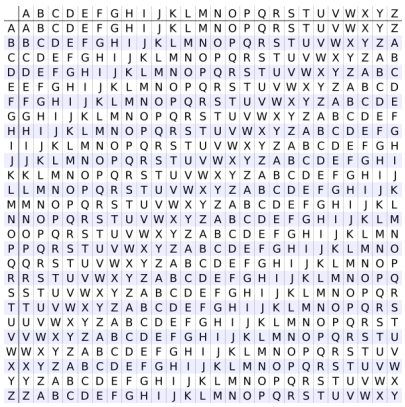
Exercice 1

Le chiffrement de César est une technique de chiffrement qui consiste à décaler le code ASCII de chaque caractère du message d'un nombre fixé.

1. Quel est le chiffrement du message "rendezvousaminuitdouze" si on décale de 12 ?
2. Quel message correspond au chiffré "exitkmbxewxiyngwnkxktxqtvmxfxgmwxnqaxnkxl" ?

Exercice 2

Dans le chiffre de Vigenère, on chiffre la première lettre du message en utilisant la première lettre de la clé. Pour cela, on choisit la colonne correspondant à la lettre du message et la ligne correspondant à la lettre de la clé ; on trouve la lettre chiffrée à l'intersection de cette colonne et de cette ligne. Pour la lettre suivante du message, on utilise la lettre suivante dans la clé, la clé étant répétée autant que nécessaire.



1. On choisit la clé ORANGE. Compléter le chiffrement du message suivant :

Message en clair	A	T	T	A	Q	U	E	A	L	A	U	B	E
Message chiffré	O	K	.	.	.	.	.	.	.	.	.	.	.

2. Déchiffrer VHLKSLBYVEJSNXI avec la clé ROUGE.

Exercice 3

Si $a = a_n \cdots a_0$ et $b = b_n \cdots b_0$ sont des nombres sur $n+1$ bits, on appelle *XOR bit-à-bit* le nombre $a \oplus b = (a_n \oplus b_n) \cdots (a_0 \oplus b_0)$, où $\oplus$ désigne le *ou-exclusif* et est défini comme suit : $(a_i \oplus b_i) = 1$ si et seulement si $a_i \neq b_i$.

1. Que vaut $(10011010)_2 \oplus (11110101)_2$? Écrire ce nombre en binaire puis en hexadécimal.
2. Le chiffrement **XOR** du message m avec la clé k est le message n dont le i-ème caractère est obtenu par $n[i] = m[i] \oplus k[i \bmod |k|]$. Donner le chiffrement **XOR** de "Allo Ali" avec la clé "yes", sachant que le code hexadécimal de `' '` est 20, de `'a'` est 61 et de `'A'` est 41.
3. Connaissant $a \oplus b$ et a, comment retrouver b ? En déduire le moyen de déchiffrer.

Exercice 4

Connaissant la clé publique $(n = 15, e = 3)$ de ce cryptogramme RSA sur 4 bits en decimal : `5 0 4 6 12 1`,

1. calculer p et q (par tous les moyens à disposition) ;
2. calculer la clé secrète d ;
3. déchiffrer le cryptogramme, sachant que le code hexadécimal de `'a'` est 61, de `'A'` est 41, et de `'1'` est 31.