Révisions et protocoles cryptographiques

Exercice 1. On considère le sytème de chiffrage de 1 bit p par une clé k de 1 bit et un ou exclusif : $c = p \oplus k$. On suppose maintenant que tous les textes clairs ne sont pas équiprobables et que les clés ne sont pas équiprobables. On suppose tout de même que la clé est choisie indépendamment du texte clair. Les probabilités sont données par :

p	$\mathbb{P}(p)$	k	$\mathbb{P}(k)$
0	$\frac{1}{4}$	0	$\frac{1}{4}$
1	$\frac{3}{4}$	1	$\frac{3}{4}$

1. Calculer $\mathbb{P}(c = 0)$, $\mathbb{P}(c = 1)$, $\mathbb{P}(p = 0 \,|\, c = 0)$ et $\mathbb{P}(p = 0 \,|\, c = 1)$.

2. Ce système est-il parfaitement sûre ?

Exercice 2. Le paradoxe des anniversaires. 1. On lance un dé rouge, un dé vert et un dé bleu.

1.a. Combien y a-t'il de tirages possibles ?

1.b. Combien y a-t'il de tirages où les trois dés sont différents ?

1.c. Combien y a-t'il de tirages où au moins deux des trois dés sont égaux ?

2. Quelle est la probabilité que deux personnes choisies au hasard aient leur anniversaire le même jour ?

3. On tire au hasard k nombres parmi n, quelle est la probabilité que deux d'entre eux soient égaux.

Exercice 3. À quelle vitesse doit être cadencée une puce (dé)chiffrant en utilisant le 3DES sur une connexion ethernet ?

Exercice 4. Cryptographie publique, premier exemple : énigmes de Merkle

Alice et Bob veulent échanger des messages secrets par un canal peu sûr. Au début du protocole ils ne disposent pas d'un secret partagé.

On propose le protocole suivant :

1. Alice et Bob se mettent d'accord sur deux protocoles à clé privée, le premier qu'ils considèrent comme sûr (AES avec une clé de 128 bits), le deuxième, `crypt`, qui n'utilise que des clés de 20 bits et qui ne peut être attaqué que par recherche exhaustive de la clé.
2. Alice choisit 2^{20} triplets (x, k, k') au hasard où x est un nombre, k est une clé AES de 128 bits et k' une clé de 20 bits, de manière à ce que chaque nombre x apparaît au plus une fois.
3. Pour chacun des triplets Alice envoie le message `crypt("Ceci est la clé numéro` x : k`",`k'`)`.
4. Bob choisit au hasard un message et le déchiffre par une recherche exhaustive de la clé k'.
5. Bob envoie à Alice le numéro x_0 du message qu'il a déchiffré.
6. Bob et Alice communique maintenant grâce à la clé k_0 contenue dans le message x_0.

1. Que doit faire un espion pour découvrir la clé secrète k_0 ?

2. Combien d'opérations sont effectuées par Alice, Bob et l'espion ?

3. Quelles doivent-être les propriétés de `crypt` ?