Securitate perfectă. Sistemul de criptare OTP (One Time Pad)

1. Se consideră sistemul de criptare OTP.
   (a) Demonstraţi că sistemul este corect (i.e. decriptarea unui mesaj criptat cu cheia corectă conduce la determinarea mesajului clar iniţial).
   (b) De ce se foloseşte XOR? Putem folosi un alt operator (AND, OR, NOT)?

2. Sistemul de criptare OTP pare nesigur dacă $k = 0^l$, unde l este lungimea textului clar pentru că $c = m \oplus k = m$, deci mesajul este trimis în clar. Considerăm îmbunătăţirea OTP care nu permite folosirea cheii 0^l (*zero-peste-tot*). Mai este OTP perfect sigur?

3. Ce cantitate de date se poate cripta cu OTP folosind o cheie de 1Gb dacă se doreşte păstrarea securităţii perfecte?

4. Analizaţi securitatea sistemului de criptare OTP în următoarele scenarii:
   (a) utilizarea multiplă a cheii când se cunoaşte o pereche (m, c) (text clar, text criptat);
   (b) maleabilitatea mesajului criptat (i.e. plecând de la un mesaj criptat dat, se poate construi un alt mesaj criptat a.î. să existe o relaţie predefinită între mesajele clare corespunzătoare?)

5. Adevărat sau Fals? Pentru orice sistem de criptare perfect sigur se satisface următoarea afirmaţie: *Pentru orice distribuţie peste spaţiul mesajelor $\mathcal{M}$ şi orice 2 mesaje clare m_1, m_2 din $\mathcal{M}$ şi orice mesaj criptat c din $\mathcal{C}$ are loc*

$$Pr[M = m_1 | C = c] = Pr[M = m_2 | C = c]$$

   Argumentaţi.

6. Adevărat sau Fals? Orice sistem de criptare pentru care lungimea cheii este egală cu lungimea mesajului clar şi pentru care cheia este uniform aleasă din spaţiul cheilor este perfect sigur. Argumentaţi.

Funcţii neglijabile

7. Care dintre următoarele funcţii sunt neglijabile în n?
   (a) $f(n) = \dfrac{1}{n^{100}}$
   (b) $f(n) = \dfrac{1}{3^n}$
   (c) $f(n) = \begin{cases} \dfrac{1}{n^{100}} & n \text{ par} \\ \dfrac{1}{3^n} & n \text{ impar} \end{cases}$

(d) $f(n) = \frac{1}{2} + negl(n)$, unde $negl(n)$ este o funcţie neglijabilă în n

(e) $f(n) = \frac{p(n)}{2^n}$, unde $p(n)$ este o funcţie polinomială în n

(f) $f(n) = \frac{1}{6}$

PRG (PseudoRandom Generator)

8. Fie $G : \{0,1\}^k \to \{0,1\}^n$, $k < n$ definit mai jos. Este G PRG?

   (a) $msb(G(s)) = 1$ pentru orice s, unde msb = most significant bit

   (b) $msb(G(s)) = 1$ cu probabilitate $\frac{1}{n^{100}}$, unde msb = most significant bit

   (c) $G(s) = G_0(s)||G_1(s)||G_2(s)$, unde $|G_0(s)| = |G_1(s)| = |G_2(s)|$, $G_2(s) = G_1(s) \oplus G_0(s)$ şi $||$ semnifică concatenare

   (d) $G(s) = G_0(s)||G_1(s)$, unde $G_0(s) = f(G_1(s))$ şi f este o funcţie cunoscută

9. Se ştie că dacă $\hat{G}$ este PRG, atunci $\hat{G}'(s) = \hat{G}(s_{n/2}, \ldots, s_n)$ este PRG, unde $s = s_1 \ldots s_n$. Fie G PRG. Se defineşte $G'(s) = G(s0^{|s|})$. Este G' PRG?

PRF (PseudoRandom Function)

10. Fie F' PRF. Este F PRF?
    $$F_k(x) = \begin{cases} F'(x) & x \text{ par} \\ F'(x+1) & x \text{ impar} \end{cases}$$

11. Fie $F : \mathcal{K} \times \mathcal{X} \to \{0,1\}^{128}$ PRF. Este F' PRF?
    $$F'_k(x) = \begin{cases} 0^{128} & x = 0 \\ F_k(x) & x \neq 0 \end{cases}$$

12. Fie G PRG şi $G'(s)$ egal cu $G(s)$ trunchiat la primii n biţi, unde $|s| = n$. Arătaţi că $F_k(x) = G'(k) \oplus x$ nu este PRF.