M1MI2016 Codes et Cryptologie

Feuille d'exercices n° 4.

Masque jetable, générateurs pseudo-aléatoires

Dans les exercices qui suivent, les textes clairs sont écrits en français, et les vingt-six lettres sont codées de 0 à 25 dans l'ordre alphabétique ; de plus, chaque entier de 0 à 25 est représenté par son écriture binaire sur cinq bits. Par exemple, $e = 4 = 00100$. Les autres caractères (blancs, accents, ponctuation, etc..) sont ignorés.

1 Ce message :

0 0 1 1 1 1 0 1 0 0 0 0 0 1 0 1 0 1 1 0 0 0 0 0 0 1 1 1 0 1 1 0 0 1 0 1 0 0 0 1
1 0 1 1 1 0 1 1 0 1 1 1 1 0 1 1 1 0 1 1 0 0 0 0 0 0 0 1 1 1 1 0 0 1 1 1 0 1 0 1
0 1 0 1 1 0 1 0 0 1 0 0 1 0 1 1 1 0 0 0 0 1 1 0 0 1 1 0 1 1 1 0 1 1 0 1 0 0 0 0
0 1 1 0 1 0 1 0 0 1 0 0 0 1 0 1 1 1 1 0 1 0 1 1 0 0 0 1 0 0 0 1 1 1 1 0 1 0 1 0
1 1 1 0 0 1 0 1 1 1 0 0 1 0 1 1 1 1 1 1 0 1 0 0 1 1 1 1 1 1 1 1 0 1 1 0 1 1 0 0
0 0 0 0 0 0 1 1 1 1 1 1 0 1 0 0 0 0 1 0 0 1 0 1 0 0 0 1 0 1 0 0 1 1 1 1 1 0 0 1

est chiffré par un chiffrement de Vernam avec la clé :

0 1 1 0 0 1 0 0 0 0 0 1 1 1 0 1 0 1 1 0 1 0 0 1 0 0 1 1 0 1 0 0 1 1 0 1 0 1 0 1
1 1 1 1 0 0 1 0 0 1 0 1 1 1 0 1 1 0 1 1 0 0 0 0 1 0 1 1 0 0 1 0 1 1 1 1 0 0 0 1
1 1 0 0 1 1 1 0 1 0 0 1 1 0 1 1 0 1 0 1 0 1 1 1 0 1 0 1 0 1 1 1 0 1 1 1 0 0 1 1
0 0 1 0 1 1 1 0 1 0 0 1 0 1 0 1 0 0 0 0 1 1 0 1 1 0 1 0 0 1 0 1 0 1 1 0 0 0 0 1
1 0 1 1 1 1 0 0 1 1 0 1 0 0 1 1 1 0 1 1 0 0 1 0 0 0 1 1 0 0 0 1 0 0 1 1 1 0 0 0
1 0 0 0 1 1 1 1 0 1 1 1 1 0 1 0 0 0 1 0 0 0 1 1 1 0 1 0 0 0 0 1 0 0 1 1 0 1 0 0

Déchiffrez-le.

2 Rastapopoulos a encore intercepté deux messages chiffrés, envoyés par Tintin au Capitaine Haddock :

0 0 0 1 0 1 0 1 0 0 1 0 0 1 1 1 1 1 1 0 0 0 1 0 0 0 1 0 0 1 1 1 1 1 1 1 0 1 0 1
1 1 1 0 1 1 1 0 0 0 0 0 1 0 0 1 1 1 0 1 0 1 0 0 1 1 0 1 1 0 1 0 0 0 0 0 1 1 1 0
0 0 0 1 1 0 0 0 0 1 0 1 0 1 1 0 0 1 1 0 0 0 1 1 0 1 0 0 0 1 0 1 1 0 1 0 0 0 0 1 0
0 1 0 1 0 0 1 0 1 1 1 0 1 0 1 1 1 1 0 1 0 1 1 0 1 0 1 1 1 0 0 1 1 1 1 1 1 1 0 0 1
0 0 1 1 1 1 1 1 1 1

1 1 0 1 0 1 1 1 1 0 1 0 1 0 1 0 1 1 0 0 0 0 1 1 1 0 1 1 1 1 1 1 1 0 0 1 1 0 1 1 1
1 0 0 1 0 0 0 1 1 1 1 0 0 1 1 1 1 1 0 0 0 1 0 1 0 1 1 0 1 0 1 0 0 0 0 0 1 1 1 1
1 0 0 1 1 0 0 0 0 1 0 0 1 0 1 1 0 1 1 0 0 0 1 1 1 1 0 0 0 1 1 0 0 1 0 1 1 1 1 1
1 0 1 0 1 1 1 1 0 0 0 0 0 1 0 1 1 1 1 0 0 1 1 0 0 0 1 0 0 1 0 0 0 1 0 1 1 0 1 1
1 1 0 1 1 0 0 0 0 1 0 0 1 0 1 0 0 1 0 1 0 1 0 1 1 1 1 0 1 0 0 1 0 0 0

Tintin a compris que le chiffrement affine n'est pas sûr, il a donc utilisé un chiffrement de Vernam. Mais il a utilisé la même clé pour les deux messages ! Aidez Rastapopoulos à décrypter ces deux messages. Il s'agit sûrement de la disparition de Tournesol...

3 Le registre à décalage linéaire binaire de longueur 4 associé à la fonction de transition $x_{k+4} = x_{k+1} + x_k$ est utilisé pour engendrer une suite pseudo-aléatoire.

1. Combien de suites binaires distinctes peut-on engendrer ?
2. On initialise le registre avec $(x_1, x_2, x_3, x_4) = (1, 0, 0, 0)$. Calculer les termes suivants de la suite. Qu'observez-vous sur sa période ?
3. Quelle est la période pour d'autres initialisations ?
4. Qu'observez-vous sur le nombre de 0 et de 1 dans une période ? Et sur l'occurence des mots de longueur 2, 3, 4 ?

4 Une suite binaire $x = (x_1, x_2, \dots)$ est engendrée par un registre à décalage linéaire de longueur s et on suppose qu'elle est périodique de période $2^s - 1$.

1. Montrez que le registre prend exactement $2^s - 1$ états distincts, correspondants à tous les mots binaires de longueur s différents de $00\dots0 = 0^s$, avant de retrouver sa position initiale.
2. En déduire que les mots de longueur $t \leq s$ différents de 0^t ont la même occurence dans chaque période.

5 On a intercepté 10 bits successifs d'une suite binaire engendrée par un registre à décalage linéaire de longueur 5 : 10110010001. Retrouvez sa fonction de transition, puis calculez les termes suivants.

6 Un générateur linéaire congruentiel de la forme

$$x_{i+1} = ax_i + b \bmod 103$$

produit la suite d'entiers :

$$36, 35, 18, 38, 69, 81, \dots$$

Trouver l'entier suivant.

7 Un générateur linéaire congruentiel de la forme $x_{i+1} = ax_i + b \bmod n$ produit la suite d'entiers : $x_0 = 47, x_1 = 93, 32, 116, 73, 15, 123, 129, 34, 132, 58, 38, 21 \dots$.

Il s'agit de reconstituer le générateur, c'est-à-dire les entiers a, b, n.

1. Former les premiers termes de la suite dérivée, soit

$$x'_0 = x_1 - x_0, x'_1 = x_2 - x_1, x'_2 = x_3 - x_2, \dots$$

2. Quelle relation a-t-on entre x'_i et x'_{i+1} ?
3. Montrer que si

$$ux'_1 + vx'_2 = 1$$

alors

$$ux'_2 + vx'_3 = a \bmod n$$

4. En déduire un représentant entier de $a \bmod n$.
5. En déduire un représentant entier de $b \bmod n$.
6. En déduire n.