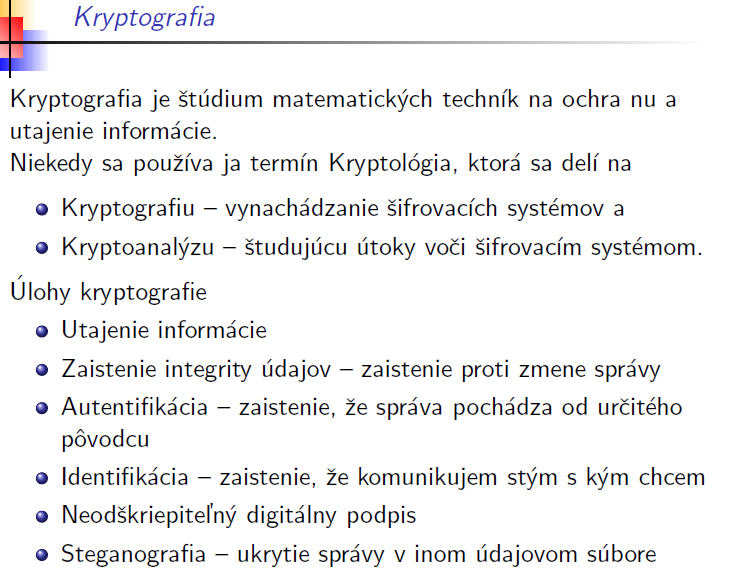
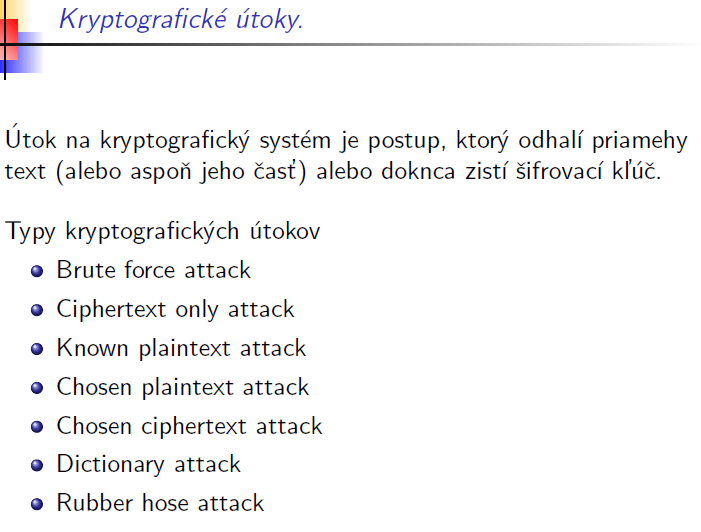
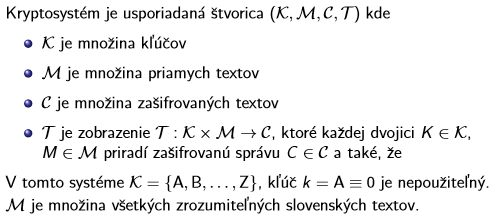
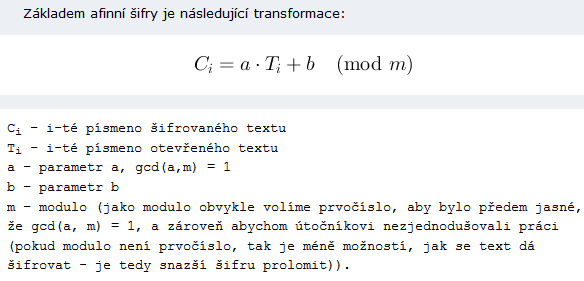
**1.**

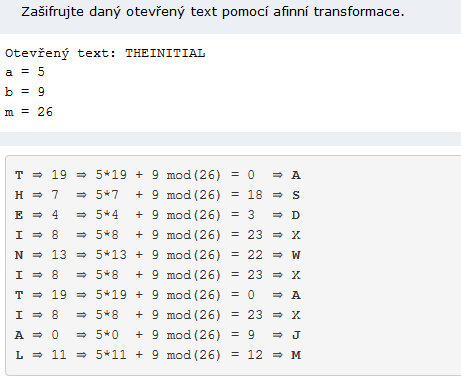


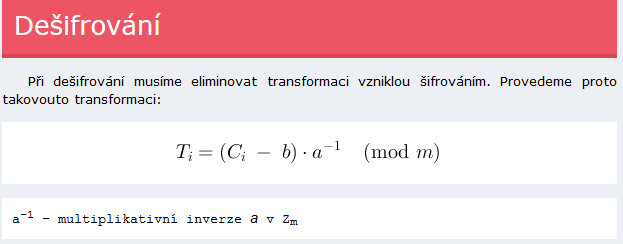


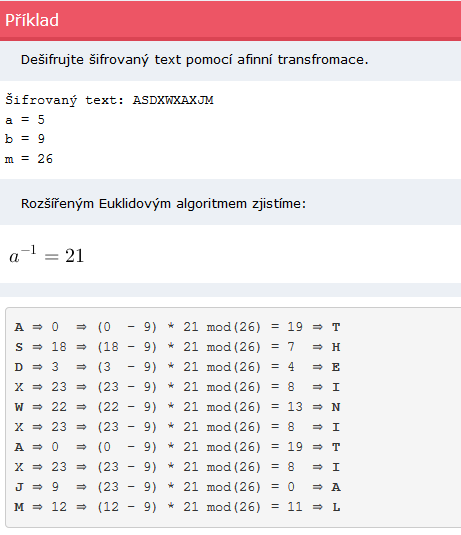


**2. Afinna sifra:**

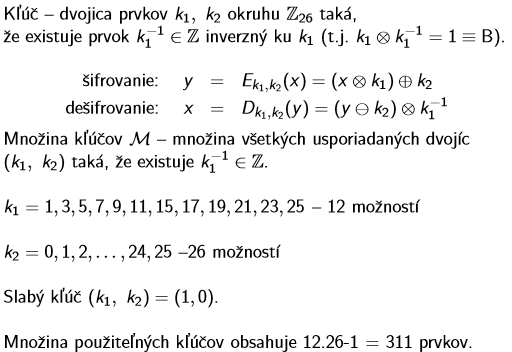


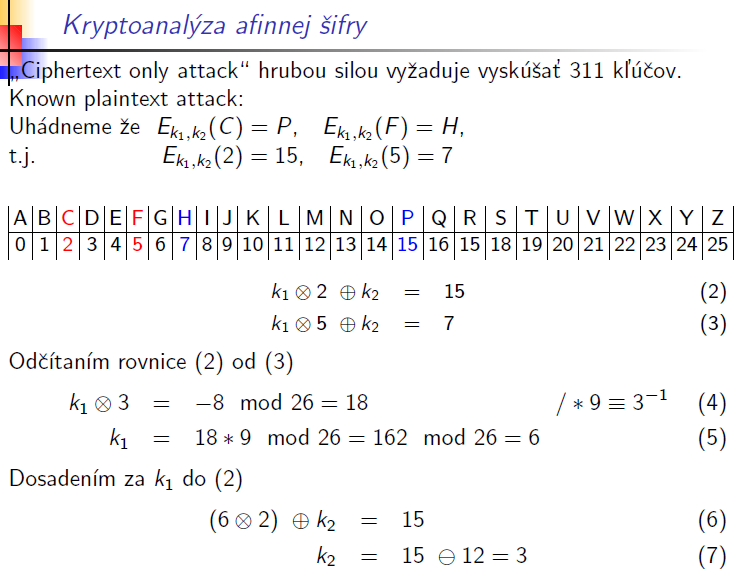




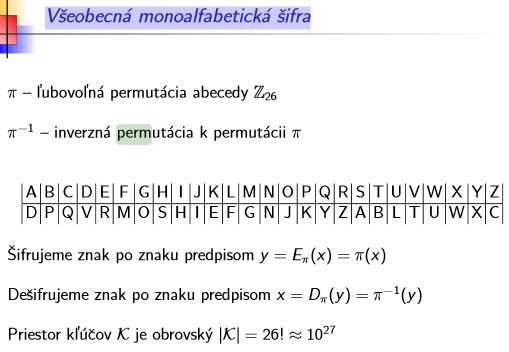


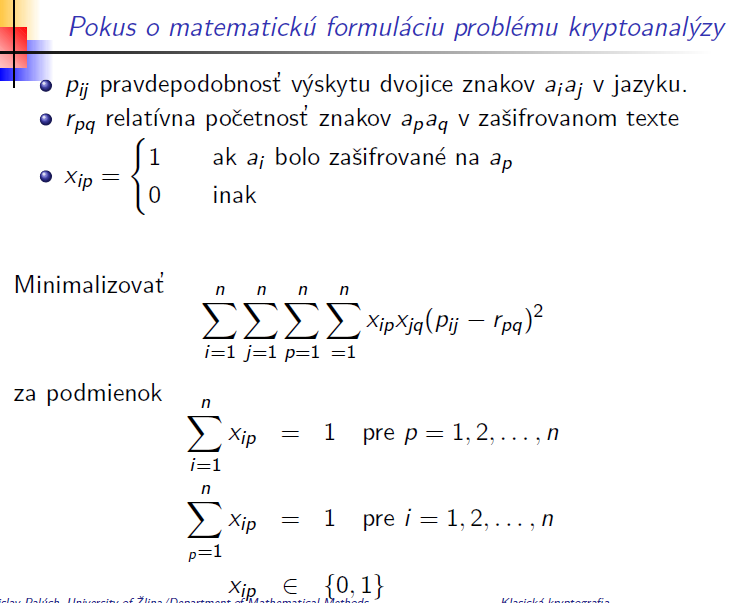


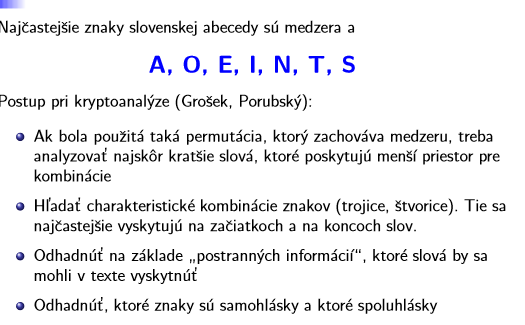


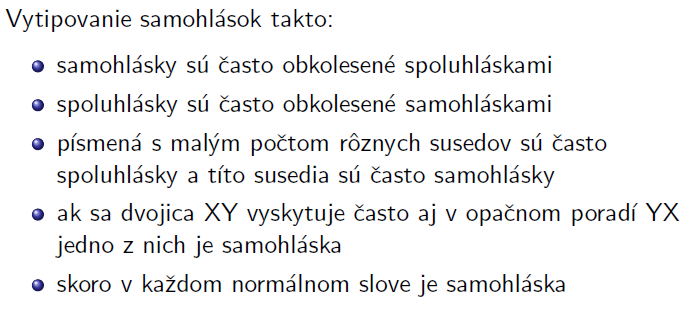


**3. Vseobecna monoalfabeticka sifra**

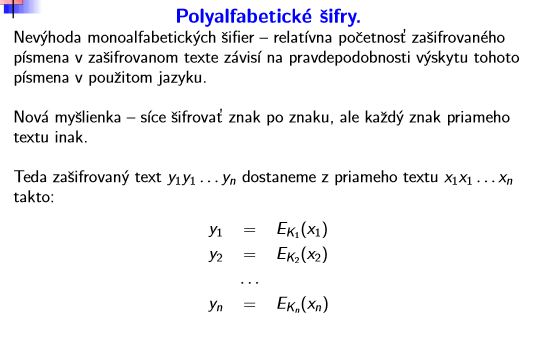


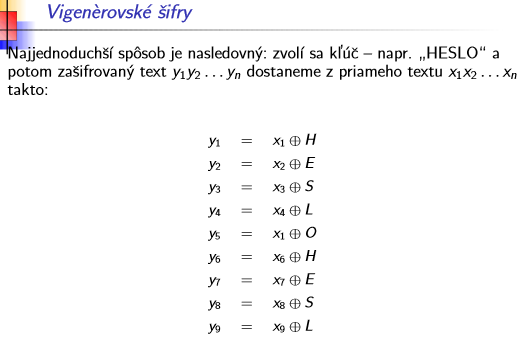


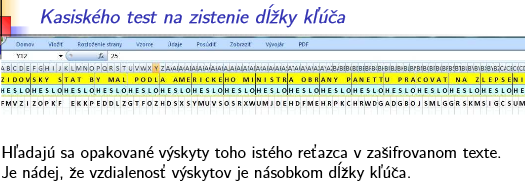




**4. Vigenerovska**

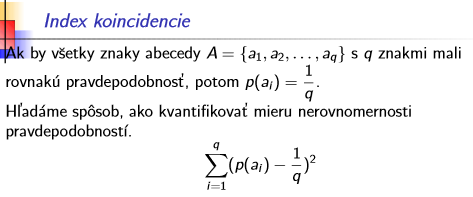


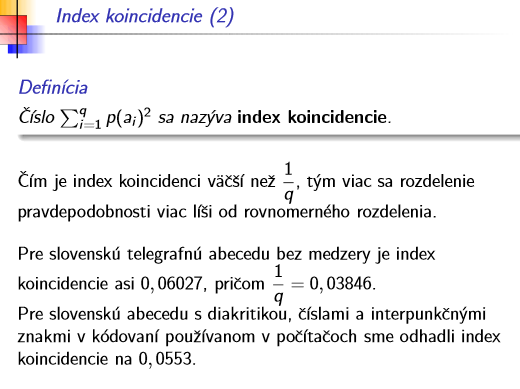


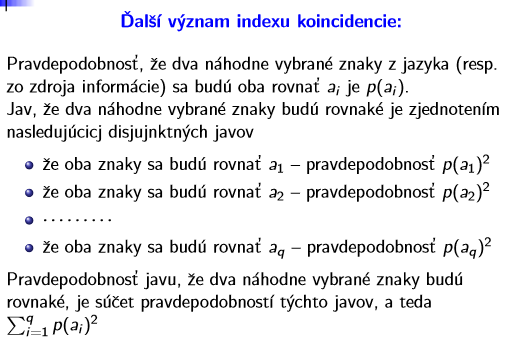


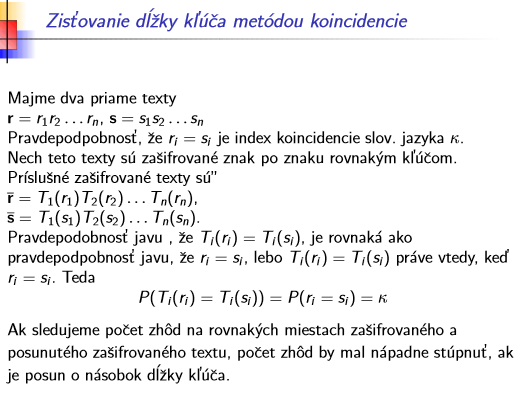


**5. Index koincidencie**

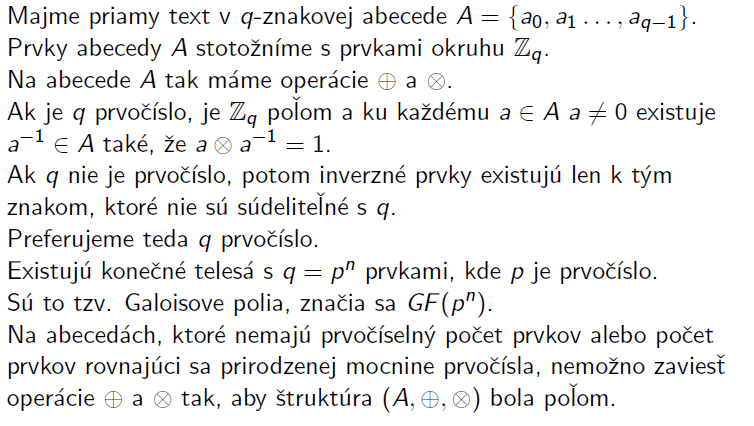


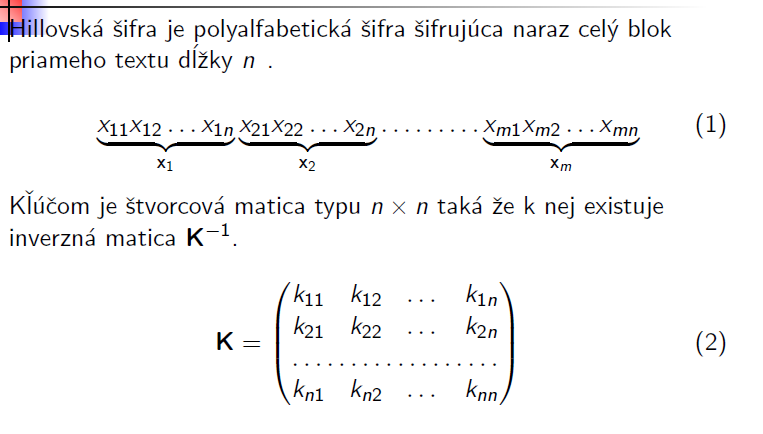


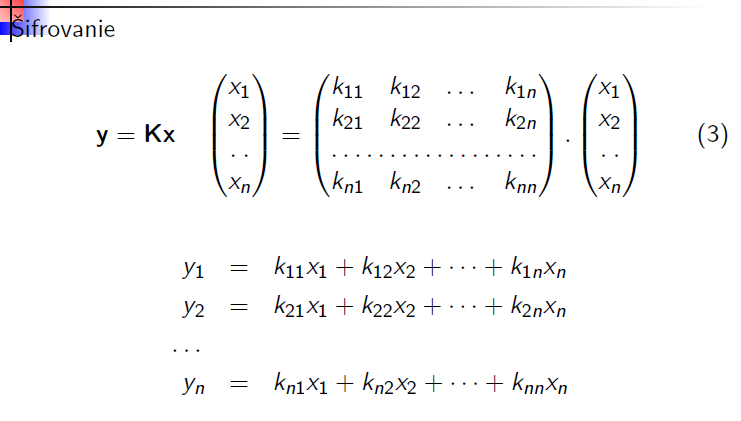


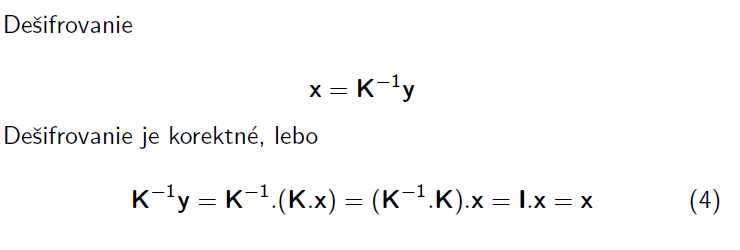


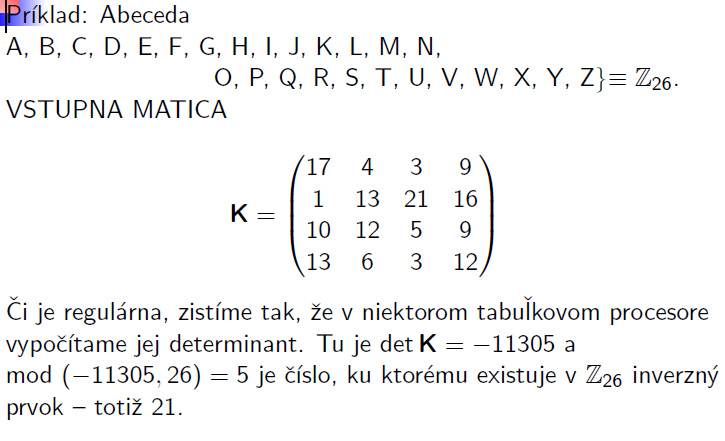
**6.Hillovska sifra**

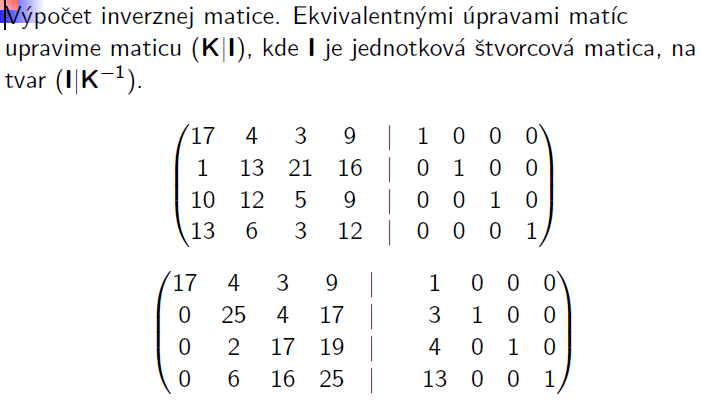


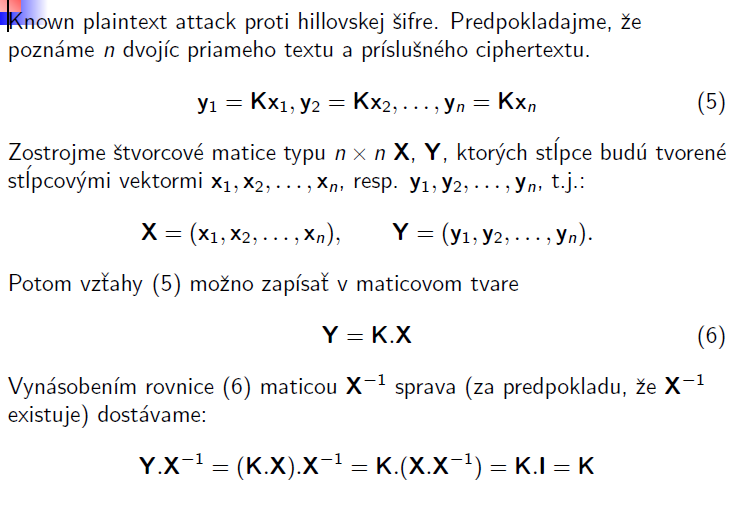




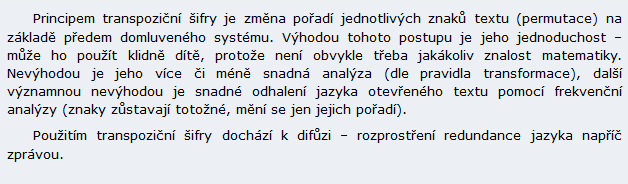


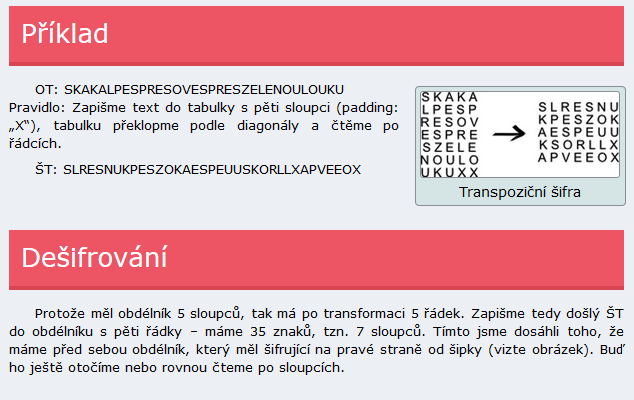


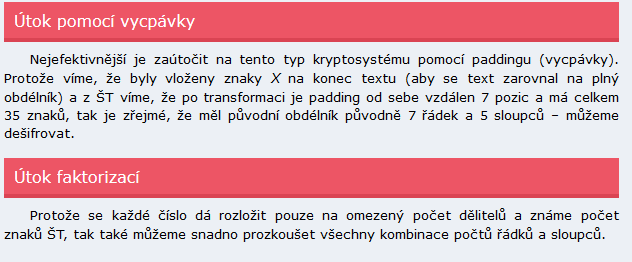




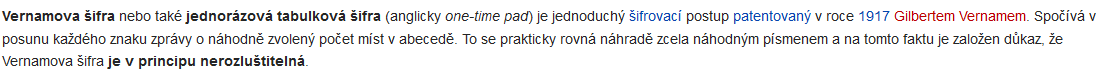
**7. Transpozicna – permutacna sifra**

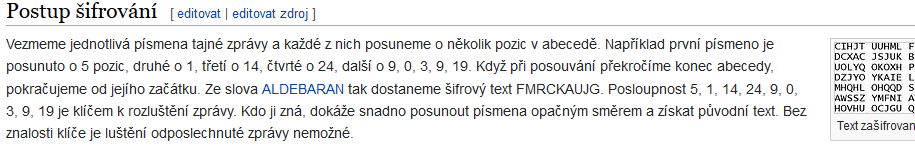


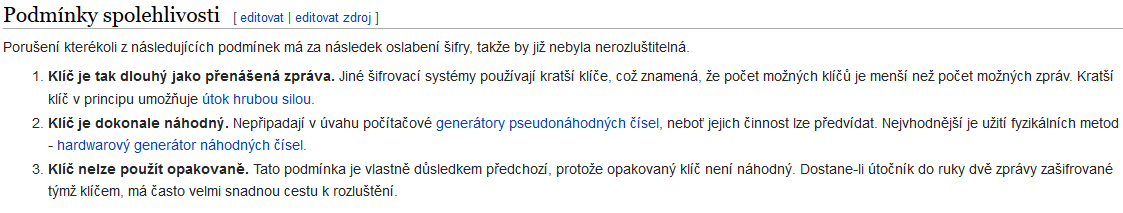


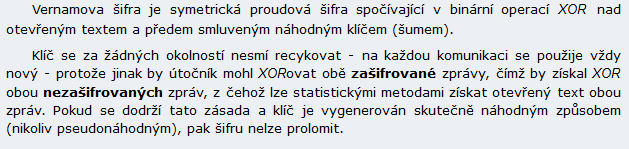


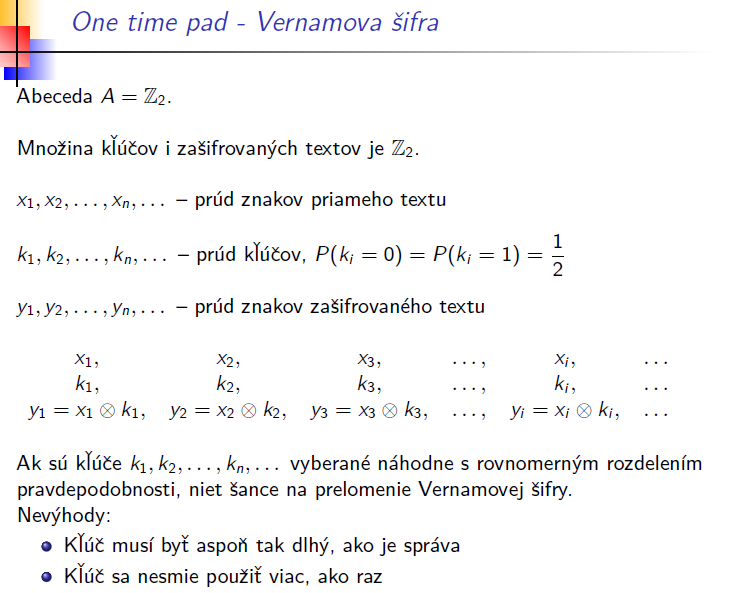
**8. One time Pad + utok**

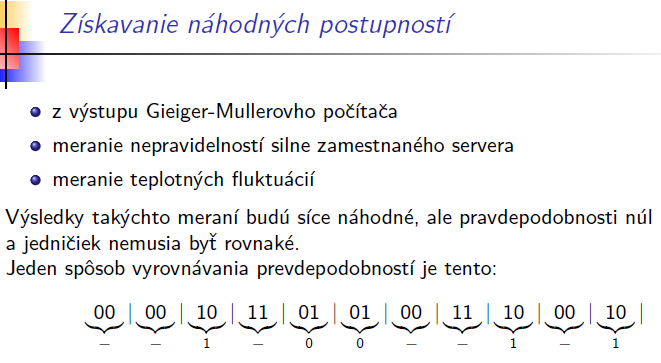




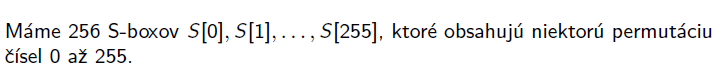


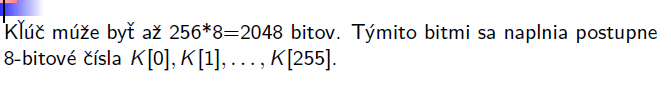


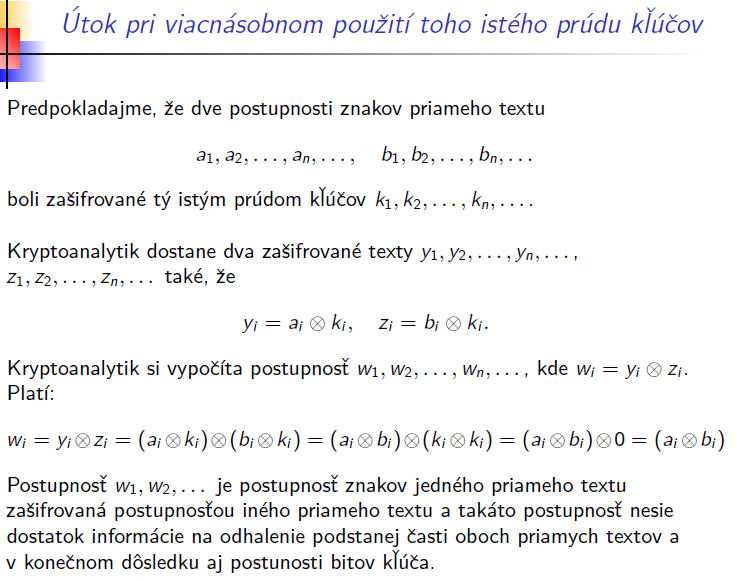


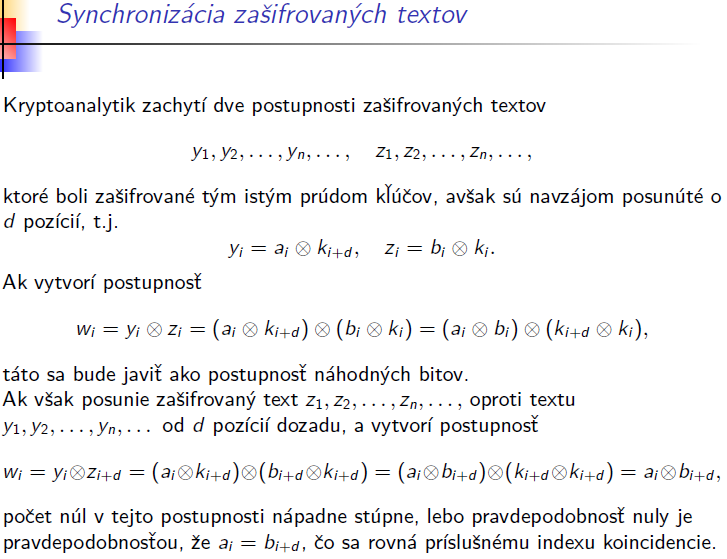


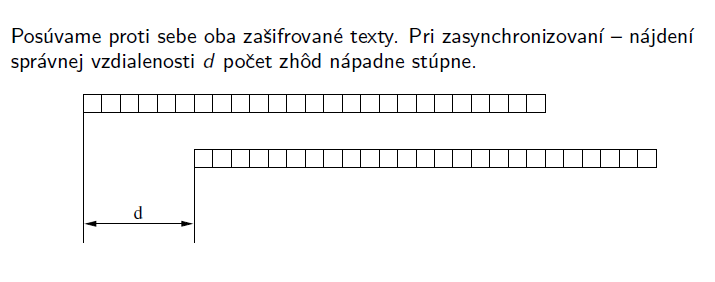






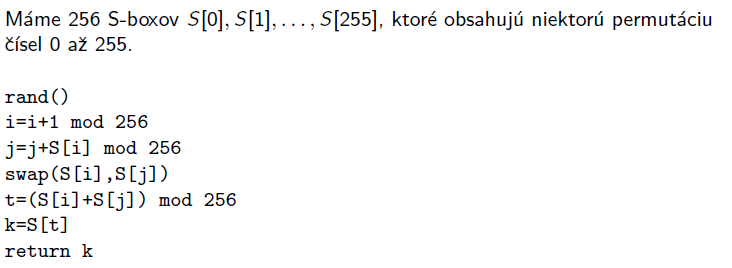


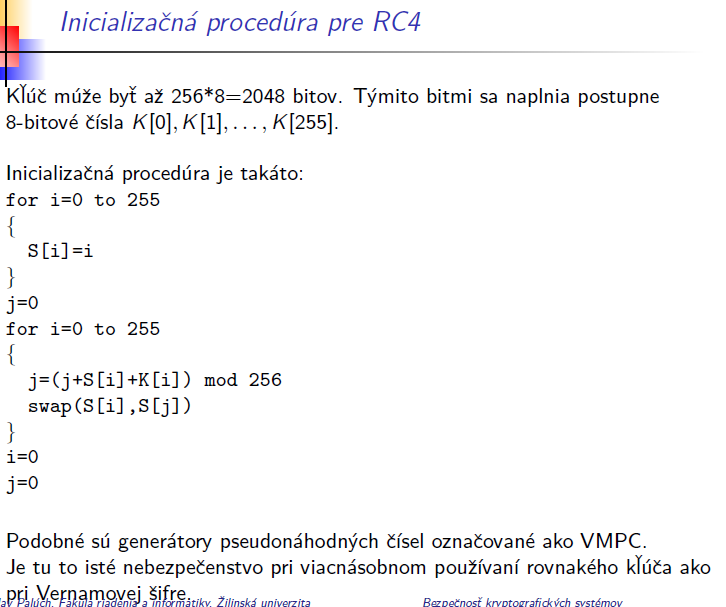




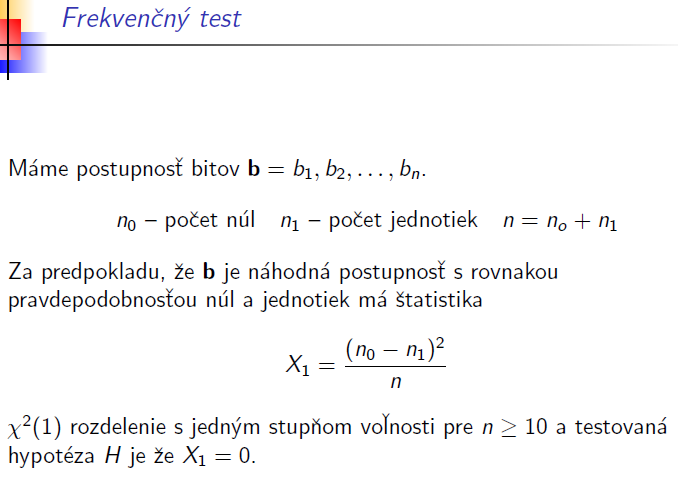
**9.Pseudogeneratory (linearny kongruencny, kvadraticky, kubicky, RC4)**

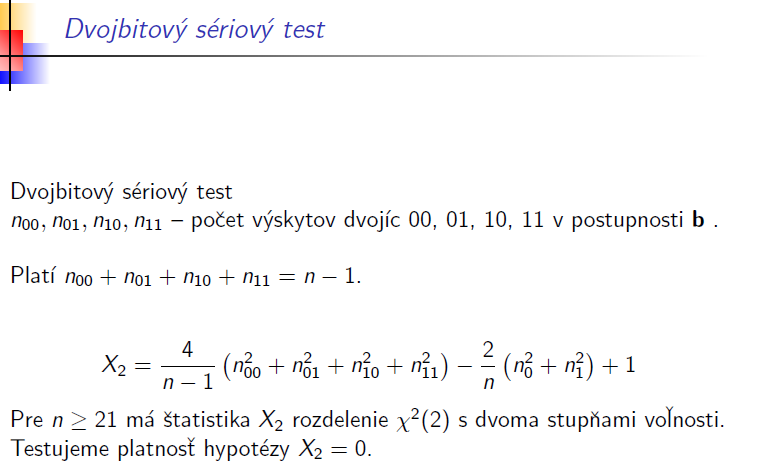




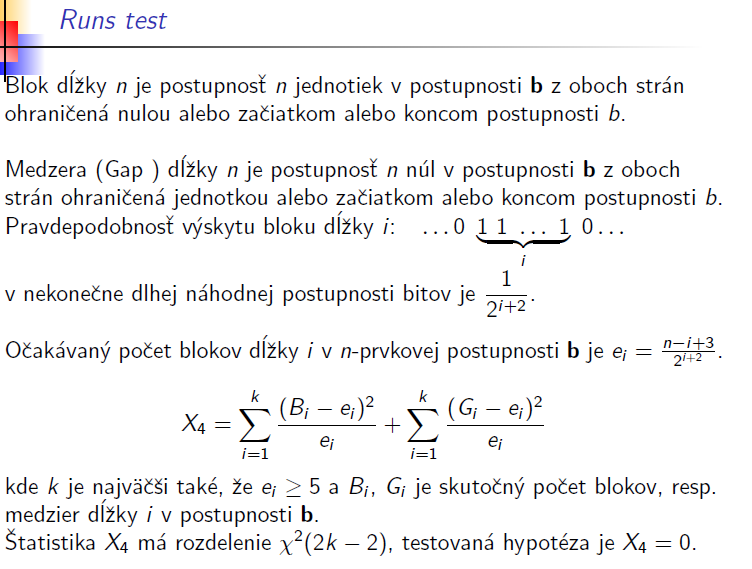


**10.Testy generatorov (frekvencny, TwoBits, Runs, Poker, FIPS 140-1, Autokorelacny)**

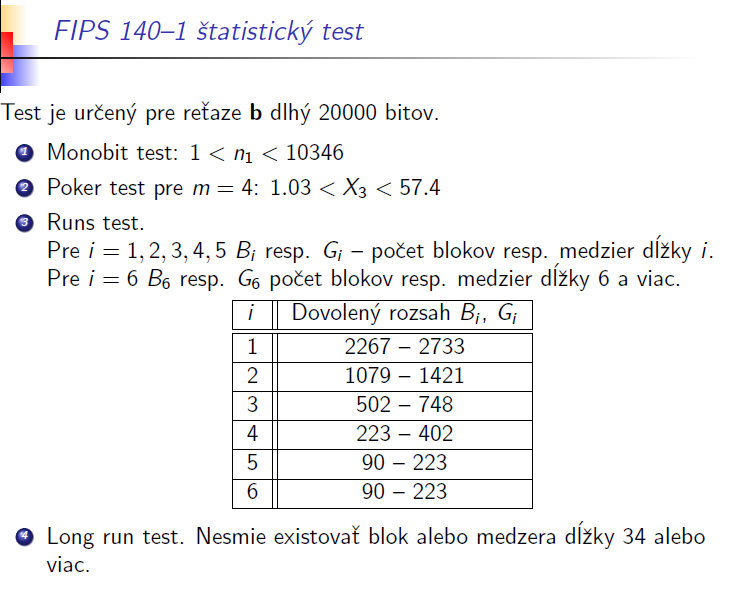




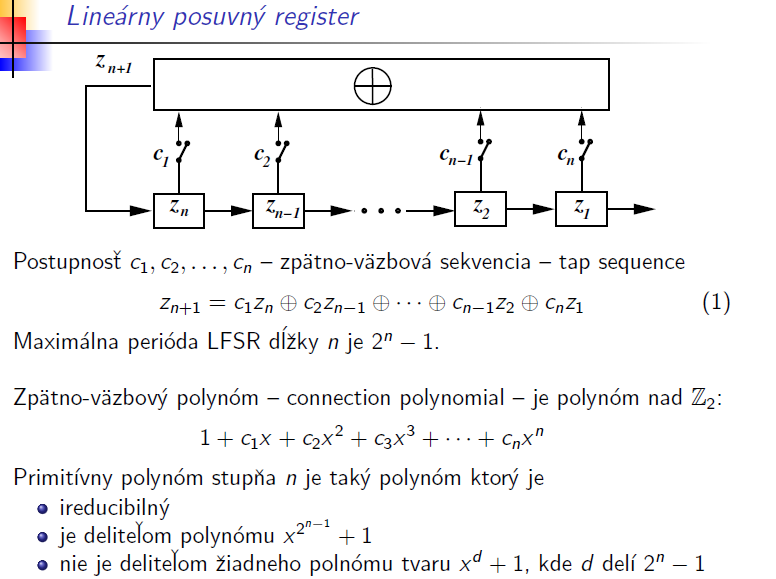


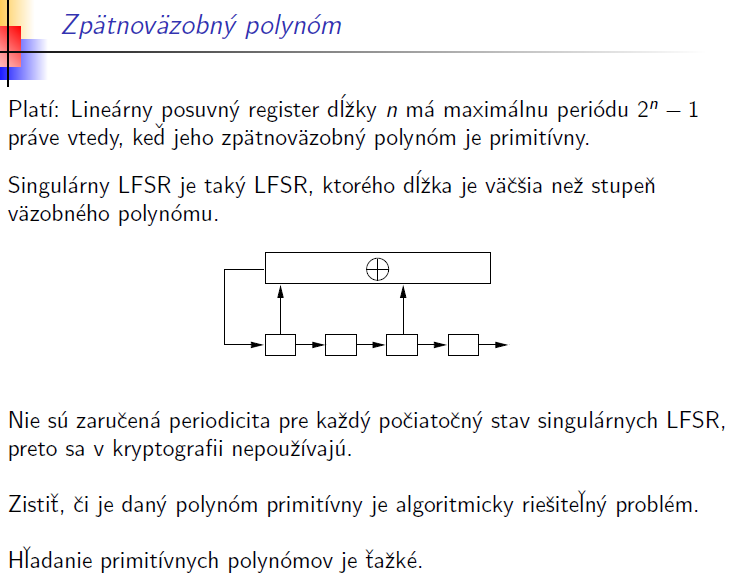




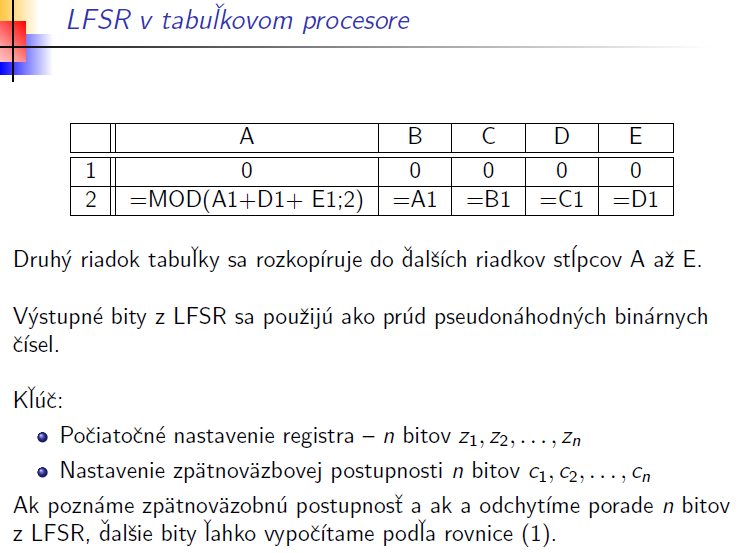


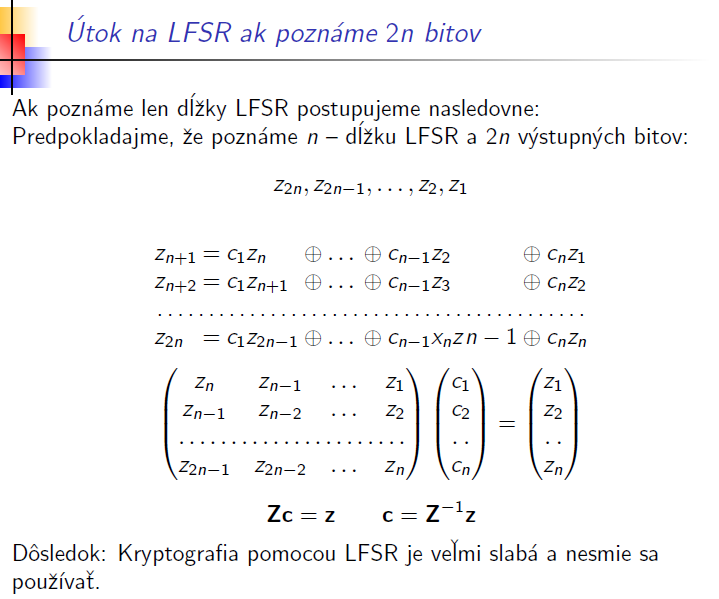
**11.LFSR**

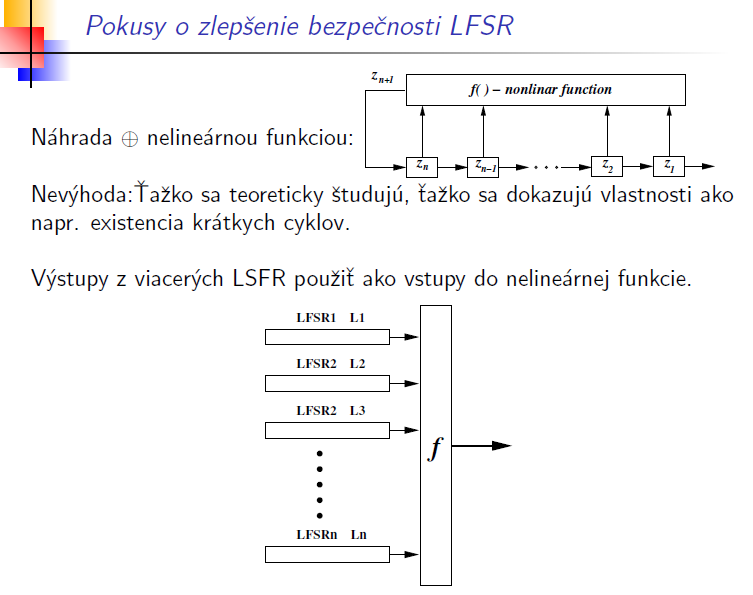




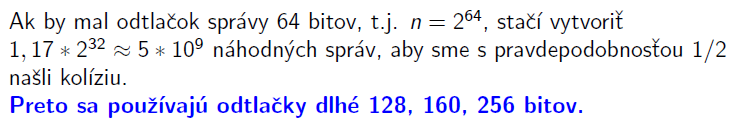


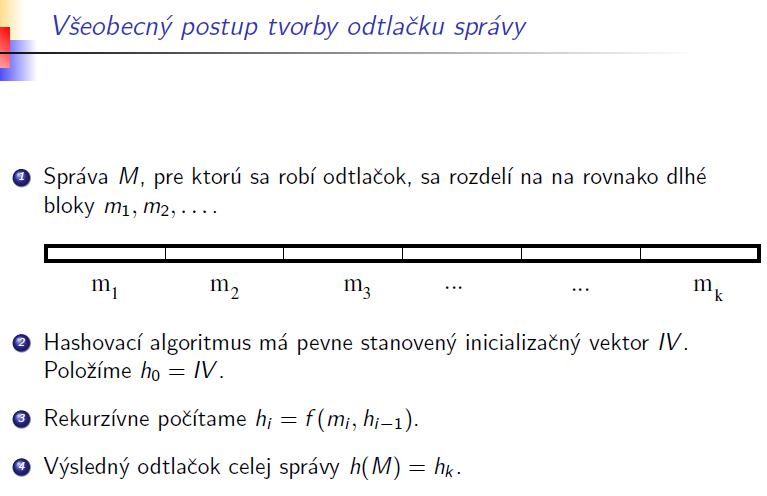






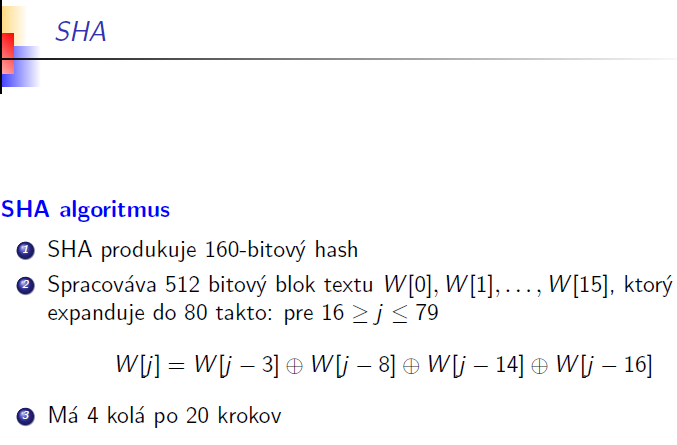
**12.Hash funkcie vseobecne, vlastnosti,(vseobecne, MD5, SHA) dorobit**



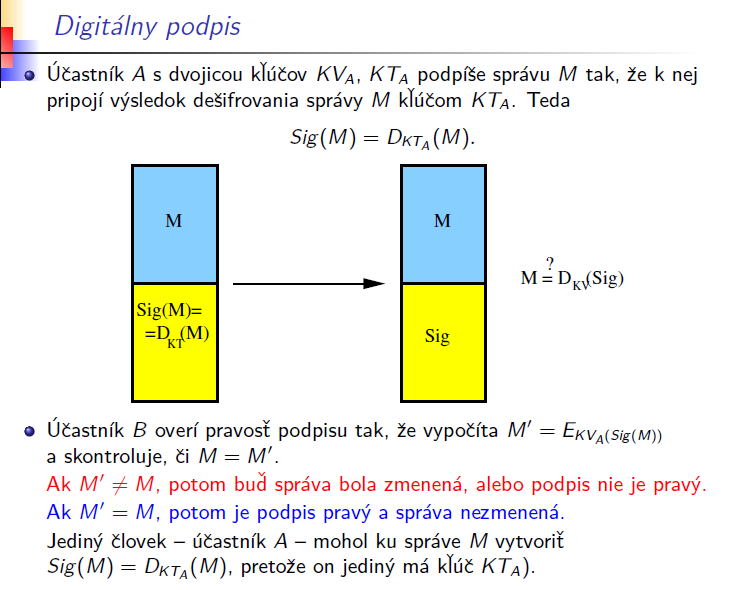


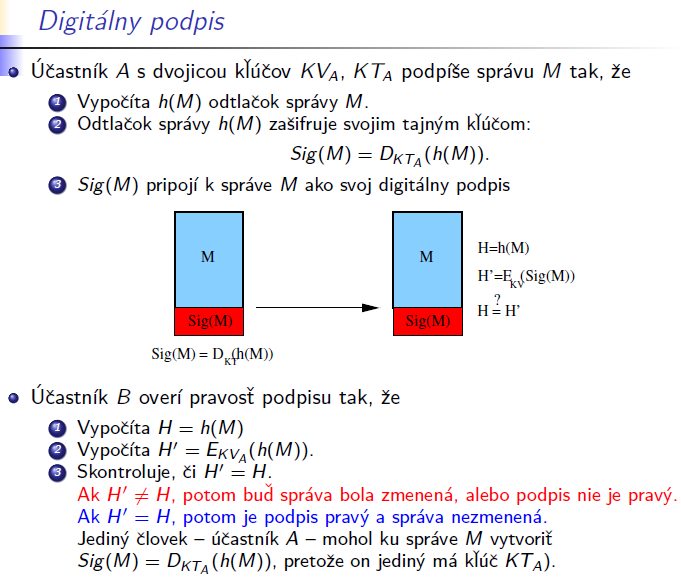
**dlzka odtlacku 3 kola**

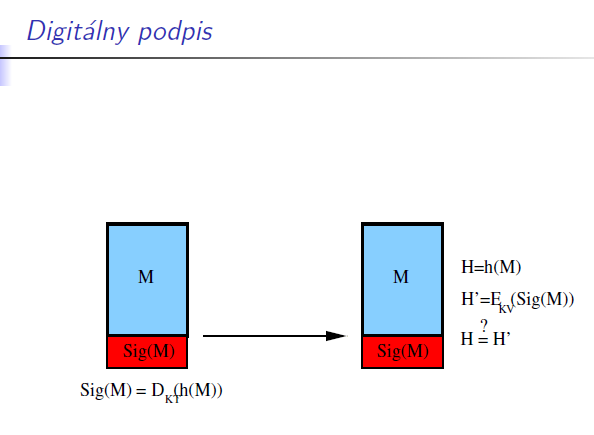




**13.Digitalny podpis - (plus Birdthday attack, zmenky)**









**14.AES**

**dorobit**

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

**dorobit**

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



