

### PRG (PseudoRandom Generator)

1. Fie  $G : \{0, 1\}^k \rightarrow \{0, 1\}^n$ ,  $k < n$  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  $|G_0(s)| = |G_1(s)| = |G_2(s)|$ ,  $G_2(s) = G_1(s) \oplus G_0(s)$  și  $||$  semnifică concatenare
  - (d)  $G(s) = G_0(s) || G_1(s)$ , unde  $G_0(s) = f(G_1(s))$  și  $f$  este o funcție cunoscută
2. Se știe că dacă  $\hat{G}$  este PRG, atunci  $\hat{G}'(s) = \hat{G}(s_{n/2} \dots s_n)$  este PRG, unde  $s = s_1 \dots s_n$ . Fie  $G$  PRG. Se definește  $G'(s) = G(s0^{|s|})$ . Este  $G'$  PRG?

### PRF (PseudoRandom Function)

3. Fie  $F' : \{0, 1\}^k \times \{0, 1\}^n \rightarrow \{0, 1\}^m$  PRF. Este  $F$  PRF?

$$F_k(x) = \begin{cases} F'(x) & x \text{ par} \\ F'(x+1) & x \text{ impar} \end{cases}$$

4. Fie  $F : \mathcal{K} \times \mathcal{X} \rightarrow \{0, 1\}^{128}$  PRF. Este  $F'$  PRF?

$$F'_k(x) = \begin{cases} 0^{128} & x = 0 \\ F_k(x) & x \neq 0 \end{cases}$$

### Moduri de operare

5. Scrieți formulele de decriptare pentru modurile de operare ECB, CBC, OBF, CTR. Care pot fi paralelizate?
6. O tranzacție bancară folosește modul de operare ECB cu structura indicată mai jos, unde Banca A, respectiv Contul CA indică proveniența banilor, iar Banca B, respectiv contul CB indică destinația banilor care se transferă. Ce strategie poate să adopte Oscar pentru a transmite banii în contul personal?

1	2	3	4	5
Banca A	Contul CA	Banca B	Contul CB	Suma transferată (EUR)

**DES. AES**

7. Un program de criptare folosește DES cu chei pe 56 de biți. Cheia este generată pe baza unei parole de 8 caractere codate ASCII extended (coduri posibile: 0-255):  $8 \cdot 8 = 64$  biți, dintre care 8 nu se iau în calcul, conform criptării obișnuite DES (mai exact, lsb din fiecare caracter este ignorat). Se presupune că un calculator obișnuit poate să testeze  $10^6$  chei pe secundă.
- (a) Care este spațiul cheilor dacă toate caracterele sunt alese aleator? Cât timp necesită o căutare exhaustivă?
  - (b) Care este spațiul cheilor dacă se consideră doar caracterele ASCII obișnuite (coduri posibile: 0-127)? Cât timp necesită o căutare exhaustivă?
  - (c) Care este spațiul cheilor dacă parola folosește numai litere mari? Cât timp necesită o căutare exhaustivă?
8. Se consideră intrarea într-o rundă AES:

$$\begin{bmatrix} 04 & 07 & E2 & 49 \\ F2 & 78 & 2F & C5 \\ CA & 28 & 01 & D7 \\ 97 & 45 & 96 & 10 \end{bmatrix}$$

și cheia de rundă

$$\begin{bmatrix} 21 & 35 & AC & 6C \\ 75 & 50 & AF & 1B \\ 17 & 62 & 6B & F0 \\ 87 & 0B & 3C & 9B \end{bmatrix}$$

Care este ieșirea din rundă?