Kompresija in kriptologija
izpit 3. marec 2005

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

   Ali je pošiljatelj res oseba, ki se predstavlja ?

2. V čem je razlika med CA in RA ?

3. Naštejte osnovne značilnosti RIJNDAEL algoritma !

4. Po algoritmu RSA z javnim ključem (n=527, e=61) šifrirajte čistopis m=40 !

5. Razložite DH algoritem izmenjave ključev !

6. V kateri razred spada zgoščevalna funkcija DES-DaviesMeyer ?
   a) blokovne,
   b) z modularno aritmetiko,
   c) namenske

7. Povzetek pri algoritmu MD5 je dolg:
   a) 64 bitov
   b) 128 bitov
   c) 160 bitov
   d) 1024 bitov

8. Kaj je glavna razlika x.509 in PGP certifikatov?

9. Na kateri plasti deluje IPSec ?

10. Kaj je HTPPS ?

Priimek in ime: _____