Master 1ère année
Initiation à la Cryptographie

Travaux Dirigés

Chiffrements « antiques »

Exercice 1 : [César] On considère le chiffrement par décalage de d positions des lettres de l'alphabet. Si $d = 3$, le chiffrement est appelé **Chiffre de César** et ainsi la lettre A devient D, la lettre B devient E, etc ...

1. Chiffrer le message suivant « CESAR VAINCRA ».
2. Déchiffrer le message suivant « DOHDMDFWDHVW ».
3. Quelle est la clé de chiffrement ? Combien en existe-t-il?
4. Donner le pseudo-code de ce chiffrement en utilisant les fonctions CHR (renvoie de la lettre à partir de la valeur ASCII) et ORD (fonction réciproque de CHR).
5. Le chiffrement par décalage de $d = 13$ lettres s'appelle ROT13. Quelle est sa principale propriété?
6. On peut généraliser par une substitution quelconque : on fait correspondre l'alphabet ordonné avec un alphabet permuté. Combien y-a-t-il de possibilités?

Exercice 2 : [**Carré de Polybe**] Le chiffrement est effectué à l'aide d'une matrice indexée par les entiers de 1 à 5 dans laquelle on met les 26 lettres de l'alphabet (W supprimé ou I et J sont dans la même case). Par exemple, on considère la matrice suivante :

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I	J
3	K	L	M	N	O
4	P	Q	R	S	T
5	U	V	X	Y	Z

Chaque lettre du message remplacée par le couple $(i; j)$ où $i = n^\circ$ de ligne et $j = n^\circ$ de colonne.

1. Chiffrer le message suivant « CARRE DE Polybe ».
2. Déchiffrer le message suivant « 232444453543241534224315 13 ».
3. Quelle est la clé de chiffrement ? Comment en changer? Combien en existe-t-il? Donner un exemple.
4. Quels sont les avantages et les défauts de ce chiffrement du point de vue transmission et sécurité (Cryptanalyse possible)?

Exercice 3 : [Permutation] On considère le chiffrement par une écriture en dent de scie : on prend une lettre sur deux du mot puis le reste.

1. Chiffrer le message suivant « MASTERLIMOGES ».
2. Quelle est la permutation qui transforme le message en son chiffré pour l'exemple précédent?
3. Pour un message de m lettres, combien existe-t-il de chiffrements par permutation possibles?
4. Donner le pseudo-code de ce chiffrement en supposant que le message est considéré comme une chaîne de caractères indexée.
5. Trouver une généralisation [Chiffrement par transposition].

Exercice 4 : [**Vigenère**, ≈ 1550] Chaque lettre du message est déplacé dans l'alphabet selon un vecteur décalage de longueur k, qui est utilisé comme clef (A=1). Ce vecteur est répété si nécessaire.

1. Si $k = 1$, quel chiffrement retrouve-t-on ?
2. Chiffrer le message VIGENERE avec le vecteur-clef MASTER.
3. Déchiffrer "PNKOWALZDYBAWHXJC" en utilisant le vecteur-clef VIRUS.
4. Si k est de taille au moins égale à la longueur du message, quel chiffrement retrouve-t-on? Quels conseils d'utilisation peut-on ajouter?

Exercice 5 : [**Playfair**, 1854] Le chiffre de Playfair utilise un tableau de 5x5 lettres, contenant un mot clé ou une phrase. La mémorisation du mot clé et de 4 règles faciles à suivre suffisait pour utiliser ce chiffrement.

Pour construire le tableau, on devait d'abord le remplir avec les lettres du mot clé (en ignorant les doublons), puis le compléter avec les autres lettres de l'alphabet dans l'ordre (soit en omettant la lettre W peu courante, soit en occupant une même case pour les lettres I et J suivant les versions). Le mot clé peut être écrit en ligne, en colonne ou même en spirale (on choisira la version ligne).

Pour chiffrer un message, il faut prendre les lettres 2 par 2 et appliquer les règles suivantes en fonction de la position des lettres dans la table :

- si les 2 lettres sont identiques (ou s'il n'en reste qu'une) mettre un 'X' après la première lettre. Chiffrer la nouvelle paire ainsi constituée et continuer avec la suivante.
- si les lettres se trouvent sur la même ligne de la table, il faut les remplacer par celles se trouvant immédiatement à leur droite (en bouclant sur la gauche si le bord est atteint),
- si les lettres apparaissent sur la même colonne, les remplacer par celles qui sont juste en dessous (en bouclant par le haut si le bas de la table est atteint),
- sinon, remplacer les lettres par celles se trouvant sur la même ligne, mais dans le coin opposé du rectangle défini par la paire originale.

1. Chiffrer le message BIENVENUE avec le mot-clef PLAYFAIR.
2. Déchiffrer NFEXOKCTFTTOSEQSGBIOQO avec le mot-clef ALPHABET.