***Biletul nr …***

1. Care din entităţile criptografice de mai jos leagă « Subject-name» - ul unui certificat de valoarea unei chei publice:

a. Un certificat de cheie publică

b. O infrastructură cu chei publice

c. O autoritate de certificare.

d. O cheie privată.

2. De ce mesajele din PGP sunt compresate înainte de a fi criptate?

3. Protocolul ESP din cadrul IPSec asigură aceleaşi servicii de securitate ca şi AH, dar în două moduri (în loc de unul singur) (Adevărat/Fals)

4. In general în TLS algoritmii cu cheie publică sunt folosiţi pentru criptarea datelor, iar algoritmii simetrici pentru schimbul de chei (Adevărat/Fals).

5. Compatibilitatea între piaţa smartcardurilor şi cea a telefoniei mobile este asigurată în principal prin \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

6. Cheia secretă Ki de pe un echipament mobil GSM este folosită pentru:

a. Criptarea mesajelor

b. Autentificare

c. Ambele variante de mai sus.