Cryptographie et arithmétique – Feuille 1

Exercice 1 (recherche exhaustive). Alice et Bob utilisent un système de chiffrement symétrique pour communiquer entre eux. Ce système de chiffrement permet d'utiliser des clés de 64 bits, 128 bits ou de 256 bits. Alice et Bob se servent d'une clé secrète de 64 bits. Oscar dispose d'un message clair m et du chiffré c de m par ce système de chiffrement. On suppose qu'Oscar utilise un ordinateur capable d'exécuter l'algorithme de chiffrement 2^{40} fois par seconde.

1. Décrire une méthode permettant à Oscar de retrouver la clé secrète utilisée par Alice et Bob. Combien de temps lui faut-il ?
2. Alice et Bob, avertis de cette attaque, décident d'utiliser une clé de 128 bits. Qu'en pensez-vous ?

Exercice 2 (chiffrement parfait). Un système de chiffrement est dit parfait si la connaissance d'un message chiffré n'apporte aucune information sur le message clair, même à un adversaire ayant des ressources calculatoires illimitées.
On considère le système de chiffrement symétrique suivant : pour échanger un message $m \in \{0,1,2\}$, Alice et Bob se rencontrent et décident d'une clé aléatoire $k \in \{0,1,2\}$ partagée. L'opération de chiffrement consiste à représenter k et m en base 2 avec 2 bits, et à effectuer le « XOR » des deux représentations.

1. Quel est l'algorithme de déchiffrement ?
2. Faire un tableau de tous les chiffrés possibles. Ce système de chiffrement est-il parfait ? Un carré latin d'ordre 3 est un tableau de nombres possédant 3 lignes et 3 colonnes. Les éléments de ce tableau appartiennent à l'ensemble $\{0,1,2\}$ et sont tels que chaque nombre de cet ensemble n'apparaît qu'une seule fois sur chaque ligne et chaque colonne. On note $l_{i,j}$ l'élément situé en ligne i et colonne j. On modifie le système de chiffrement de la manière suivante : le chiffré du message $m \in \{0,1,2\}$ avec la clé $k \in \{0,1,2\}$ est l'élément $l_{k,m}$.
3. Donner un exemple de tel carré latin.
4. Quel est l'algorithme de déchiffrement ? Le système de chiffrement est-il parfait ?

Exercice 3 (chiffrement par substitution). Soit σ une permutation de $\mathbb{Z}/26\mathbb{Z}$. Chaque lettre de l'alphabet est identifiée à un élément x de $\mathbb{Z}/26\mathbb{Z}$ et est chiffré $\sigma(x)$.

1. Comment chiffre-t-on et déchiffre-t-on un message ? Combien a-t-on de clés différentes possibles ? Comparer avec le nombre de clés différentes possibles dans le cas du chiffrement par décalage.
2. Montrer que l'application $x \mapsto x^5$ ne définit pas une permutation de $\mathbb{Z}/31\mathbb{Z}$, mais que $x \mapsto x^7$ si, et déterminer la fonction de déchiffrement (on admet le petit théorème de Fermat, qui implique en particulier que $x^{30} \equiv 1 \mod 31$ pour tout entier x non divisible par 31).

Exercice 4 (clés involutives). Le but de l'exercice est de trouver des chiffrements dont la fonction de déchiffrement est la même que la fonction de chiffrement.

1. Si la fonction de chiffrement est involutive quelle est la clé de déchiffrement ?
2. On se place dans le cas d'un chiffrement par décalage sur un alphabet à n lettres. Trouver toutes les clés involutives (*i.e.* telles que la fonction de chiffrement est involutive). Traiter les cas $n = 26$ et $n = 29$.

3. Si le chiffrement est un chiffrement par substitution de longueur n, combien y a-t-il de clés involutives ?

Exercice 5 (cryptanalyse par fréquence). Le but de l'exercice est de déchiffrer le texte chiffré ci-dessous grâce à une analyse de fréquence. Le texte est en français. On utilisera le fait que la lettre la plus fréquente en français est le E, viennent ensuite S puis A.

XGCLKPHEUL GPFQYYWHST YIYHFENYIG HFYIGHQASY
DQWGTHGWYC SLQWYLXYWC EIISTQCGHQ ETWTSIYLQA
SYW

1. Si, comme on peut s'y attendre, la lettre la plus fréquente du message clair est le E, peut-on affirmer que le message a été chiffré par décalage ?
2. Déchiffrer le message ci-dessus.
3. On veut maintenant adapter cette méthode à un chiffrement de Vigenère. Trouver la longueur de la clé utilisée pour chiffrer le message suivant.

   PVCIGHMSRO RWMSWNOTQW WYTEAOZLPV CIGHMSMRLD
   PAILUZMLNH OEWOUWXCOU MVXGUNNSXL MJNUMKVLOF
   QFMEIITJLS NXXEAOZLPV CIGHMETAWM AWUPIVBMWM
   KLPGILXVQL MK

4. Connaissant la longueur de la clé, comment peut-on se ramener à un chiffrement par décalage ?