TP 1 – Cryptage de Vernam

1 Prise en main

Pour crypter un message à l'aide du cryptage de Vernam, on combine à l'aide d'un ou-exclusif (XOR) les bits du message avec ceux d'une clé :

$$c_i = m_i \oplus k_i$$

Le cryptage de Vernam proprement dit utilise une clé aussi longue que le message.

Le fichier `\\labinfo\dfs\cours\CRYSE\TPs\TP1\encrypt.c` implémente une version simplifiée de ce cryptage, avec une clé d'une longueur d'un octet.

Récupérez et compilez ce fichier[1] et testez-le sur quelques fichiers (cryptage et décryptage).

2 Tester la solidité

Cette partie a pour but de vous faire éprouver la solidité de ce cryptage de Vernam simplifié.

1. (Vérification du fonctionnement) Demandez à un collègue de vous envoyer un fichier crypté ainsi que sa clé. Décryptez le message et vérifiez qu'il correspond au fichier d'origine.
2. Demandez à votre collègue de vous envoyer les fichiers cryptés suivants, *sans vous transmettre la clé*, et essayez de les décrypter :
   - Un fichier texte, en français, d'au moins une page A4.
   - Un fichier html.
   - Un fichier zip.
   - Un fichier pdf[2].
3. Demandez maintenant à votre collègue de vous crypter un fichier d'un type courant, mais sans vous dire lequel. Parviendrez-vous à récupérer le fichier original ?

3 Allonger la clé

Améliorez l'implémentation du cryptage de Vernam de la manière suivante :

- La clé peut être de longueur arbitraire ;
- elle sera lue par le programme directement dans un fichier donné en paramètre (à la place de l'actuel paramètre de clé) ;
- si la clé est plus courte que le message, elle sera répétée autant de fois que nécessaire.

Pour chacun des types de fichiers que vous avez récupéré dans la partie précédente, quelle est la longueur maximale de clé qui vous permettrait toujours de casser le cryptage ?

[1] ou, si vous préférez, réimplémentez l'algorithme dans le langage de votre choix !

[2] Vous pouvez bien sûr allonger la liste si d'autres types vous intéressent...

BY-NC-SA distribué sous licence creative common | détails sur www.matthieuamiguet.ch