Lucrarea de laborator nr. 4

1. Următorul text este scris in limba româna, numai cu liere mari, fără diacritice, fără spaţii între cuvinte şi fără punctuaţie, după care a fost cifrat prin substituţie monoalfabetică (fiecare literă este substituită cu altă literă din alfabet, corespondenţa fiind aceeaşi la fiecare apariţie):

   ```
   VIDYGGDJGODEHTYGPDVNVKYKPXTGVYUVPQDPXXKT
   KXIXFPKODGXUYKZYGXGKGXDEHTHVSFVZDGXIV
   ```

   Se cere să se descifreze textul.

2. Descărcaţi de pe pagina proiectului Putty cheia publică a proiectului, şi unul din programe împreună cu fişierul semnătură. Verificaţi semnătura (folosiţi comanda `gpg` din linux).

3. La punctul precedent, presupuneţi cheia publică descărcată ca fiind corectă, dar presupuneţi că fişierul conţinând programul *putty* şi fişierul conţinând semnătura au fost descărcate de pe un site mirror suspect. E posibil ca programul descărcat să nu fie cel creat de autorul *putty*? Justificaţi.

4. Folosind gpg (Gnu Privacy Guard), generaţi-vă o pereche de chei pentru semnături digitale şi o pereche de chei pentru cifrare. Cereţi unui coleg cheile lui publice şi daţi-i cheile voastre.

   Trimiteţi apoi colegului un mesaj cifrat cu cheia lui publică şi semnat cu cheia voastră secretă, şi cereţi-i să procedeze la fel. Descifraţi şi verificaţi semnătura mesajului primit.

5. Configuraţi, pentru conectarea folosind *putty* la `linux.scs.ubbcluj.ro`, un sistem de autentificare cu cheie publică. Cifraţi cu parolă cheia privată şi utilizţi *pageant* pentru a ţine cheia publică în clar pe durata unei sesiuni.

6. La semnarea documentelor electronice folosind criptografie asimetrică, valoarea funcţiei de dispersie aplicată documentului se trece prin funcţia de descifrare. De ce nu se poate folosi în loc funcţia de cifrare?

7. Dacă A şi B nu au un canal sigur pentru a-şi transmite o cheie, pot totuşi să-şi stabilească un canal de comunicaţie confidenţial fie folosind criptografie asimetrică, fie stabilindu-şi o cheie de cifrare prin protocolul

Diffie-Hellman. Arătaţi cum un intrus activ T poate să comunice cu A dându-se drept B şi cu B dându-se drept A, putând obţine efectiv interceptarea canalului dintre A şi B (atacul se numeşte men-in-the-middle, omul-din-mijloc). De asemenea, justificaţi de ce o apărare impotriva acestui atac nu este posibilă.

8. Pe baza punctului anterior, explicaţi mesajul de avertizare dat de orice program client *ssh* la prima conectare la un server. Explicaţi de ce, dacă la prima conectare clientul s-a conectat la serverul adevărat, la cea de-a doua conectare nu mai este nici un pericol.

9. Scrieţi un program care calculează şi afişează în hexa dispersia MD5 a unui fişier. Folositî de exemplu biblioteca *openssl*. Comparaţi rezultatul programului vostru cu ieşirea comenzii `md5sum` (din linux).