13/11/2023. HAI709I : Fondements cryptographiques de la sécurité. Questions de mi-parcours.

Question 1. Soit $P(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3$ un polynôme tel que chaque coefficient a_i est un nombre entier entre 0 et 16. On sait que $a_3 = 2$ et

$$P(1) = 0 \mod 17, \quad P(2) = 0 \mod 17, \quad P(3) = 0 \mod 17.$$

Trouvez a_0.

Question 2. Pour une paire de variables aléatoires conjointement distribuées (X, Y), on sait que $H(X \mid Y) = 3$, $H(X) = 6$ et $H(Y) = 5$. Trouvez $H(Y \mid X)$.

Question 3. Nous considérons un schéma de partage de secret avec quatre participants A, B, C, D tels que
- les groupes $\{A, B\}$, $\{A, C\}$, $\{A, D\}$, et toutes leurs extensions connaissent le secret ;
- les autres sous-ensembles de participants n'ont aucune information sur le secret.

En Français : pour connaître le secret, nous avons besoin de l'utilisateur A et en plus d'au moins un autre utilisateur.

Supposons que le secret k est choisi au hasard avec une distribution uniforme dans l'ensemble $\{1, 2, \ldots, N\}$.

(a) Soit (S_A, S_B, S_C, S_D) la distribution correspondante des probabilités sur les parts des participants. Prouvez que l'entropie de Shannon de S_B ne peut pas être inférieure à $\log_2 N$.

(b) Proposez un schéma de partage de secret (construisez une distribution conjointe de la clé secrète avec (S_A, S_B, S_C, S_D)) où $H(S_A) = H(S_B) = H(S_C) = H(S_D) = \log_2 N$.

Question 4. Soit $f(n)$ une fonction négligeable. Prouvez que les fonctions

$$g(n) = 10 \cdot f(100 + n) \text{ et } h(n) = f^2(n) + 2^{-n}$$

sont également négligeables.

Question 5. Soit $G : \{0,1\}^n \to \{0,1\}^{2n}$ une fonction qui transforme chaque chaîne de n bits x vers la chaîne de $(2n)$ bits xx (l'entrée répétée deux fois). Prouvez que $G(x)$ n'est pas un générateur pseudo-aléatoire.

Question 6. Soit $\Pi = (Gen, Enc, Dec)$ un schéma de chiffrement qui est sûr au sens calculatoire. Nous considérons l'expérience suivante :
- nous produisons une clé secrète aléatoire k pour le paramètre de sécurité n, $k \leftarrow Gen(1^n)$
- nous produisons un message clair aléatoire $m = x_1 \ldots x_n \in \{0,1\}^n$ (avec une distribution uniforme, c'est-à-dire que chaque message de longueur n est choisi avec une probabilité de $1/2^n$)
- nous calculons un message chiffré $e = Enc(m, k)$
- l'adversaire obtient 1^n et le message chiffré e, et tente de deviner le XOR des dix premiers bits du message clair $x_1 \oplus \ldots \oplus x_{10}$ et renvoie le résultat $j \leftarrow Adv(1^n, e)$.

Le succès de l'adversaire est défini comme

$$\textbf{succès} = \begin{cases} 1, & \text{si } j = x_1 \oplus x_2 \oplus \ldots \oplus x_{10} \\ 0, & \text{sinon.} \end{cases}$$

Prouvez que pour chaque algorithme calculable en temps polynomial Adv,

(a) il existe une fonction négligeable $g(n)$ telle que

$$\left| \text{Prob}[\textbf{succès} = 1] - \frac{1}{2} \right| \leq g(n),$$

(b) il existe $n_0 \in \mathbb{N}$ tel que pour tout $n \geq n_0$

$$1/3 < \text{Prob}[\textbf{succès} = 1] < 2/3.$$

(c) Répondez aux mêmes questions pour un schéma *parfaitement* sûr.