Kompresija in kriptologija
izpit 18. maj 2006

1. Katere vidike celovitosti pri prenosu sporočila nam zagotavlja digitalni podpis ?

2. Kakšne verzije 3DES algoritma poznate ?

3. Kaj je značilnost Feistelove šifre ?

4. Skicirajte model, ki ponazarja princip delovanja iteracijske zgoščevalne funkcije na zaporedju blokov sporočila!

5. Na osnovi tajnih praštevil (p=13, q=31) izberemo ključ **e**=37. Izračunajte pripadajoči RSA ključ **d** !

6. Podana sta parametra (g=19, p=29) in tajna ključa uporabnikov ***tkA***=5, ***tkB***=11. Po DH algoritmu izračunajte skupni tajni ključ ***tkAB***!

7. Razvrstite protokole za varno komunikacijo po internetu po plasteh od najnižje k najvišji: SHTTP, IPSec, TSL.

8. Kakšna je razlika med S-HTTP je HTTPS ?

9. Kaj je glavna razlika med X.509 in PGP certifikati?

10. Kakšno šifriranje se uporablja v profesionalnem celičnem omrežju TETRA ?

11. Naštejte šifrirne algoritme, ki jih uporablja omrežje GSM!