Mod de notare: 1 punct fiecare problemă.
Total: 7 puncte (6 + 1 punct bonus). Pentru promovare este necesar un punctaj de minim 3 puncte. Se acordă punctaje parţiale.

Nume: ______________________ Grupă: __________

1. Considerăm o parolă de 10 caractere ASCII (fiecare reprezentat pe câte 8 biţi). Pentru simplitate considerăm, în mod ipotetic, că toate caracterele ASCII sunt caractere posibile.
   (a) Câte astfel de parole distincte există?
   (b) Care este dimensiunea în biţi a parolei?
   (c) Se utilizează reprezentarea binară a parolei drept cheie de criptare AES-192. Câte caractere trebuie să aibă în acest caz parola?

Solution: (a) $(2^8)^{10} = 2^{80}$; (b) 80 biţi ; (c) $192/8 = 24$ caractere

2. Se consideră $(Enc_k(m), Dec_k(m))$ un sistem de criptare bloc. Se criptează o secvenţă de blocuri $m_1||m_2||m_3||\dots$ într-o secvenţă de blocuri $c_1||c_2||c_3||\dots$ astfel:

$$c_i = m_{i-1} \oplus 00\dots0 \oplus Enc_k(m_i \oplus c_{i-1}), i \geq 1$$

   unde m_0 şi c_0 sunt vectori de iniţializare publici şi fixaţi.
   (a) Indicaţi cum se realizează decriptarea.
   (b) Presupunând că un bloc c_i suferă erori de transmisie, care blocuri de text clar sunt impactate?

Solution: (a) $m_i = c_{i-1} \oplus Dec_k(m_{i-1} \oplus c_i)$
(b) c_i eronat rezultă m_i eronat rezultă m_{i+1} eronat, deci toate blocurile m_j, $j \geq i$ sunt eronate.

3. Fie $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ o PRF. Se defineşte un sistem de criptare (Enc, Dec) cu funcţia de criptare $Enc_k(m) = r||(F_k(m) \oplus r)$, unde r este o valoare aleatoare pe n biţi. Arătaţi că sistemul nu este CCA-sigur.

Solution:

Challenge: $m_0 = 0^n$; $m_1 = 1^n$. Răspuns: $r||F_k(m_b) \oplus r$. $\mathcal{A}$ determină r ca primii n biţi, apoi calculează $F_k(m_b)$. $\mathcal{A}$ transmite oracolului de decriptare $r_1||F_k(m_b) \oplus r_1$, cu r_1 aleator pe n biţi şi primeşte m'. $m' = m_0$ sau $m' = m_1$, deci $\mathcal{A}$ determină b cu probabilitate 1.

4. Se consideră $Enc_k(m)$ un sistem de criptare bloc sigur. Se defineşte o funcţie hash H astfel:

   i. m se concatenează cu 0-uri până la un multiplu de lungimea blocului;

   ii. Se sparge secvenţa obţinută anterior în n blocuri, i.e. $m_0||m_1||...||m_{n-1}$;

   iii. Se aplică:

```
c ← Enc_{m0}(m0)
for i = 1 to n-1 do
    d ← Enc_{m0}(mi)
    c ← c ⊕ d
end for
H(m) ← c
```

   Este H rezistentă la coliziuni? Argumentaţi.

Solution: Nu este rezistentă la coliziuni - ex. $H(m_0||m_1||m_2) = H(m_0||m_2||m_1)$ sau $H(m_0) = H(m_0||m_1||m_1)$.

5. Fie (Mac, Vrfy) un MAC sigur definit peste (K,M,T) unde $M = \{0,1\}^n$ şi $T = \{0,1\}^{128}$. Este MAC-ul de mai jos sigur? Argumentaţi răspunsul.

$$Mac'(k, m) = (Mac(k, m), Mac(k, 0^n))$$
$$Vrfy'(k, m, (t_1, t_2)) = [Vrfy(k, m, t_1) \text{ and } Vrfy(k, 0^n, t_2)]$$

Solution:

MAC-ul nu este sigur pentru ca un adversar poate cere un tag pentru $m = 1^n$, obţine $Mac(k, 0^n)$ şi deci $(Mac(k, 0^n), Mac(k, 0^n))$ un tag valid pentru $m = 0^n$;

6. Alice vrea să comunice cu Bob folosind următoarea schemă în care:

   - G este un grup de ordin prim p şi g un generator al lui G.

- Alice alege x, y aleatoare în $\mathbb{Z}_p$ şi un număr $a \in \mathbb{Z}_p$ şi îi trimite lui Bob $(A_0, A_1, A_2) = (g^x, g^y, g^{xy+a})$.
- Bob alege r, s aleatoare în $\mathbb{Z}_p$ şi un număr $b \in \mathbb{Z}_p$ şi îi trimite inapoi lui Alice $(B_1, B_2) = (A_1^r g^s, (A_2/g^b)^r A_0^s)$.

Arătaţi cum poate Alice verifica dacă $a = b$ în urma execuţiei schemei de mai sus.

Solution:

Avem că $B_1 = g^{yr+s}$ şi $B_2 = (g^x)^{yr+s} g^{r(a-b)}$. Alice testează dacă $a = b$ verificând dacă $B_2/B_1^x = 1$.

7. Se consideră o schemă de criptare cu cheie publică (Enc, Dec), pk_A şi pk_B cheile publice corespunzătoare lui Alice, respectiv Bob, N_A şi N_B două numere aleatoare unice (nonce) generate de Alice, respectiv Bob. Pentru a se autentifica reciproc, Alice si Bob folosesc următorul protocol:

   a) Alice alege N_A şi îi trimite lui Bob mesajul $Enc_{pk_B}(N_A, "Alice")$;
   b) Bob alege N_B şi îi trimite lui Alice mesajul $Enc_{pk_A}(N_A, N_B)$;
   c) Alice confirmă primirea lui N_B trimiţând lui Bob $Enc_{pk_B}(N_B)$;

   Cerinţe:

   (a) Care dintre valorile N_A, N_B sunt cunoscute de Alice la finalul protocolului? Dar de către Bob?
   (b) Arătaţi că protocolul este vulnerabil la un atac de tip "Man-in-the-middle".

Solution:

(a) Alice şi Bob ştiu amândoi N_A şi N_B

(b) Oscar procedeaza astfel pentru un atac MITM:

a) Alice alege N_A si ii trimite lui Oscar mesajul $Enc_{pk_I}(N_A, "Alice")$;

b) Oscar trimite mesajul lui Bob $Enc_{pk_B}(N_A, "Alice")$;

c) Bob alege N_B si trimite Alice mesajul $Enc_{pk_A}(N_A, N_B)$;

d) Oscar preia mesajul si il transmite neschimbat lui Alice $Enc_{pk_A}(N_A, N_B)$;

e) Alice decripteaza mesajul, afla N_B si ii trimite confirmarea lui Oscar $Enc_{pk_I}(N_B)$.

f) Oscar afla N_B, recripteaza si ii trimite lui Bob mesajul $Enc_{pk_B}(N_B)$.