SOLUTIONS - INTRODUCTION À LA CRYPTOGRAPHIE

Antoine Douteau[1]
[1]Normandie Univ, UNICAEN, ENSICAEN, CNRS, GREYC, 14000 Caen, FRANCE
[1]en thèse dirigée par Adeline Roux-Langlois
antoine.douteau@unicaen.fr

GREYC
Laboratoire de recherche en sciences du numérique

Informations

Si vous comparez les définitions du chiffrement de Vigenère (et César avec les clés étant des lettres) entre mes activités et d'autres activités différentes vous pouvez voir que j'ai modifié en considérant que l'on considérant la position de chaque lettre comme étant le décalage. Dans le cas générale, on ne considère pas la "position" mais bien la "position -1".
J'ai préféré ça par simplicité d'explication.
Pour la partie affine, je n'explique pas du tout que l'on doit choisir la première partie de la clé comme étant premier avec 26 car certaines cursus de collège ne savent pas encore ce que c'est.

Chiffrement de César

A vous de jouer : De tête ou utilisant les outils à disposition, déchiffrez les différents messages ci-dessous :

1. *GBDJMF MB DSZQUPHSBQIJF* pour une clé valant 1,
2. *H'YG AMKNPGQ* pour une clé valant -2,
3. *LKZK JK RG YIOKTIK* pour une clé valant *F* (quand la clé est une lettre, on cherche la position de la lettre avant d'additionner cette valeur).

Solutions

1. *FACILE LA CRYPTOGRAPHIE*
2. *J'AI COMPRIS*
3. *FETE DE LA SCIENCE*

Analyse de fréquence

A vous de jouer : De tête ou utilisant les outils à disposition, déchiffrez le message ci-dessous :

VK MEBSYCSDO OCD EX FSVKSX NOPKED WKSC EXO ZOBCYXXO WKV SXDOXDSYXXOO X'K AEO NOC NOPKEDC.

Solutions

La lettre la plus fréquente est la lettre O avec 12 occurences. On suppose alors que E qui est la lettre la plus fréquente dans l'alphabet française est alors chiffré par la lettre O, on applique alors le même décalage ($+10$) sur toutes les autres lettres. On obtient alors :
LA CURIOSITE EST UN VILAIN DEFAUT MAIS UNE PERSONNE MAL INTENTIONNEE N'A QUE DES DEFAUTS

Chiffrement de Vigenère

A vous de jouer : De tête ou utilisant les outils à disposition, déchiffrez les différents messages ci-dessous :

1. *LBFRXJ* pour une clé valant *FACILE*,
2. *FZIXSJQ GBZD HSFTJ* pour une clé valant *SUPER CLE*,
3. Faites vos propres exemples entre vous.

Solutions

1. *FACILE*
2. *MESSAGE BIEN CACHE*

Chiffrement affine

A vous de jouer : De tête ou utilisant une calculatrice :

- Déchiffrez le message *TVQFS EJGGJDJMF* pour une clé valant $(1, 1)$.
- Chiffrez le message *BAOBAB* pour une clé valant $(5, 6)$. Donnez un autre couple (**clair, clé**) donnant le même **chiffré** ?

Solutions

- *SUPER DIFFICILE*,
- *LGYLGL*. D'autres couples donnant le même chiffré, on essaie simplement de déchiffrer *LGYLGL* pour d'autres valeurs de clés exemple : (*MTZMTM*,(3,1)).

Normandie Université
UNICAEN
ENSI CAEN ÉCOLE PUBLIQUE D'INGÉNIEURS CENTRE DE RECHERCHE
cnrs