Sécurité des communications informatiques TD#1

2024–01-26

Exercice 1 : One-time pad

Q.1 : On considère deux variables aléatoires X et Y indépendantes sur $\{0,1\}$. X suit une distribution uniforme et Y une distribution quelconque ; on note $p := \Pr[Y = 0]$.

Soit $Z := X \oplus Y$ la variable aléatoire sur $\{0,1\}$ donnée par le OU EXCLUSIF entre X et Y, calculez :

1. $\Pr[Z = 0]$
2. $\Pr[Z = 1]$
3. $\Pr[Z = 0 \wedge Y = 0]$; en déduire que Z est indépendante de Y.
4. $\Pr[Z = 0 \wedge X = 0]$; en déduire que Z est indépendante de X ssi. $p = 1/2$.
5. $\Pr[Y = 0 : Z = 0]$

   Indice. Utilisez la formule des probabilités conditionnelles :

   $$\Pr[A : B] = \frac{\Pr[B : A]\Pr[A]}{\Pr[B]}$$

   (pour $\Pr[B] > 0$).
6. $\Pr[Y = 0 : Z = 0]$, en prenant cette fois une distribution quelconque pour X, en notant $q := \Pr[X = 0]$. Comparez avec le résultat précédent.

Q.2 : On rappelle que n variables aléatoires $X_0, \ldots, X_{n-1}$ d'images $\mathcal{X}_0, \ldots, \mathcal{X}_{n-1}$ sont *mutuellement indépendantes* ssi. :

$$\forall (x_i)_{0 \leqslant i < n} \in \mathcal{X}_0 \times \cdots \times \mathcal{X}_{n-1},\ \Pr\left[\bigwedge_{0 \leqslant i < n} X_i = x_i\right] = \prod_{0 \leqslant i < n} \Pr[X_i = x_i]$$

ou de façon équivalente ssi. :

$$\forall (x_i)_{0 \leqslant i < n} \in \mathcal{X}_0 \times \cdots \times \mathcal{X}_{n-1},\ \forall j \in [\![0, n-1]\!],$$
$$\Pr\left[X_j = x_j : \bigwedge_{0 \leqslant i \neq j < n} X_i = x_i\right] = \Pr[X_j = x_j]$$

On considère une variable aléatoire $X = (X_i)_{0 \leqslant i < n} \in \{0,1\}^n$.

1. Montrez que X suit une distribution uniforme sur $\{0,1\}^n$ ssi. les X_i sont uniformes sur $\{0,1\}$ et mutuellement indépendantes.

Q.3 :

1. Déduire des questions précédentes que si X et Y sont deux variables aléatoires sur $\{0,1\}^n$, avec X uniforme, alors $Z := X \oplus Y$ donnée par le OU EXCLUSIF bit à bit de X et Y est uniforme sur $\{0,1\}^n$ et indépendante de Y.

Remarque : De façon générale, on peut montrer que ce résultat reste valable sur n'importe quel quasigroupe fini.

Exercice 2 : Attaque générique et valeurs de paramètres

Q.1 : On considère une fonction quelconque $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$.

1. Montrez que :
$$\mathbf{Adv}_F^{\mathrm{PRF}}(2, 2^n) \approx 1$$
2. Quelle valeur minimale conseilleriez vous de prendre pour n, si vous avez pour objectif d'atteindre un niveau de sécurité PRF permettant de résister à une attaque de la planète entière ?
3. Est-il suffisant de prendre le n conseillé précédemment pour garantir que F aura une « bonne » sécurité PRF ?