Rozdiel medzi kodovaním a šifrovaním

Pojem kódovanie označuje spôsob transformácie informácie pre potreby ich spracovávania prostredníctvom elektronických prostriedkov (napr. pre text sú to formáty súborov ako doc, rtf, pdf atď.).

Pojem šifrovanie označuje špeciálny spôsob transformácie informácie tak, aby ich opätovné sprístupnenie bolo možné po zadaní utajeného parametra (kľúča, hesla).

--- viem cele

-- skoro cele

- uff bieda

! neviem

1. Klasicku kryptografiu (Afinnu, Vigenerovsku, Index koincidencie, permutacne sifry, VMS)

2. One Time Pad sifru + utoky

3. Pseudogeneratory (linearny kongruencny, kvadraticky, kubicky, RC4)

4. LFSR a jeho modifikacie (geffeho, alternative step, shrinking)

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

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

7. Asymetricka kryptografia (vseobecne principy, RSA)

8. Hashovacie funkcie - (vseobecne, MD5, MD4, SHA, Ako vytvárame HASH)

9. Digitalny podpis - (plus Birdthday attack, zmenky)

10. Hillovsku sifru - nasobenie matic, utoky

11. AES

12. Deffie-Helmanova výmena kľúčov

- k vsetkym sifram sa zvykne pytat aj na UTOKY

urcite treba vediet vzdy dlzku bloku, dlzku kluca, pocet kol...