TD1 - chiffrements symétriques

September 2022

1 Introduction

Objectif: manipuler les différents concepts d'arithmétique modulaire appliqués au chiffrement César et commencer à réfléchir sur l'implémentation de ce chiffrement pour préparer le TP.
Prérequis:

- connaître les bases de l'arithmétique modulaire
- connaître le fonctionnement des méthodes de chiffrement symétrique vues en cours
- savoir effectuer des additions en binaire

Connaissances à acquérir:

- effectuer des calculs simples (additions, soustractions, multiplication et divisions) sur des ensembles Z/nZ
- appliquer les algorithmes de Polybe, César et Vigenère

Instructions: Réaliser ces exercices en groupes de 3 (maximum).

2 Arithmétique modulaire

2.1 Relation de congruence

Ces congruences sont-elles vraies ?

- $100 \equiv 5$ [5]
- $1024 \equiv 16$ [16]
- $102 \equiv$ -23 [98]
- $49 \equiv 70$ [7]
- $8 + 31 \equiv 7$ [4]

- $305 + 950 \equiv 100$ [200]
- $15472 + 15489 \equiv 1$ [15480]
- $8 * 15 \equiv -1$ [11]
- $10 * 13 \equiv 20$ [11]
- $5^3 \equiv 5$ [3]
- $94^{10} \equiv 1020$ [92]
- $12^{100} \equiv 2$ [11]

2.2 Exponentiations

Calculez les exponentiations suivantes:

- $c \equiv 10^5 \pmod{500}$
- $c \equiv 10^5 \pmod{495}$
- $c \equiv 3^{17} \pmod{26}$
- $c \equiv 4^9 \pmod{48}$
- $c \equiv 9^9 \pmod{79}$
- $c \equiv 2^{11} \pmod{1998}$
- $c \equiv 5^5 \pmod{26}$
- $c \equiv 7^6 \pmod{40}$
- $c \equiv 8^5 \pmod{63}$

3 Chiffrement par substitution

3.1 Polybe

Présentation: le carré de Polybe est une technique de chiffrement par substitution vue pour la première fois en 150 avant J-C. Elle consiste à remplacer les lettres d'un message par des chiffres. Le carré de la figure 1 sert de clé pour le chiffrement et de le déchiffrement du message. L'alphabet français comportant 26 lettres, deux lettres sont associées à la même case.
Le principe: chaque lettre du carré de Polybe possède une coordonnée dans le carré. Le message est chiffré en substituant chacun de ses caractères par sa coordonnée dans le carré. Par exemple, la lettre *H* est remplacée par *23*.

Dans cette exercice il est demandé de chiffrer les messages suivants:

Peste	Raisin	Anniversaire
Effrayant	Osier	Couches
Latex	Fils	Corne

Puis de déchiffrer ceux-ci:

34421424331144154542	131132243433	1323242121421532153344
355444233433	32154343112215	4234454415
3315334535231142	1133442431343515	22333445

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

Figure 1: Carré de Polybe

3.2 César

Présentation: le chiffrement César est un chiffrement par décalage utilisée par Jules César pour ses correspondances secrètes.
Le principe: chaque lettre du message est remplacée par une autre lettre à distance fixe. Par exemple, le A est remplacée par le B, le B pa rle C, *etc.* La clef de cette méthode correspond au décalage de l'alphabet. Dans l'exemple précédent, elle est de 1. Le décalage s'effectue toujours dans le même sens et à la même distance. Lorsque l'on souhaite décaler une lettre de la fin de l'alphabet, on continue de compter le décalage à partir du début de l'alphabet. Par exemple, un décalage de 2 pour encoder la lettre Z donnerait la lettre B.

Décodez le message suivant en vous aidant du tableau de fréquences de chaque lettre:

Pk xktzxk inkf suo. Yax rk zxuzzuox, at nussk yk vxusktk, yky jkad saykzzky xksvroky jk rkmasky ktzxk yky juomzy.

E	21×	23.33%
S	11×	12.22%
R	8×	8.89%
T	8×	8.89%
M	7×	7.78%
O	6×	6.67%
U	5×	5.56%
N	4×	4.44%
I	4×	4.44%
D	3×	3.33%
L	3×	3.33%
P	2×	2.22%
G	2×	2.22%
H	2×	2.22%
Z	1×	1.11%
C	1×	1.11%
X	1×	1.11%
J	1×	1.11%

Figure 2: Fréquence des lettres dans le texte à déchiffrer

4 Chiffrement par bloc

Vous disposez du message et de la clé suivante:

- message: "Jadis, dans un pays lointain"
- clé initiale: "001101001101"

L'objectif est de chiffrer ce message avec un opérateur XOR. Pour cela, nous encoderons chaque lettre du message de la manière suivante:

- j = 0000
- a = 0001
- d = 0010
- i = 0011
- s = 0100
- n = 0101
- u = 0110
- p = 0111

- y = 1000
- l = 1001
- o = 1010
- t = 1011
- espace = 1100
- , = 1101

Vous devrez casser le message en plusieurs blocs de manière à les encoder avec la clé mise à disposition. Pour imiter le processus degénération pseudo-aléatoire de clés de l'algorithme AES tout en le gardant accessible pour un TP papier, nous allons supposer que la clé initiale est modifiée après chaque usage. La nouvelle clé sera la somme de l'ancienne et du binaire *010101010101*.

Lorsque le message est codé, essayez de le décoder avec la même clé et vérifiez votre résultat !

Conseil: si vous êtes en groupe, répartissez vous le travail et décodez chacun un message codé par un autre membre de votre groupe.

5 Automatisation

Proposez un pseudo-code permettant d'automatiser les tâches effectuées dans l'exercice précédent.

Proposez 3 fonctions en pseudo-code pour les tâches suivantes:

- Génération de clés: la fonction prend en paramètre la clé précédemment utilisée et retourne la nouvelle clé.
- Chiffrement de messages: la fonction prend un bloc déchiffré en paramètre et le retourne chiffré.
- Déchiffrement de messages: la fonction prend un bloc chiffré en paramètre et le retourne déchiffré.