Série 5

Problème 5.1

1. En utilisant les indications de notre indic', nous pouvons déjà identifier quelques correspondances (dans le cas d'une substitution monoalphabétique). Nous savons donc que :

chiffré	W	V	E	K	U	E	L	W
clair	S	R	R	R	P	A	S	S

Cela nous montre clairement qu'Homer a tort : s'il avait raison, cela signifierait que la lettre S se code à la fois en W et en L ; pire encore la lettre R, une fois codée, deviendrait alors à la fois V, E et K. La substitution monoalphabétique associant une et une seule lettre de code à une lettre en clair, il est impossible que ce soit cette méthode de cryptographie.

Il est en revanche tout à fait envisageable qu'un code de Vigenère ait été utilisé. C'est par cette méthode que nous allons décrypter le message.

2. Pour décoder ceci, nous devons d'abord poser ce que nous savons :

Clair	S****R**R****R****PASS*****
Clé	(encore rien)
Chiffré	WNZTNVIEEGTJYKRRWYUELWNZTNV

Afin de respecter la *thèse de Kerckhoffs*, nous savons qu'il s'agit d'un code de Vigenère. De là, nous n'avons qu'à observer les positions des lettres en claire que nous avons, ainsi que des lettres codées correspondantes ($A = 0, Z = 25$), puis soustraire la position claire à la position chiffrée (modulo 25). Par exemple, pour la première lettre, nous regardons $W/22 - S/18 = E/4$. Depuis là, nous pouvons poser quelques lettres de la clé :

Clair	S****R**R****R****PASS*****
Clé	E****E**N****T****FETE*****
Chiffré	WNZTNVIEEGTJYKRRWYUELWNZTNV

Depuis là, nous devons chercher la longueur de la clé, sachant qu'elle se répète. Il est tentant "d'aligner" le premier E de la clé avec un autre. Aligner avec le second ne donne pas de bon résultat (car le F et le T seraient alors à la même position dans la clé). Après quelques essais de longueur (+ que 5, car il y a 4 lettres différentes et les deux E de la fin sont trop proches pour être à la même position). Finalement, la longueur 7 semble convenir, les lettres s'alignant merveilleusement. En tentant de décoder de la sorte, nous trouvons des résultats pour la clé et le plaintext. Ainsi :

Le sujet de l'examen important est *Savoir par cœur n'est pas savoir*

La clé de chiffrement utilisée est *ENEFFET*

Problème 5.2

Non, cette méthode n'est pas plus sûre. En effet, appliquer deux clés de même longueurs à la suite revient à utiliser une seule clé (obtenue par une composition des deux). Par exemple, appliquer sur notre texte la clé *dora*, (donc décaler chaque lettre de respectivement 3, 14, 17, 0), puis appliquer la clé *toto* (décalage de 19, 14, 19, 14) revient à décaler de la "somme" des deux clés (modulo 25), à savoir (19+3), (14+14), (19+17), (14+0), soit la clé *wclo*, ce qui n'est pas plus sécurisé qu'appliquer une seule clé.

En revanche, si elle avait décidé d'appliquer deux clés de longueurs différentes, son message crypté aurait été plus sécurisé.

Problème 5.3

1. Par définition, un codage est à confidentialité parfaite si connaître le texte chiffré C ne dit rien sur la source X_1. Or, si C = 49, alors X_1 est forcément 7. Ce cas (parmi d'autres) montre clairement que ce système n'est pas à confidentialité parfaite.

2. Bien sûr. Pour cela, elle a simplement à changer X_0 et X_1 en code binaire sur 3 bits (afin de pouvoir représenter tous chiffres de 1 à 7), de la

manière habituelle ($1 \rightarrow 001,\ 2 \rightarrow 010, ..., 7 \rightarrow 111$). Elle pourra obtenir le cyphertext de la manière suivante : $C = X_1 \bigoplus X_0$. Ayant les mêmes probabilités d'apparition et étant encodés de la même manière, X_0 et X_1 auront la même entropie.

De plus, C et X_1 seront indépendants (savoir C ne permettra en rien de savoir X_1).

Par exemple, prenons C = 101 ; tous les X_1 possible peuvent engendrer ce C, seule la clé changeant alors. Nous pouvons d'ailleurs généraliser à toutes les combinaisons : comme le chiffre 1 peut être obtenu par $1 \bigoplus 0$ ou $0 \bigoplus 1$ et que 0 est obtenable par $0 \bigoplus 0$ ou $1 \bigoplus 1$, chaque combinaison du message codé a la même probabilité d'apparition (notons aussi que les chiffres de 1 à 7 s'encoderont proposant toutes les combinaisons de 000 à 111 de manière équiprobable). Chaque probabilité est la même $\frac{1}{7}$. Tout cela mis ensemble nous prouve que l'entropie de la clé, du message en clair et du message codé sont la même, à savoir $7 \times \frac{1}{7} \log_2(7) = \log_2(7) \simeq 2.81$. Ce système est donc à confidentialité parfaite.

Notons que pour décoder C, Bart n'aura qu'à faire l'opération inverse, à savoir $C \bigoplus X_0$