A test:

1) Ali je sprejeto sporocilo res enako oddanemu sporocilu?

2) Kaj je mešani postopek šifriranja in zakaj ga uporabljamo?

3) Kaj je znacilnost Feistelove šifre?

4) RSA šifriranje

5) Razložite DiffieHellman algoritem

6) Izvlecek pri algoritmu SHA-1 je dolg?

7) V cem je razlika med transportnim in tunelskim nacinom delovanja IPSec?

8) Za katere namene se uporablja šifrirni algoritem A3?

9) Kakšno je varno geslo?

10) ona 74. naloga za narisat :)

Kukr se jst spomnem je blo pr B izpitu tko:

1. Kako imenujemo vidik celovitosti: "Ali nam sporocilo res pošilja predstavljeni pošiljatelj?"?

2. Kakšne lastnosti mora imeti zgoščevalna funkcija?

3. Kakšne so osnovne znacilnosti DES algoritma?

4. RSA šifriranje/dešifriranje

5. Cemu služi postopek Diffie-Hellman?

6. Koliko je dolžina izvlecka pri MD4?

7. Za kaj se uporablja šifrirni algoritem A8?

8. Zakaj je potrebno zasebni kljuc skrbno varovati?

9. Kakšen je postopek pri izdelavi digitalnega podpisa?