Corrigé – Sécurisation des communications

Exercice 1

Enigma est une machine électromécanique portative servant au chiffrement et au déchiffrement de l'information. Elle a été créée en 1919. Son utilisation la plus célèbre fut celle faite par l'Allemagne nazie et ses alliés, avant et pendant la Seconde Guerre mondiale, la machine étant réputée inviolable selon ses concepteurs. Néanmoins un nombre important de messages Enigma ont pu être déchiffrés près de sept ans avant la guerre puis pendant, grâce aux cryptanalystes britanniques, dont Alan Turing.

Exercice 2

Méthode que Pierrot doit mettre en œuvre pour déchiffrer le message :

- Regarder dans la table de Vigenère toutes les possibilités pour une même lettre, et ce pour chaque lettre du message chiffré ;
- Étudier les différentes combinaisons possibles pour identifier un texte qui ressemble à un message.

C'est Bob qui obtient le résultat en premier car il possède la clef et n'a qu'à regarder la correspondance dans la table de Vigénère alors que Pierrot doit tester toutes les possibilités en espérant tomber sur la bonne.

Exercice 3

1. "ri", message chiffré, en binaire : 0111 0010 0110 1001 -> résultat du XOR entre le clef 0000 1010 et le message d'origine. On déduit du XOR que le message d'origine est : 0111 1000 0110 0011, soit "xc"
2. (a) La clef publique de A (AKpub, celle « de l'autre » personne).

   (b) La clef privée de A (AKpriv, la « sienne »).
3. HTTPS permet de chiffrer les données qui transitent sur le web grâce à une méthode de chiffrement asymétrique et d'un certificat géré par un organisme extérieur dédié. Ceci permet d'ouvrir une sorte de tunnel sécurisé où les messages sont chiffrés de manière symétrique.

Exercice 4 – *(Exercice tiré du bac 2021)*

1. (a) 0110 0011 $\Leftrightarrow$ 63 en hexa $\Leftrightarrow$ caractère "c" ; 0100 0110 $\Leftrightarrow$ 46 en hexa $\Leftrightarrow$ caractère "F" $\implies$ "cF"

   (b) 0b 1000 1101 1011 0110
2. (a) $(a \texttt{ xor } b) \texttt{ xor } b$

a	b	a xor b	(a xor b) xor b
0	0	0	0
0	1	1	0
1	0	1	1
1	1	0	1

   On observe que $(a \texttt{ xor } b) \texttt{ xor } b = A$

   (b) On peut remarquer que (a xor b) xor b permet de retrouver a, donc si a correspond au message non chiffré et a xor b correspond au message chiffré, un (a xor b) xor b permet donc de retrouver le message non chiffré. Si on appelle m le message non chiffré, m' le message chiffré et k la clé de chiffrement, un m' xor k permettra de retrouver m.

Source parmi d'autres : `https://dav74.github.io/site_nsi_term/`