Science de l'information : Série 6

Exercice 6.1 :

Nous voyons rapidement qu'il ne s'agit pas d'un chiffre de César (les écarts entre C et R et celui entre H et Y ne sont pas les mêmes). Ensuite, sachant qu'il s'agit d'un code de Vigenère, j'ai écrit un code permettant de trouver la clé, qui se trouve être PRINTEMPS. La méthode pour trouver une telle clé est simple : nous attribuons un chiffre à chaque lettre du message clair et du message codé en fonction de sa place dans notre alphabet. Nous regardons ensuite leur différence, et cherchons la lettre à cette place dans notre alphabet.

Exercice 6.2

1. Le code utilisé pour encoder le numéro de téléphone est clairement à décodage unique, car le code morse pour les chiffres se compose toujours de 5 caractères (selon une logique bien précise). Comme chaque chiffre a une longueur de 5 caractères, aucun n'est le prédécesseur d'un autre, donc le code est à décodage unique.

2. Le numéro (en binaire) et le masque ont tous deux une longueur de 50 caractères, avec le même alphabet. Les caractères du numéro ne sont pas indépendants (en morse, on n'aura jamais 01110, les 1 et les 0 sont clairement séparés) et les caractères du masque sont indépendants (hasard). Ainsi, l'entropie du masque est plus grande que celle du message, ce qui garantit une confidentialité parfaite.

3. Le message n'est pas à confidentialité parfaite, pour la même raison qu'à la question 2. En effet, le masque est formé de 10x un code de 5 bits, avec des caractères indépendants. Ce code de 5 bits a donc une entropie largement inférieure à celle du message, ce qui nous assure qu'il n'est pas à décodage unique (pour les sceptiques, regarder la question suivante).

4. Pour cette question, nous pouvons avoir recours à deux méthodes : la logique et la brute. La brute consiste à regarder le premier caractère, supposer tous les caractères du message possibles (0-9) et en déduire toutes les clés possibles pour ce caractère. Ensuite, nous testons ces clés sur le caractère suivant, et retirons de la liste toutes les clés qui, via cette clé, ne donnent pas de chiffre en morse. Nous réitérons ensuite sur les caractères suivants, afin de trouver une seule clé possible (10010). Une fois cette clé trouvée, il devient trivial de décoder le numéro de téléphone (via 10 opérations xor entre la clé et le message codé).

   La manière logique épargne du travail, mais on risque de causer une erreur. Vu qu'il s'agit d'un numéro de téléphone, nous pouvons supposer que le numéro commence par un 0. De là, en ''sachant'' ce premier caractère, via la même opération xor entre ce

caractère (00000) et le caractère codé (10010), nous pouvons trouver la clé, qui est la même que via la méthode brute.

Le numéro de téléphone de l'agent est donc celui de Serge Vaudenay (http://people.epfl.ch/serge.vaudenay), à savoir **021 639 76 96**.

5. Ici, la méthode logique ne peut pas se faire, aucune supposition ne pouvant être faite, nous devons passer par la méthode brute. Cela se fait de la même manière qu'au précédent. D'abord nous imaginons toutes les possibilités pour le premier caractère (0-9) et trouvons les 10 clés correspondantes possibles, puis testons toutes ces clés sur les caractères suivants (en regardant si la combinaison (message codé) xor (clé) donne un chiffre). Les clés se dispersent rapidement pour ne laisser que deux clés possibles : 10010 (la même qu'avant, donc Bart ne saurait pas générer un nouveau masque ou la chance est extraordinaire) ou alors 01101 (l'exact opposé de l'autre clé, ce qui semble logique). Les deux codes engendrés par ces clés sont donc respectivement 3847635 et 8392180 (ce qui correspond à l'inverse morse [point devient trait] du premier code).

   Or, comme Dolph a droit à trois essais avant de bloquer la porte, il n'aura qu'à tenter de rentrer les deux codes, et sera sûr de rentrer sans encombre (pour autant qu'il ne se trompe pas dans la saisie du code), et pourra ainsi rencontrer le terrible M. Vaudenay, l'agent de la NSA.

Exercice 6.3

1. décomposition de 52 : 2*2*13

   décomposition de 143 : 11*13

   décomposition de 176 : 2*2*2*2*11

2. PGDC(52, 143) : 13

   PGDC(52, 176) : 2*2 = 4

   PGDC(142, 176) : 11

3. Aucuns de ces chiffres ne sont premiers entre eux, car leurs PGDC respectifs sont tous différents de 1.

4. Pour trouver cela, il nous faut décomposer un peu ce chiffre : il vaut 9+8*10^6 + 7*10^12 + 6*10^18 + 5*10^24 + 4*10^30 + 3*10^36 + 2*10^42 + 1*10^48.

   9 modulo 999999 vaut 9, cela est évident. Et par la suite, 10^6 modulo 999999 vaut 1, donc 10^12 modulo 999999 = 10^6 modulo 999999 * 10^6 modulo 999999, et ainsi de suite pour toutes les puissances multiples de 6. Donc le modulo sera de 9+8*1+7*1+6*1+5*1+4*1+3*1+2*1+1*1 = 1+2+3+4+5+6+7+8+9 = **45**