DAHAN Gabriel
COHEN Sacha

I. Chiffrement de César

Le type de chiffrement suit une logique précise, il est donc facile de déchiffrer le message : “RENDEZ VOUS CE SOIR AU CAFE DE LA GARE LE SIGNE DE RECONNAISSANCE SERA UN PARAPLUIE BLEU”.

II. Chiffrement monoalphabetique

1. Ce procédé paraît plus sûr que le chiffrement de César car ce dernier suit une logique bien précise. Par conséquent, le déchiffrement est facile, même à la main. Le chiffrement monoalphabétique aussi, mais sa permutation est choisie aléatoirement, il est donc bien plus compliqué de déchiffrer un texte car il faudrait tester toutes les combinaisons possibles.

2. $\frac{26!}{60\times60\times24} \simeq 4.67 \times 10^{21}$ et $\frac{26!}{60\times60\times24\times365} \simeq 1.28 \times 10^{19}$

Ainsi, il faudrait environ 4.67×10^{21} jours soit 1.28×10^{19} années afin de tester toutes les combinaisons possibles dans le but de déchiffrer un message chiffré avec cette méthode. Ceci correspond donc à la durée maximale nécessaire au déchiffrement.

III. Cryptanalyse

Par lecture graphique, la fréquence d’apparition de la lettre ‘e’ dans la langue française est de 17.39%. De plus, encore par lecture graphique, la fréquence d’apparition de la lettre ‘o’ dans ce message est d’environ 17%. On peut ainsi conjecturer que toutes les lettres ‘e’ ont été transformées par des ‘o’ lors du chiffrement.