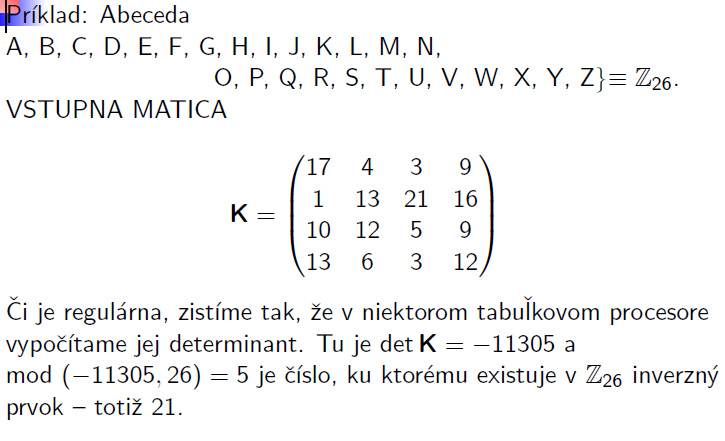
**6.Hillovska sifra**

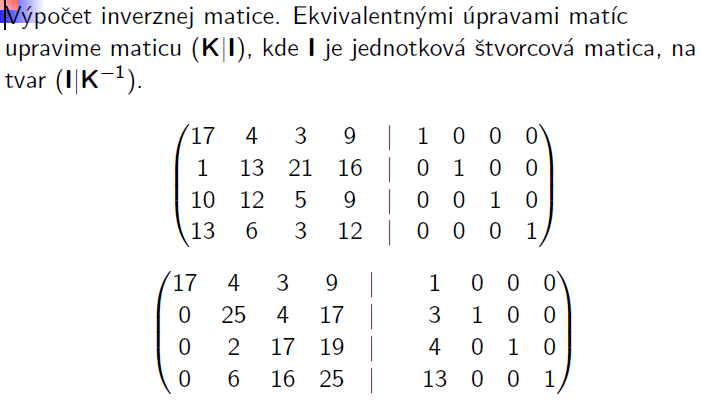


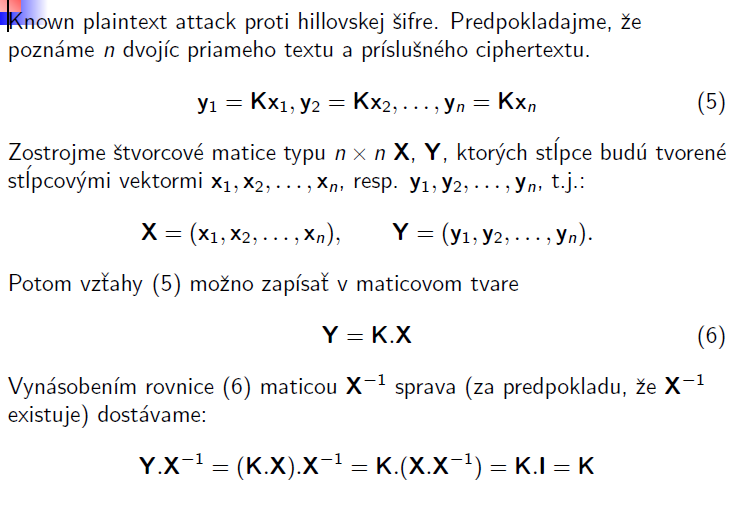




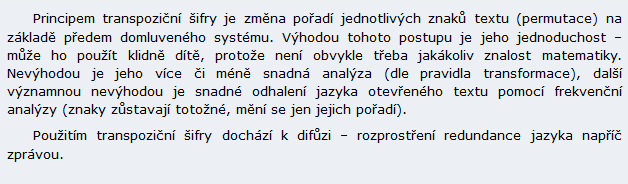


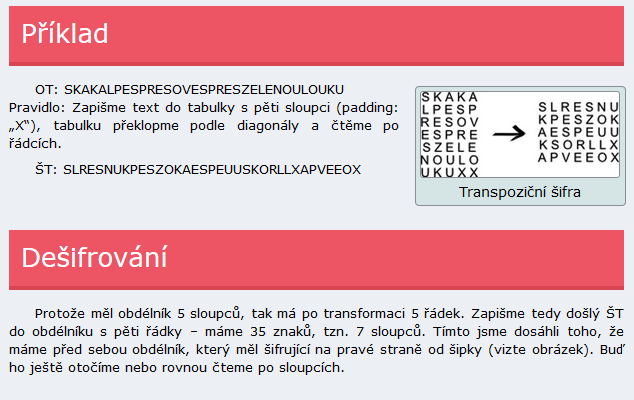


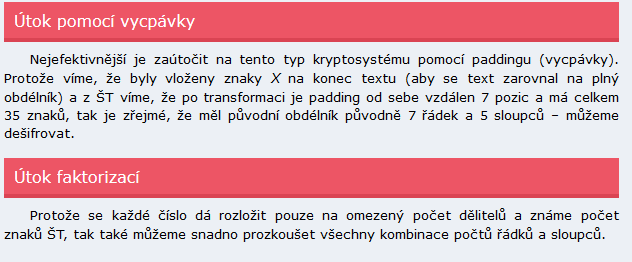




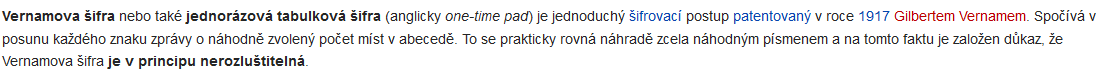
**7. Transpozicna – permutacna sifra**

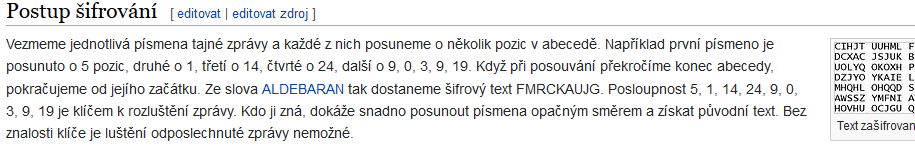


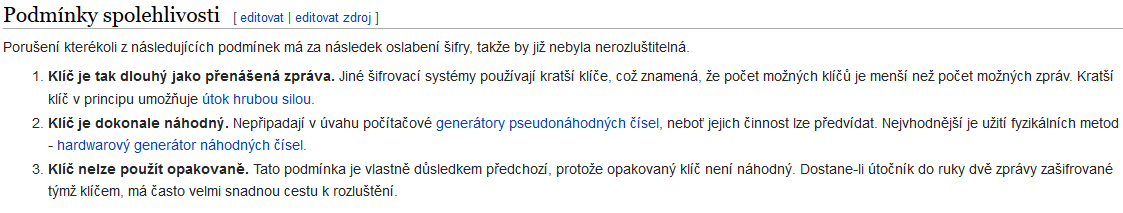


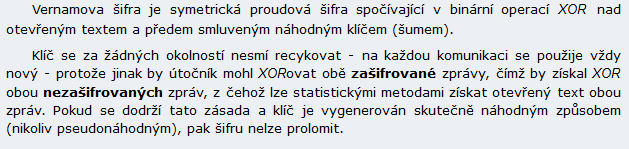


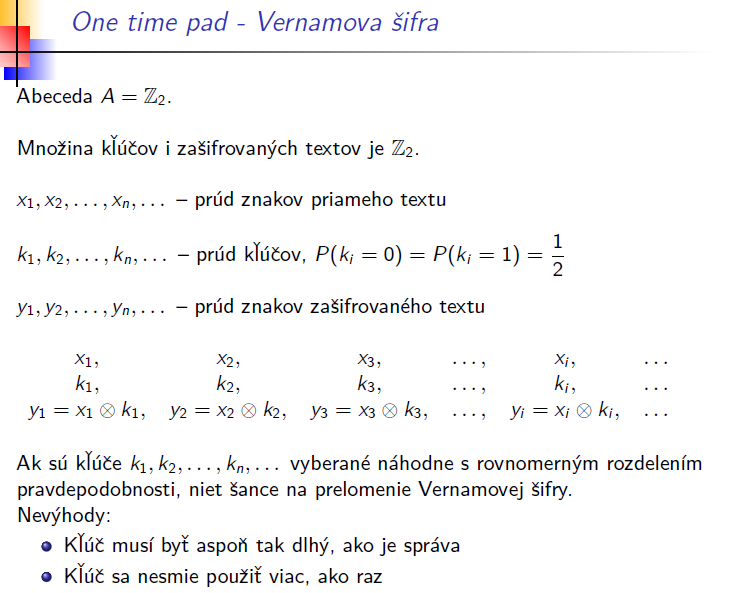
**8. One time Pad + utok (Vernamova šifra)**

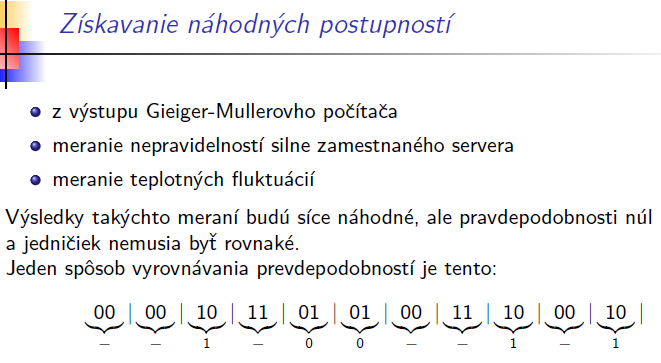




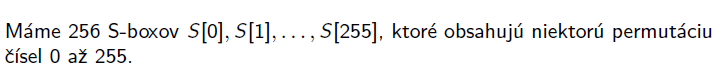


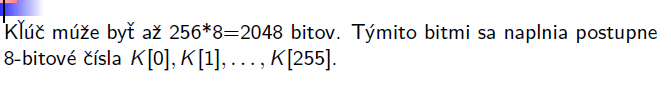


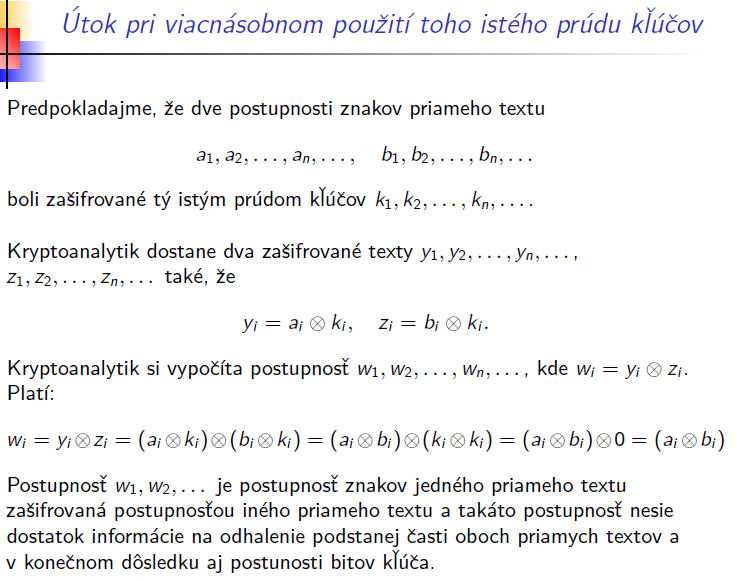


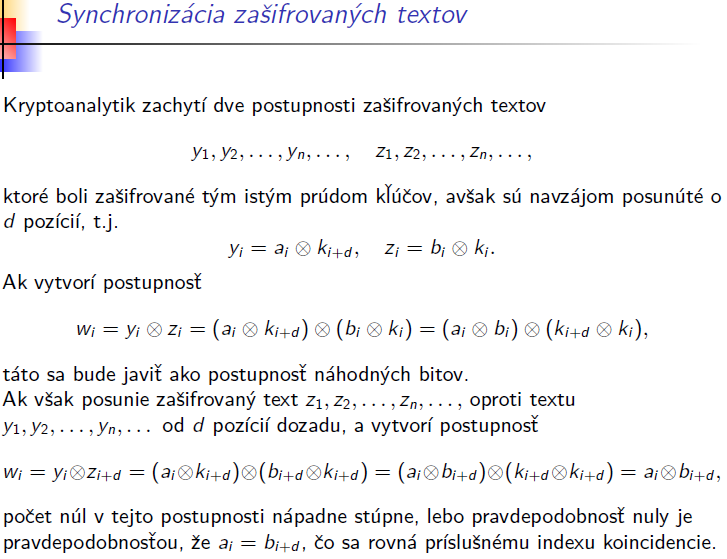


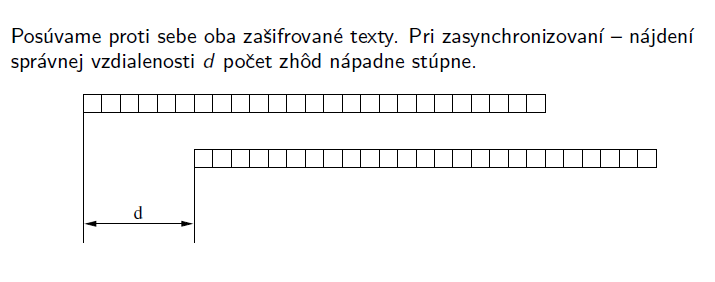






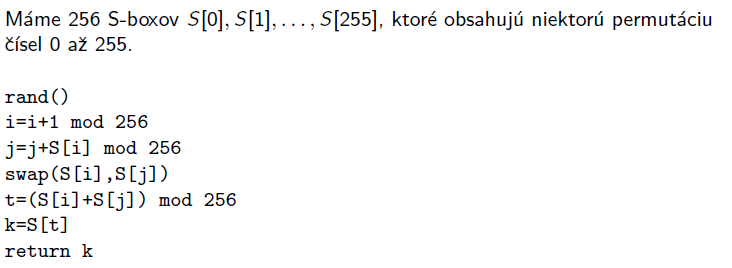


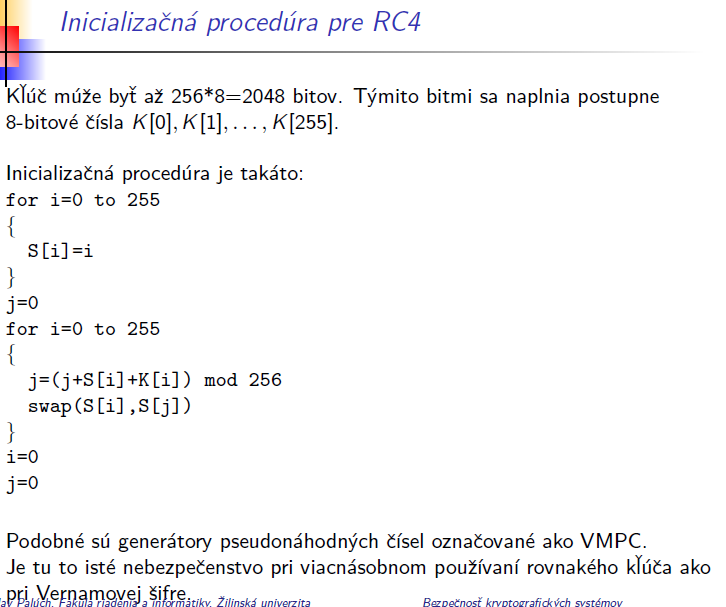




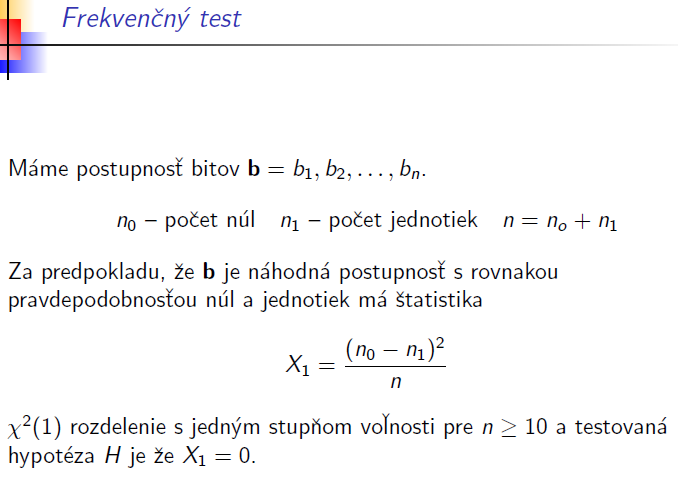
**9.Pseudogeneratory (linearny kongruencny, kvadraticky, kubicky, RC4)**

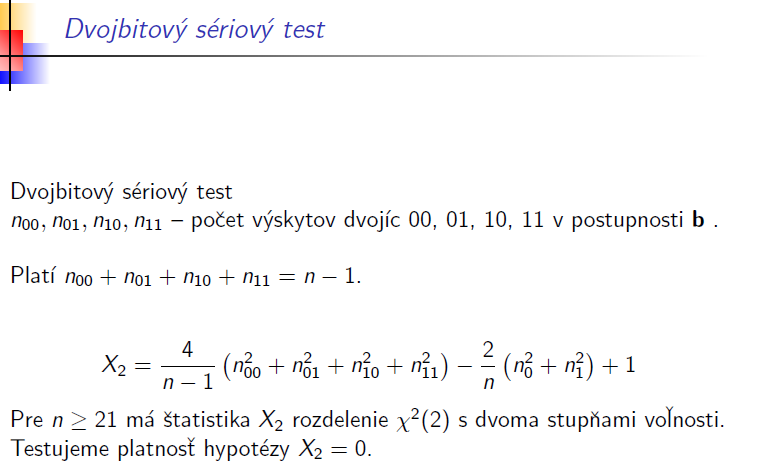




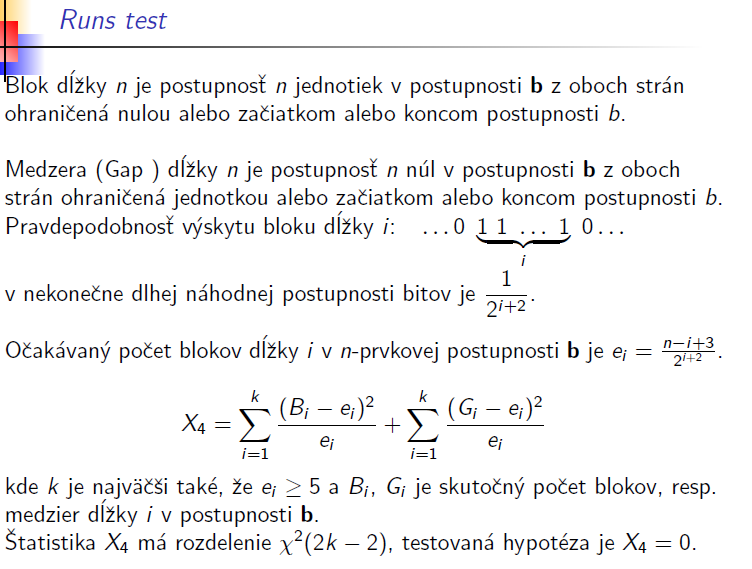


**10.Testy generatorov (frekvencny, TwoBits, Runs, Poker, FIPS 140-1, Autokorelacny)**

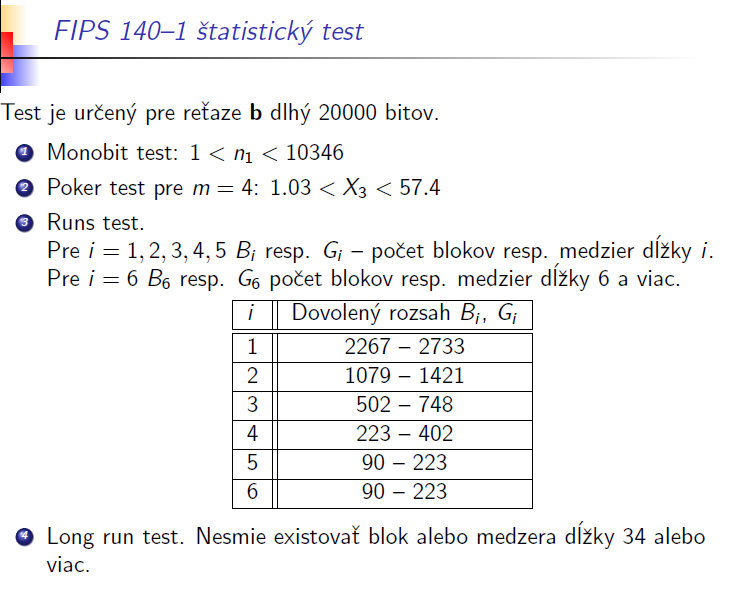




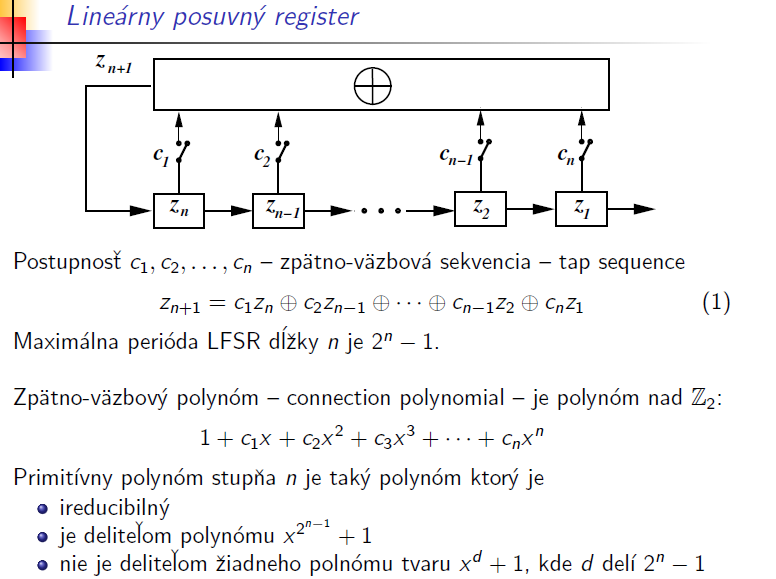


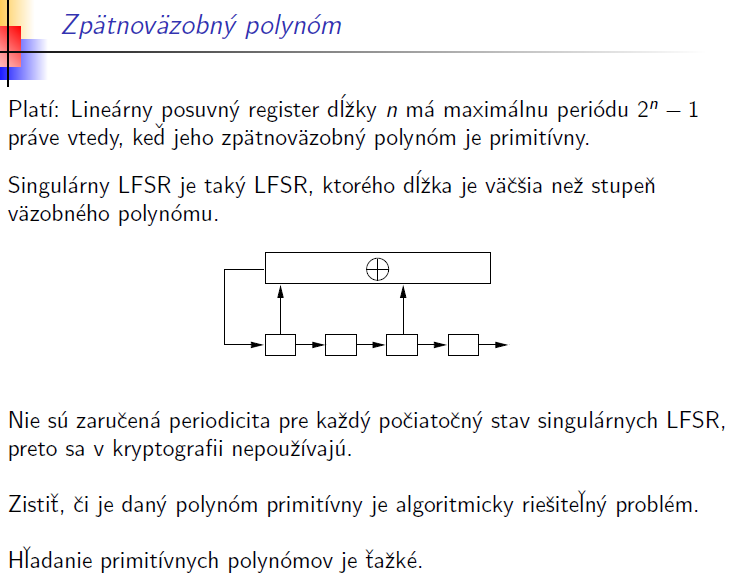




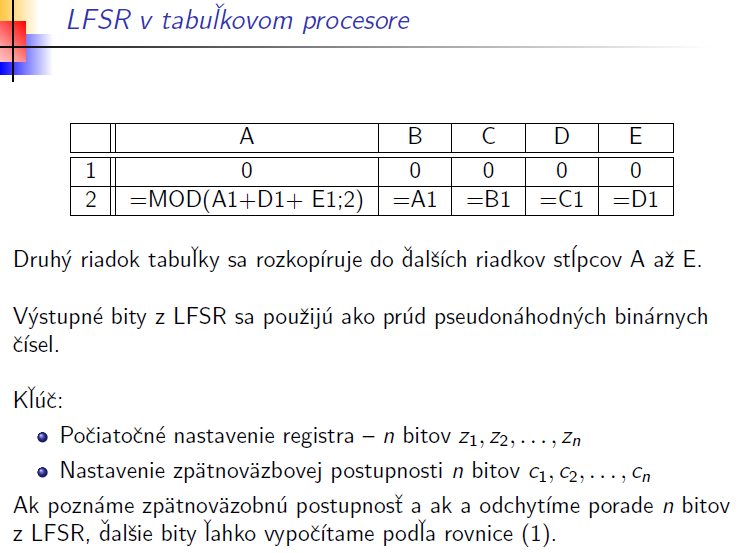


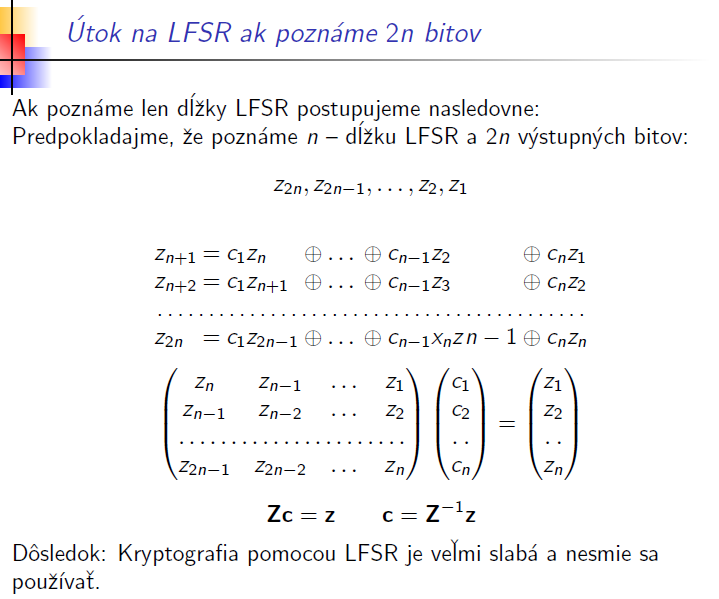
**11.LFSR**

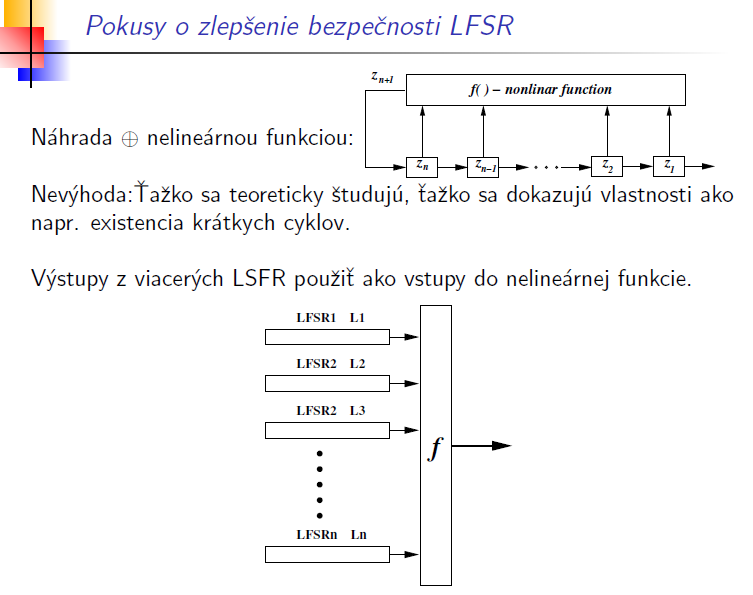






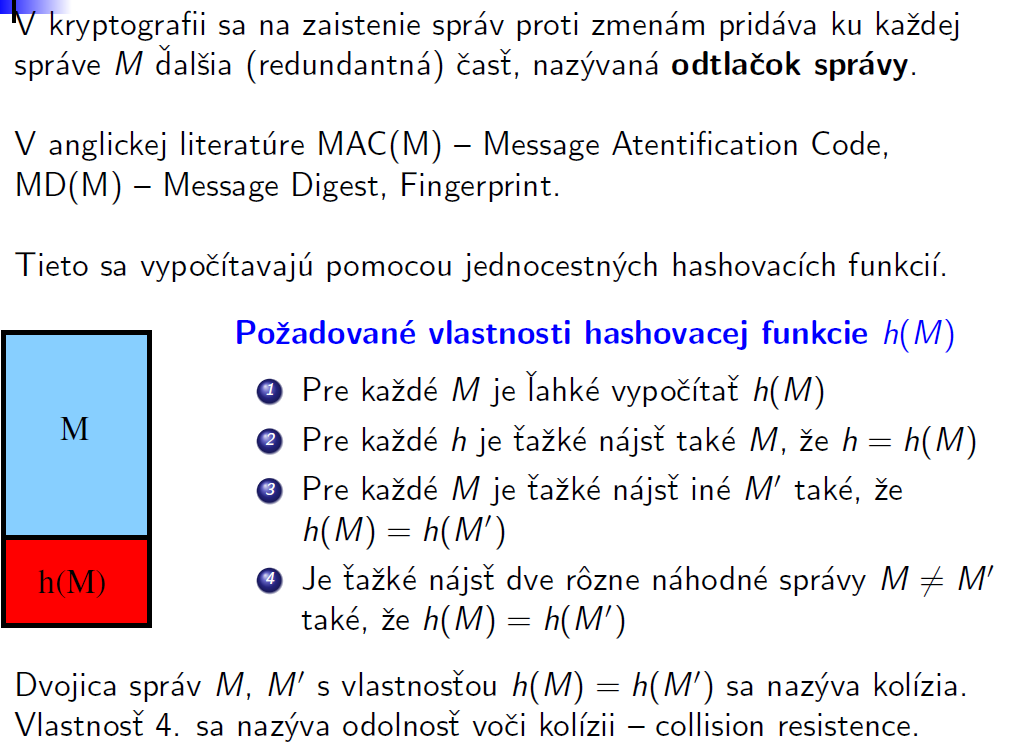






**12.Hash funkcie vseobecne, vlastnosti,(vseobecne, MD5, SHA)**

**Vlastnosti hashu by prednáška:**

****

**Medzi hlavné vlastnosti hashovacej funkcie patrí:**  
- akékoľvek množstvo vstupných dát poskytuje rovnako dlhý výstup (odtlačok)

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

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

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

**Ako sa hash robí:**

Celý blok textu sa rozdelí na menšie bloky:  
| m1 | m2 | m3 | … |

Postupne pričítame hodnotu hi = f (mi hi-1)

h1 = f(m1h0) h0 = IV

h0 sa stanoví na nejaký inicializačný vektor a už sa nemení ďalej (zostáva stále rovnaký)

Máme M = m1 m2 m3 .... mk správu, potom:

H(M) = h(m k) => posledný blok správy

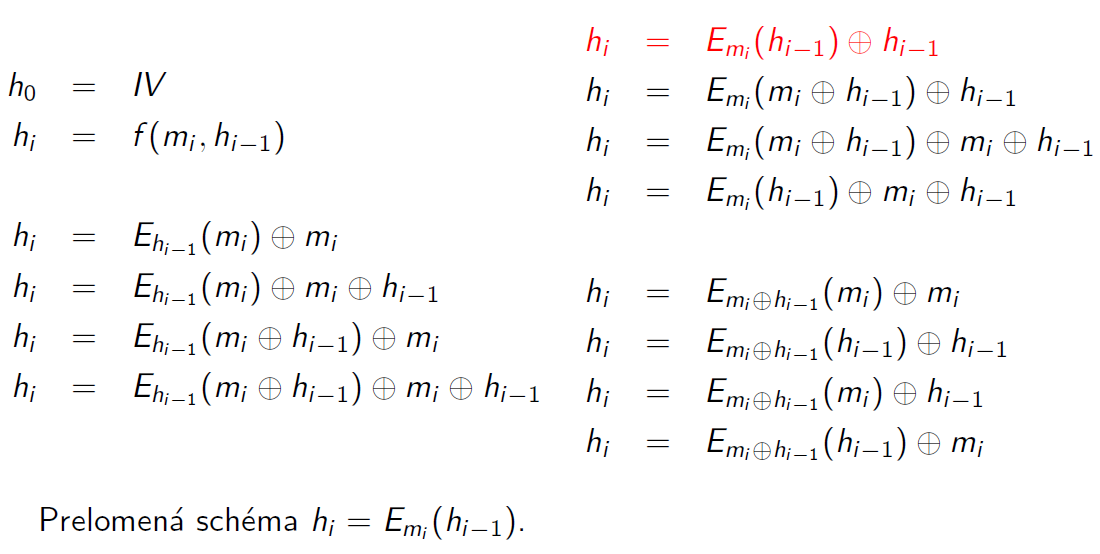
dĺžka => d(H(M)) by mala byť najmenej 128,160,255

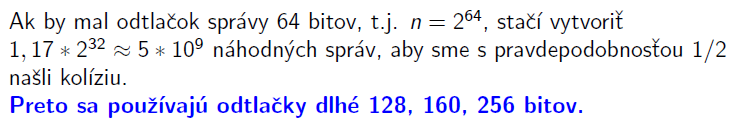
(Kvôli birthday effect)

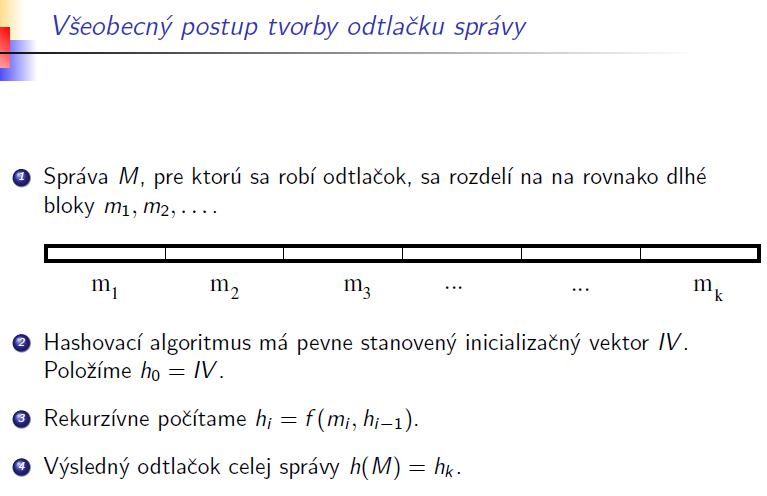
**Hash pomocou kryptosystému:**

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

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

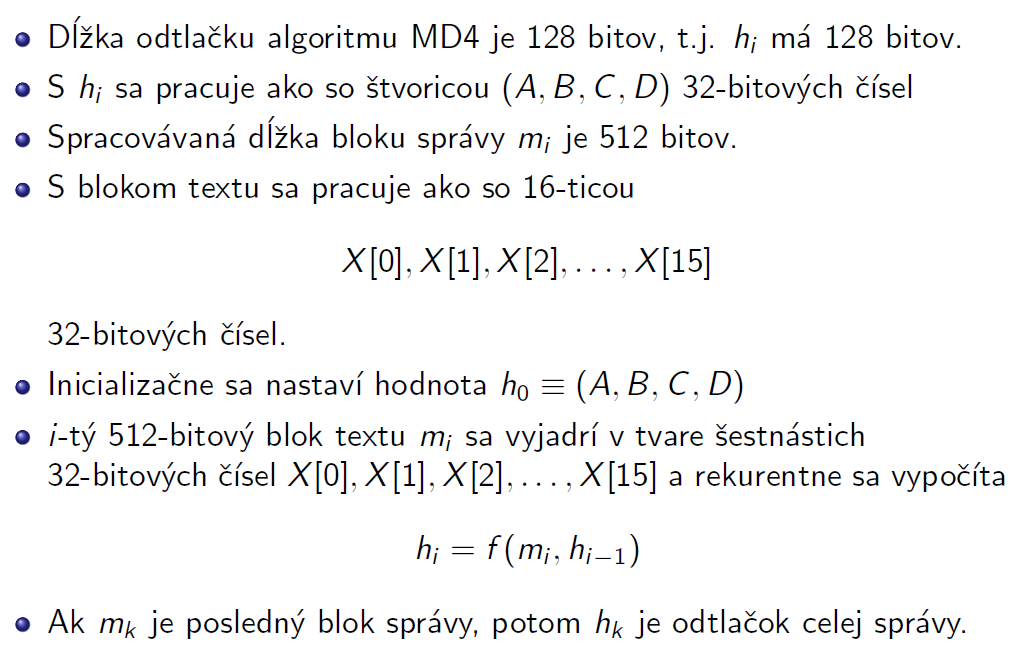
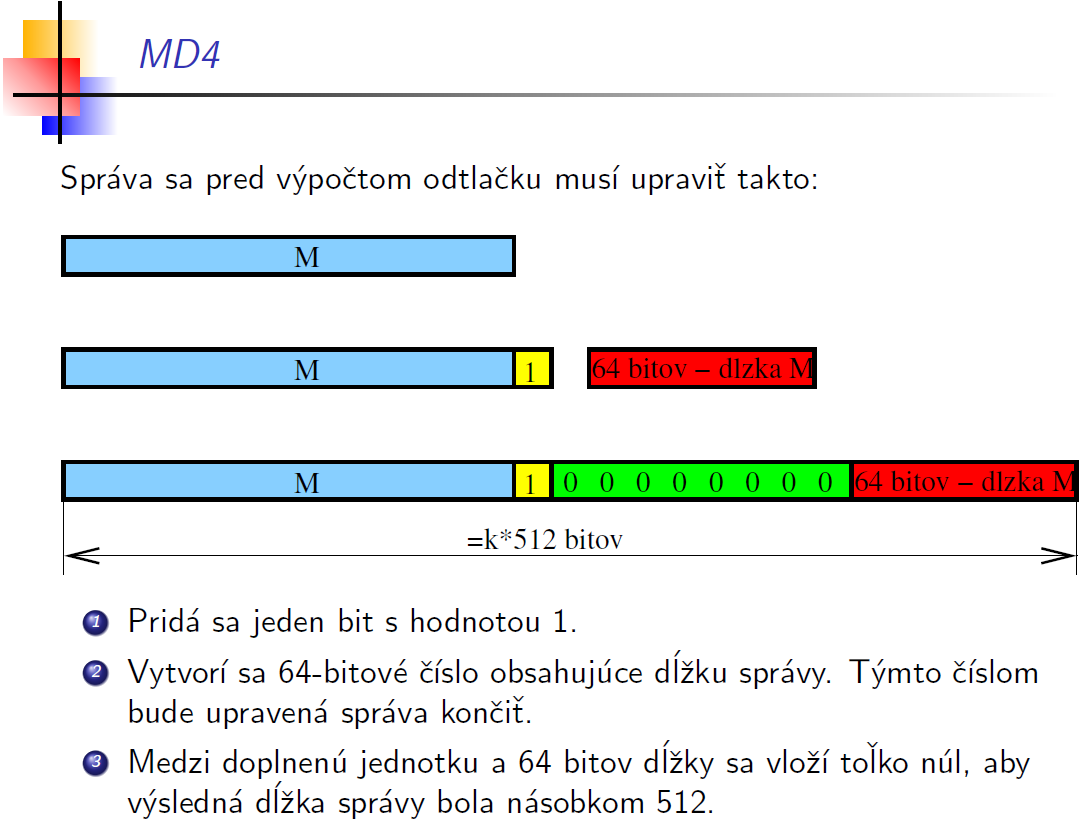


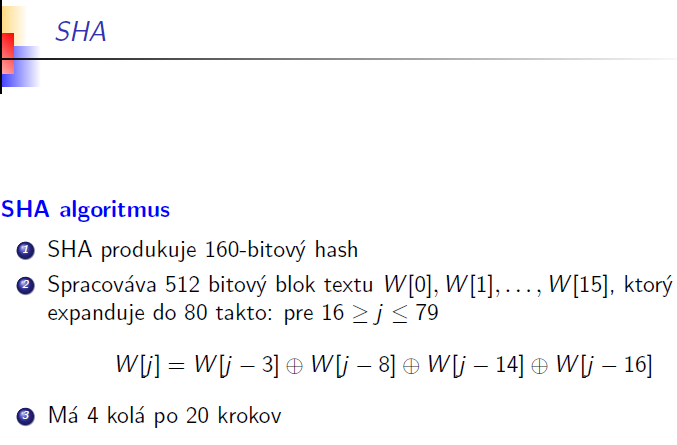




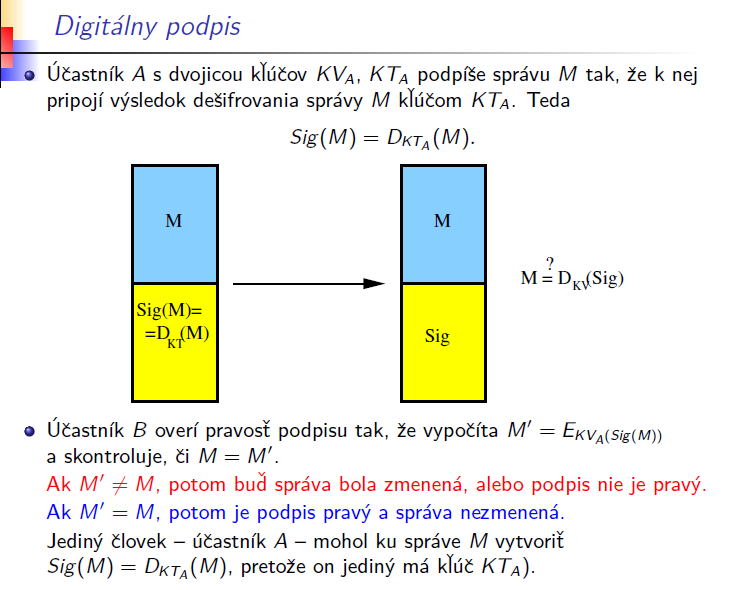
**dlzka odtlacku 3 kola**

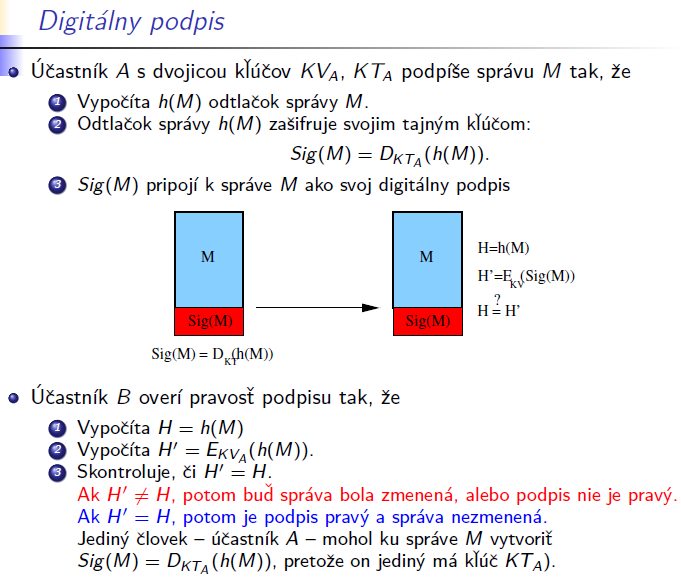


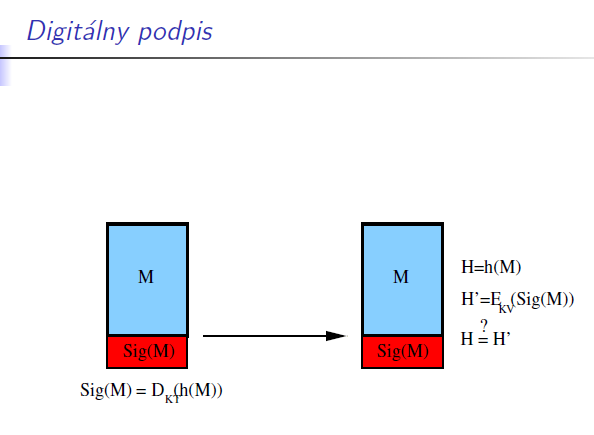
****



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

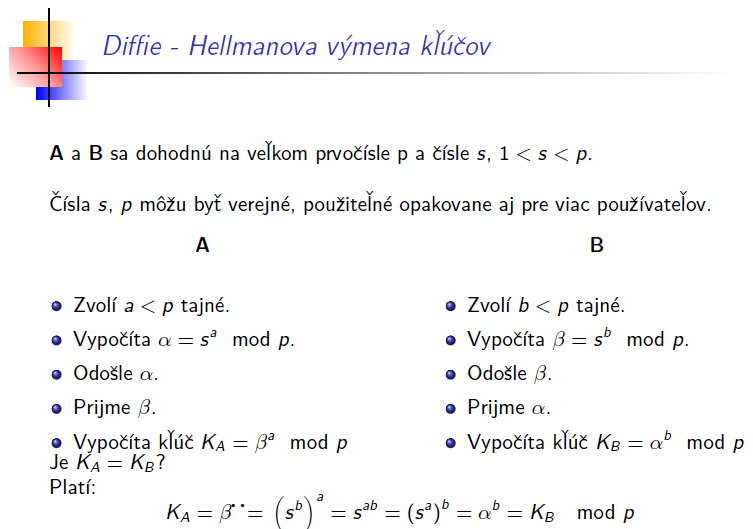


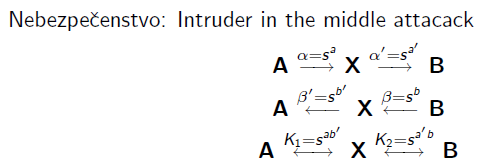






**Deffie – Hellmanova výmena kľúčov**

****

****

**14.AES**

- Symetrická bloková šifra

- 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

|  |  |  |  |
| --- | --- | --- | --- |
| Ɛ00 |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  | Ɛ33 |

Kolový kľúč

S týmto stavom sa iteračne vykonáva niekoľko kôl operácií, niektoré z nich závisia na kolovom kľúči reprezentovanom ako matica bajtov.  
  
AES je jediný verejne dostupný šifrovací algorytmus schválený NSA pre najtajnejšie informácie.

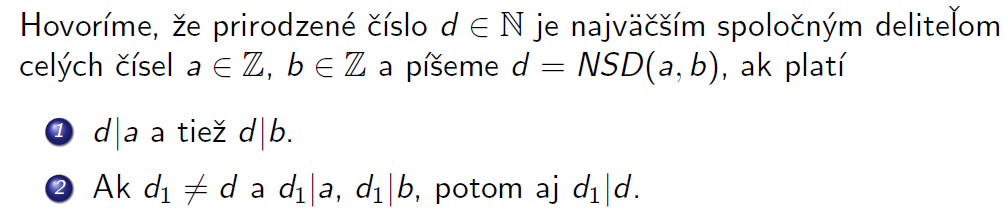
**15.Asymetricka kryptografia (vseobecne principy, RSA) - TODO**

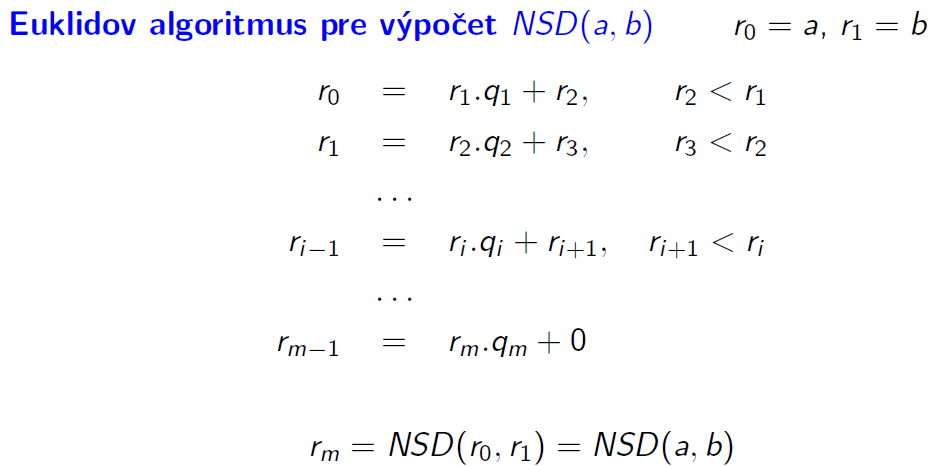
**Všeobecne:**

Základna 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 asymetrickej 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 účastnikovi 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 algorytmus:**

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)

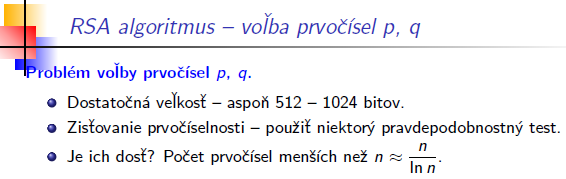
1. Verejný kľúč účastníka A je dvojica (e, n), jeho tajný kľúč je dvojica (d, n).
2. Účastník B bude správu x < n pre účastníka A šifrovať predpisom:

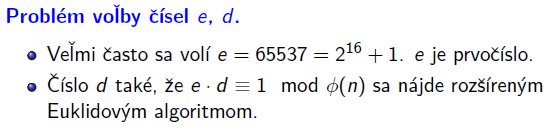
y = xe mod n

1. Účastník A dešifruje správu y predpisom:

x = yd mod n

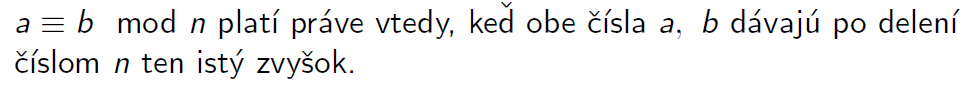
**Voľba prvočísel p,q v RSA:**

****

****

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:



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



