TD - Chiffrement XOR

Sources : https://pixees.fr/informatiquelycee/n_site/nsi_term_archi_secu.html
Pour controler éventuellement ses résultats : https://www.dcode.fr/chiffre-xor

Le OU exclusif (XOR) est une méthode de cryptographie qui consiste à chiffrer un message en binaire avec une « **clé de chiffrement** » répétée par une multiplication par OU Exclusif.

C'est une méthode de **chiffrement symétrique**, la **clé** utilisée doit être **partagée** et connue des participants à l'échange.

Table de vérité "XOR"		
E1	E2	S
0	0	0
0	1	1
1	0	1
1	1	0

La méthode la plus utilisée en matière de chiffrement symétrique se nomme **AES** (Advanced Encryption Standard). Cette méthode utilise une technique de chiffrement plus élaborée que celle que l'on va voir avec le XOR, mais les grands principes restent identiques.

Le cryptage **XOR** utilise l'opérateur binaire **XOR** (**Ou Exclusif**, symbolisé par ⊕) et comme opérandes le texte clair et la clé (préalablement encodés en binaire).

Le déchiffrement **XOR** (decryptage **XOR**) est identique au chiffrement car l'opération **XOR** est symétrique (inverse **XOR** = **XOR**). Non seulement la même clé est utilisé pour chiffrer et déchiffrer, mais le même algorithme également.

Le principe.

L'opération logique XOR (pour eXclusive OR), ou exclusif, est un opérateur logique (au même titre que AND, OR, etc) de **l'algèbre de Boole**. Cet opérateur logique va comparer deux bits et produire un bit de retour. Ce bit sera égal à 1 si les deux bits comparés sont différents, 0 s'ils sont semblables.

Le chiffrement XOR peut être utilisé dans les méthodes de **chiffrements symétriques.** L'opérateur XOR est donc appliqué bit à bit entre le texte à chiffrer et la clé que nous choisissons.

Liens utiles : http://sebsauvage.net/comprendre/ascii/index.html
https://sebastienguillon.com/test/javascript/convertisseur.html

A vous 1.

Prenez donc le mot "xor" pour le chiffrer avec la clé partagée "cle".

a) Transformez, à la main, en utilisant les liens indiquez ci-dessus si nécessaire, le texte à chiffrer et la « clé de chiffrement » en binaire. Pour cela utilisez la table ASCII.

"xor" : 1111000 1101111 1110010

"cle" : 1100011 1101100 1100101

b) Comparez bit à bit le texte à chiffrer et la « clé de chiffrement » avec l'opérateur xor (*voir table de vérité*). Vous obtenez le message chiffré en binaire tel qu'il « *voyage sur la toile* ».

xor	1	1	1	1	0	0	0		1	1	0	1	1	1	1	1	1	1	0	0	1	0	
cle	1	1	0	0	0	1	1		1	1	0	1	1	0	0	1	1	0	0	1	0	1	
Chiffré binaire	0	0	1	1	0	1	1		0	0	0	0	0	1	1	0	0	1	0	1	1	1	

c) A la réception du message, on le déchiffre en appliquant toujours xor entre le message reçu et la clé, on traduit le binaire en caractère par lot d'un octet.

Remarque : la fonction XOR est commutative (a XOR b = b XOR a), comme une multiplication.

M chiffré	0	0	1	1	0	1	1		0	0	0	0	0	1	1		0	0	1	0	1	1	1
clé	1	1	0	0	0	1	1		1	1	0	1	1	0	0		1	1	0	0	1	0	1
⊕	1	1	1	1	0	0	0		1	1	0	1	1	1	1		1	1	1	0	0	1	0
Base 10	120								111								114						
caractères	x								o								r						

d) Vérifiez votre résultat : vous devez retrouver le texte initial après déchiffrement.

On trouve “xor”

A vous 2.

Procédez de même pour chiffrer le mot « bonjour » avec la clé de chiffrement « cle ».

Içi la clé de chiffrement est plus courte que le message à chiffrer, on concatène autant que nécessaire les caractères de la clé de chiffrement à elle-même pour obtenir une chaine de la même longueur que le texte à chiffrer.

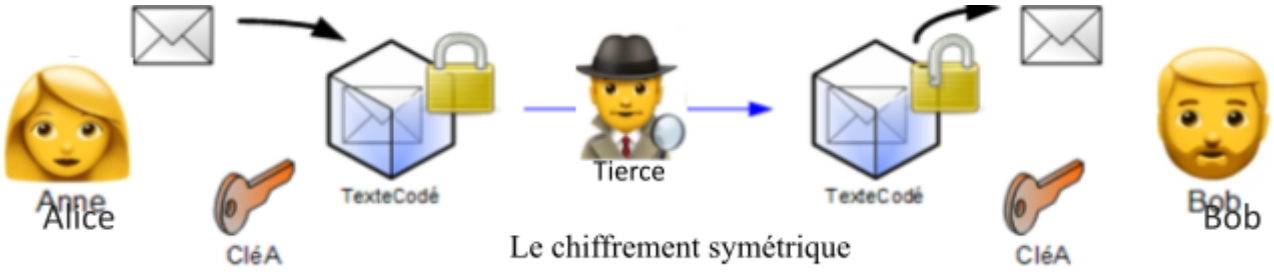
Mot à chiffrer : bonjour
Clé de chiffrement : cleclec

bonjour	1	1	0	0	0	1	0		1	1	0	1	1	1	1		0	1	1	0	1	1	1		1	1	0	1	0	1	0
	1	1	0	1	1	1	1		1	1	1	0	1	0	1		1	1	1	0	1	0	1								
cleclec	1	1	0	0	0	1	1		1	1	0	1	1	0	0		1	1	0	0	1	0	1		1	1	0	0	0	1	1
	1	1	0	1	1	0	0		1	1	0	0	1	0	1		1	1	0	0	0	1	1								
Chiffré binaire	0	0	0	0	0	0	1		0	0	0	0	0	1	1		1	0	1	0	0	0	1		0	0	0	1	0	0	1
	0	0	0	0	0	1	1		0	0	1	0	0	0	0		0	0	1	0	1	1	0								

Plus la clé de chiffrement est courte, plus il est facile de la « casser » et plus les attaques auront de chance d’aboutir !
Il faut pour ce système que les deux interlocuteurs échangent et la clé de chiffrement et le message chiffré.
Il faut éviter d’utiliser le même canal pour transmettre ces deux éléments !
Il faut que la clé de chiffrement soit transmise de façon sécurisée si l’on ne veut pas qu’elle soit interceptée !

A vous 3.

A faire par groupe de trois : Alice et Bob, qui ont des messages à échanger, et Tierce l’intermédiaire (l’espion) qui va intercepter le message.



Le chiffrement symétrique

Alice et Bob se mettent d'accord sur une clé de chiffrement/déchiffrement (choisissez un mot qui jouera le rôle de clé, ce mot, la « clé de chiffrement » doit rester secret entre Alice et Bob).
Celui, celle, d’entre vous qui joue le rôle d’Alice écrit un message à faire parvenir à Bob. Alice chiffre le message et note le résultat du chiffrement en binaire, sur une feuille.

Alice donne cette feuille à Tierce, une ou un camarade, (qui ne connait pas la clé, ce camarade joue le rôle de l'espion) qui est chargé(e) de la transmettre à Bob. Tierce recopie le message avant de le transmettre à Bob.
Tierce devra essayer de trouver le message envoyé par Alice à Bob (sans la clé de chiffrement), donc de le décrypter.
Bob devra déchiffrer le message à l'aide de la clé.

Vous pouvez utiliser le site cité ci-dessous afin d'assurer les passages :

texte code ASCII binaire et code ASCII binaire texte.

Pour traduire votre message en binaire :
https://www.rapidtables.com/convert/number/ascii-to-binary.html

Le problème avec le chiffrement symétrique, c'est qu'il est nécessaire pour Alice et Bob de se mettre d'accord à l'avance sur la clé qui sera utilisée lors des échanges. Le chiffrement asymétrique permet d'éviter ce problème.

Pour aller plus loin.

Les plus avancés codent l'algorihtme de codage xor.