Kompresija in kriptologija
izpit 17. junij 2005

1. Kako imenujemo vidik celovitosti pri prenosu sporočil, ki zagotavlja pritrdilen odgovor na vprašanje:

   Ali je vsebina sporočila res dostopna samo naslovniku ?

2. Razložite ElGamalov algoritem za digitalni podpis!

3. Na osnovi tajnih praštevil (p=11, q=7) izberemo ključ **e**=53. Izračunajte pripadajoči RSA ključ **d** !

4. Po algoritmu RSA z javnim ključem (n=527, e=53) šifrirajte čistopis m=54 !

5. Razložite DH algoritem izmenjave ključev !

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

7. V kateri razred spada zgoščevalna funkcija SHA-1 ?
   a) blokovne,
   b) z modularno aritmetiko,
   c) namenske

8. Povzetek pri algoritmu MD4 je dolg:
   a) 96 bitov
   b) 128 bitov
   c) 160 bitov
   d) 1024 bitov

9. Zakaj se uporablja LFSR? Navedite primer praktične uporabe!

10. Kolikokrat se ponovi jedrna funkcija DES algoritma?

Priimek in ime: _____