Travaux Dirigés [série n°3] – partie 1

Exercice 1: Le carré de Polybe

Le carré de Polybe est un outil de chiffrement qui permet de coder des messages en remplaçant chaque lettre par une paire de chiffres. Il a été inventé par le philosophe grec Polybe au 2ème siècle avant J.-C.
Le carré de Polybe est formé d'une grille carrée dans laquelle les lettres de l'alphabet sont disposées. Cette grille est généralement de dimension 5x5, à l'exception de la lettre J qui est souvent omise car elle était rarement utilisée en latin à l'époque de Polybe. Les lettres sont placées dans la grille en commençant par la première ligne et en remplissant chaque colonne avant de passer à la suivante.
Pour chiffrer un message à l'aide du carré de Polybe, chaque lettre est remplacée par une paire de chiffres correspondant à ses coordonnées dans la grille. Par exemple, la lettre "A" est remplacée par "11", la lettre "B" par "12", la lettre "C" par "13", et ainsi de suite.
Le carré de Polybe est un chiffrement relativement simple et facile à comprendre, mais il présente des vulnérabilités à certaines attaques cryptographiques, telles que l'analyse fréquentielle. Par conséquent, il est souvent utilisé en combinaison avec d'autres techniques de chiffrement pour renforcer sa sécurité.

- **Chiffrement**

Chiffrez **à la main** le texte suivant avec le carré de Polybe (sans mot-clef) : L'homme est un ange déchu qui se souvient du ciel.

- **Déchiffrement**

Déchiffrez **à la main** le texte suivant avec le carré de Polybe en utilisant le mot-clef "Blaise Pascal» :
122115 141221 412321 214521 44412 112242 123211 521152 213232 115144 125144 114153 521252 544131 421

Exercice 2: Le chiffre Playfair

Le chiffre Playfair est un système de chiffrement par substitution qui a été inventé par le scientifique britannique Charles Wheatstone en 1854, et qui a été perfectionné et popularisé par son compatriote Sir Frederick Playfair.
Le chiffre Playfair utilise une grille de 5x5 lettres pour encoder des messages. Cette grille est remplie avec les lettres de l'alphabet (à l'exception de la lettre "J", qui est généralement remplacée par la lettre "I") dans un ordre spécifique, déterminé par une clé choisie par l'utilisateur. Cette clé peut être n'importe quelle combinaison de lettres, mais elle doit être utilisée de manière cohérente par l'expéditeur et le destinataire du message.
Le chiffrement est effectué en divisant le message original en paires de lettres (ou en ajoutant une lettre supplémentaire si le nombre total de lettres est impair), puis en appliquant une série de règles pour remplacer chaque paire de lettres par une paire de lettres chiffrées.
Le processus de chiffrement implique les étapes suivantes :

1. Si deux lettres identiques apparaissent dans la même paire, ajoutez une lettre supplémentaire (généralement la lettre "X") entre elles pour les séparer.
2. Trouvez la position de chaque lettre de la paire dans la grille de chiffrement.
3. Si les deux lettres de la paire se trouvent sur la même ligne de la grille, remplacez-les par les deux lettres qui se trouvent immédiatement à leur droite, en bouclant autour de la ligne si nécessaire.
4. Si les deux lettres de la paire se trouvent sur la même colonne de la grille, remplacez-les par les deux lettres qui se trouvent immédiatement en dessous, en bouclant autour de la colonne si nécessaire.
5. Si les deux lettres de la paire ne sont ni sur la même ligne ni sur la même colonne, remplacez-les par les deux lettres qui se trouvent aux coins opposés du rectangle formé par leurs positions dans la grille.

Le message chiffré est obtenu en combinant toutes les paires de lettres chiffrées, dans l'ordre dans lequel elles apparaissent.
Le chiffre Playfair était considéré comme un chiffrement relativement sûr pour son époque, mais il a depuis été largement cassé à l'aide de techniques cryptographiques modernes.

- **Chiffrement**

Chiffrez **à la main** le texte suivant en Playfair avec la clef "Charles Baudelaire" :
Souvent pour s'amuser, les hommes d'équipage Prennent des albatros, vastes oiseaux des mers.

- **Déchiffrement**

Déchiffrez **à la main** le texte suivant en Playfair avec la clef "Charles Baudelaire":
PDFEE JTSMV FMBQC DMVEH PNORF OPOBE STPXB ODCSM HXJCB ICKBV BHMVB DLCSB OXSJJ HSBCO UCEH

Exercice 3: Le chiffre de Vigenère

Le chiffre de Vigenère est un système de chiffrement par substitution poly alphabétique inventé par le cryptographe français Blaise de Vigenère au 16ème siècle. Il est considéré comme l'un des premiers exemples de chiffrement poly alphabétique, qui utilise plusieurs alphabets pour chiffrer un même message. Le chiffre de Vigenère est basé sur une clé secrète, qui est une série de lettres qui déterminent la transformation à appliquer sur chaque lettre du message original. La clé est répétée autant de fois que nécessaire pour avoir une longueur égale à celle du message original. Ainsi, chaque lettre du message original est chiffrée avec une lettre différente de la clé.

Le processus de chiffrement implique les étapes suivantes :

1. Choisir une clé secrète qui doit être connue de l'expéditeur et du destinataire du message.
2. Répéter la clé autant de fois que nécessaire pour avoir une longueur égale à celle du message à chiffrer.
3. Assigner un nombre à chaque lettre du message original, en utilisant par exemple la position de la lettre dans l'alphabet (A = 1, B = 2, C = 3, etc.).
4. Utiliser la clé pour générer une série de nombres qui seront utilisés comme décalage pour chiffrer chaque lettre du message original. Pour chaque lettre, le chiffrement est obtenu en ajoutant le nombre correspondant de la clé à celui de la lettre du message original, en prenant en compte les cycles de l'alphabet. Par exemple, si la lettre "A" est chiffrée avec la lettre "D" de la clé, la lettre chiffrée sera la lettre "D" de l'alphabet, soit la quatrième lettre.
5. Reconstituer le message chiffré en remplaçant chaque nombre chiffré par la lettre correspondante.

Le chiffre de Vigenère est considéré comme un chiffrement relativement sûr pour son époque, car il utilise une clé secrète relativement longue et ne crée pas de motifs répétitifs dans le message chiffré. Toutefois, il peut être cassé à l'aide de techniques cryptographiques modernes si la clé est faible ou si le message original est suffisamment long pour permettre l'analyse statistique des fréquences de lettres.

- **Chiffrement**

Chiffrez **à la main** le texte suivant avec le chiffre de Vigenère en utilisant le mot-clef "Jeanne-Marie":
Jeanne-Marie a des mains fortes, Mains sombres que l'été tanna

- **Déchiffrement**

Déchiffrez **à la main** le texte suivant avec le chiffre de Vigenère en utilisant le mot-clef "Jeanne-Marie":
VEIAF TMLVA GXQMR QIEMR QRBQO EGIES FVXLI DRFQM IEAHN NUNAE

- **Vigenère sans clef secrète commune**

Le chiffre de Vigenère tel que décrit ci-dessus exige, comme presque la totalité des systèmes de chiffrement, que les deux correspondants connaissent une clef secrète commune. Il est cependant possible, moyennant trois envois de message au lieu d'un, de se passer de clef commune. Tentez de trouver la manière de faire...

Exercice 4 :

Donner le chiffré du message «the big bang theory» en utilisant les systèmes de chiffrement suivants :
a) César
b) Chiffrement mono-alphabétique à clé (clé : TELECOM)
c) Chiffrement par transposition à clé (clé : TELECOM)
d) Affine y= ax+b (mod26), clé :(a, b) = (17,1). Quelle est la clé utilisée si A est chiffré par G et E est chiffré par A ?

On donne la table de multiplication modulo26 :

×	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
2	4	6	8	10	12	14	16	18	20	22	24	0	2	4	6	8	10	12	14	16	18	20	22	24
3	6	9	12	15	18	21	24	1	4	7	10	13	16	19	22	25	2	5	8	11	14	17	20	23
4	8	12	16	20	24	2	6	10	14	18	22	0	4	8	12	16	20	24	2	6	10	14	18	22
5	10	15	20	25	4	9	14	19	24	3	8	13	18	23	2	7	12	17	22	1	6	11	16	21
6	12	18	24	4	10	16	22	2	8	14	20	0	6	12	18	24	4	10	16	22	2	8	14	20
7	14	21	2	9	16	23	4	11	18	25	6	13	20	1	8	15	22	3	10	17	24	5	12	19
8	16	24	6	14	22	4	12	20	2	10	18	0	8	16	24	6	14	22	4	12	20	2	10	18
9	18	1	10	19	2	11	20	3	12	21	4	13	22	5	14	23	6	15	24	7	16	25	8	17
10	20	4	14	24	8	18	2	12	22	6	16	0	10	20	4	14	24	8	18	2	12	22	6	16
11	22	7	18	3	14	25	10	21	6	17	2	13	24	9	20	5	16	1	12	23	8	19	4	15
12	24	10	22	8	20	6	18	4	16	2	14	0	12	24	10	22	8	20	6	18	4	16	2	14
13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13
14	2	16	4	18	6	20	8	22	10	24	12	0	14	2	16	4	18	6	20	8	22	10	24	12
15	4	19	8	23	12	1	16	5	20	9	24	13	2	17	6	21	10	25	14	3	18	7	22	11
16	6	22	12	2	18	8	24	14	4	20	10	0	16	6	22	12	2	18	8	24	14	4	20	10
17	8	25	16	7	24	15	6	23	14	5	22	13	4	21	12	3	20	11	2	19	10	1	18	9
18	10	2	20	12	4	22	14	6	24	16	8	0	18	10	2	20	12	4	22	14	6	24	16	8
19	12	5	24	17	10	3	22	15	8	1	20	13	6	25	18	11	4	23	16	9	2	21	14	7
20	14	8	2	22	16	10	4	24	18	12	6	0	20	14	8	2	22	16	10	4	24	18	12	6
21	16	11	6	1	22	17	12	7	2	23	18	13	8	3	24	19	14	9	4	25	20	15	10	5
22	18	14	10	6	2	24	20	16	12	8	4	0	22	18	14	10	6	2	24	20	16	12	8	4
23	20	17	14	11	8	5	2	25	22	19	16	13	10	7	4	1	24	21	18	15	12	9	6	3
24	22	20	18	16	14	12	10	8	6	4	2	0	24	22	20	18	16	14	12	10	8	6	4	2
25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1