W1 - Rattrapages

W-RAT-010

Enigma

Rattrapages rush 5

1.1

Enigma

delivery method: enigma on Github
language: PHP

- The totality of your source files, except all useless files (binary, temp files, obj files,...), must be included in your delivery.
- All the bonus files (including a potential specific Makefile) should be in a directory named *bonus*.
- Error messages have to be written on the error output, and the program should then exit with the 84 error code (0 if there is no error).

Introduction

Enigma est une machine electromecanique portable servant au chiffrement et au dechiffrement de l'information. Elle fut inventee par l'Allemand Arthur Scherbius, reprenant un brevet du Neerlandais Hugo Koch, datant de 1919. Enigma fut utilisée principalement par les Allemands (Die Chiffriermaschine Enigma) pendant la Seconde Guerre mondiale.
Son utilisation la plus célèbre fut celle faite par l'Allemagne nazie et ses alliés, avant et pendant la Seconde Guerre mondiale, la machine étant réputée inviolable selon ses utilisateurs. Néanmoins un nombre important de messages Enigma ont pu être décryptés près de sept ans avant la guerre.
Votre objectif est de mettre au point votre enigma pour correspondre avec vos alliés sans craindre que vos communications ne soient interceptées par l'ennemi.

Openclassroom (https://openclassrooms.com/courses/les-premiers-algorithmes-de-chiffrement)

Sujet

Créer une page **enigma.php** qui permet à l'utilisateur de crypter ou décrypter une phrase en utilisant un des chiffrements suivants.

Notions

- Chiffrement

Le chiffre de César (8 pts)

Introduction

Le chiffre de César(ou chiffrement par décalage) est un algorithme de chiffrement très simple que Jules César utilisait pour chiffrer certains messages qu'il envoyait. Il s'agit d'une substitution mono-alphabétiquecar il remplace chaque lettre par une autre lettre de l'alphabet, toujours la même.

Principe de chiffrement

Ce cryptosystème consiste à remplacer chaque lettre du texte clair, par une lettre différente, située x lettres après dans l'alphabet, où x est la valeur de la clé passée en argument.

Tâche

Faites-en sorte qu'un romain puisse, en choisissant une clé entre 1 et 26, chiffrer et déchiffrer des messages afin que les irréductibles gaulois ne tombent jamais dessus !

Chiffre de Vigenère (6 pts)

Introduction

Le chiffre de Vigenère est un algorithme de chiffrement établi par le cryptographe français Blaise de Vigenère. Ce cryptosystème est de type poly-alphabétique, en opposition au mono-alphabétique, que nous avons déjà vu, c'est-à-dire qu'il consiste à changer une lettre par une autre, mais cette dernière n'est pas toujours là même. Cela permet une plus grande sécurité. Cet algorithme utilise une clé, ici sous la forme d'un mot ou d'une phrase, que vous choisirez. Plus l'expression sera longue, plus le cryptogramme sera sécurisé. Un autre outil indispensable pour chiffrer un message avec cette méthode est la table de Vigenère :

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

Principe de chiffrement

Le chiffrement se déroule en deux étapes. Dans un premier temps, on choisit un message, par exemple « Bonjour les zéros ! » et une clé, par exemple «Zozor». Bref, commencez par écrire votre message sur le papier.

BONJOUR LES ZÉROS !

En-dessous de chaque lettre, écrivez chaque lettre de la clé, et répétez le motif autant de fois que nécessaire. Ce qui donne, dans notre exemple :

BONJOUR LES ZÉROS !
ZOZORZO ZOR ZOZOR !

Dans un second temps, sachez que le message correspond aux colonnes de la table, et la clé aux lignes. Pour chaque lettre du message, la lettre chiffrée correspond au croisement entre la colonne correspondant à la lettre du message et la ligne correspondant à la lettre de la clé. Par exemple, la lettre qui est au croisement entre la colonne 'B' et la ligne 'Z' est 'A'. La première lettre du message chiffrée est donc 'A'. Si l'on continue, cela donne au final :

BONJOUR LES ZÉROS !
ZOZORZO ZOR ZOZOR !
ACMXFTF KSJ YSQCJ !

Le message chiffré est donc « ACMXFTF KSJ YSQCJ ! ». Bien qu'à première vue le message semble sécurisé, il est évident que la clé **ZOZOR** est trop courte et, de manière générale, le chiffre de Vigenère n'est pas un algorithme très sécurisé. Il est donc facile de casser le cryptogramme, du moins pour les personnes un peu expérimentées dans ce domaine.

Principe de déchiffrement

Pour déchiffrer le texte chiffré, on prend de nouveau un bout de papier, et on note le message codé, suivi du motif de la clé répété autant de fois que nécessaire, ce qui donne :

ACMXFTF KSJ YSQCJ !
ZOZORZO ZOR ZOZOR !

Ensuite, on fait l'inverse que lors du chiffrement. On va vers la ligne correspondant à la lettre actuelle de la clé, et on cherche la lettre actuelle du texte chiffré dans cette ligne. La lettre en clair correspond à la colonne correspondante. Ce qui donne, dans notre cas :

ACMXFTF KSJ YSQCJ !
ZOZORZO ZOR ZOZOR !
BONJOUR LES ZEROS !

On retrouve donc notre message de départ !

Tâche

Faites-en sorte qu'en rentrant une clé, l'utilisateur puis chiffrer et déchiffre ses messages.

Le masque jetable (6 pts)

Introduction

Le masque jetable est un cryptosystème établi par l'ingénieur Gilbert Vernam. En théorie, cet algorithme de chiffrement est réputé comme étant le seul à être impossible à casser.

Principe de chiffrement

Pour chiffrer un message, on doit prendre une clé, qui doit avoir les caractéristiques suivantes :

- La clé doit avoir un nombre de caractères supérieur ou égal à celui du message ;
- Les caractères de la clé doivent avoir été choisis de manière aléatoire ;
- Chaque clé ne doit être utilisée qu'une seule fois.

Toutes ces propriétés dans le but final de garantir une sécurité optimale. Si elles sont respectées à la lettre, la sécurité garantie est absolue.
Bien, on passe à un exemple concret. Pour ne pas mettre trop de temps à chiffrer le message, nous allons en prendre un de quatre lettres : **ZERO**. Nous tirons ensuite une chaîne de quatre lettres au hasard. Le résultat : **JRVG**. Ceci est la clé. On attribue ensuite une valeur différente à chaque lettre de l'alphabet. Pour faire simple, nous choisissons le même principe que pour le chiffre de César : 'A' vaut 0, 'B' vaut 1, 'C' vaut 2, etc. La suite est semblable au calcul du chiffre de Vigenère : on additionne la valeur de chaque lettre du message avec la valeur de la lettre de la clé correspondante, puis on fait modulo 26. Armez-vous de votre papier et de votre crayon, pour obtenir, normalement, ces résultats :
Z + J = 25 + 9 = 34 - 26 = 8 = I
E + R = 4 + 17 = 21 = V
R + V = 17 + 21 = 38 - 26 = 12 = M
O + G = 14 + 6 = 20 = U
Ce qui nous donne au final, le cryptogramme suivant : **IVMU**.

Principe de déchiffrement

Le déchiffrement s'effectue à peu près de la même manière, mis à part que, cette fois-ci, on soustrait la valeur de la lettre de la clé à la valeur de la lettre du cryptogramme correspondante et que l'on ajoute 26 lorsque le résultat est négatif. Cela nous donne :
I - J = 8 - 9 = -1 + 26 = 25 = Z
V - R = 21 - 17 = 4 = E
M - V = 12 - 21 = -9 + 26 = 17 = R
U - G = 20 - 6 = 14 = O
Et on retrouve bien le message **ZERO** de départ.

Tâche

Faites-en sorte qu'en rentrant une clé, l'utilisateur puis chiffrer et déchiffre ses messages.