Baptiste Cottier
baptiste.cottier@icloud.com
INSA - Hauts de France
21 novembre 2025

TD Initiation à la cryptographie

1 Chiffrement par substitutions - A faire à la main

Exercice 1. Chiffrement par décalage (Chiffrement de César)

1. Chiffrer le message "IL FAUT TUER ASTERIX ET OBELIX" à l'aide du chiffrement par décalage et de la clé $K = 17$

2. Dans la langue française, les lettres les plus fréquentes sont le A (8.4 %) et le E (17.26 %). Sachant que le message suivant est en français, utiliser ces fréquences pour déterminer la clé et en déduire le message initial: "XACTBTHTBQATEPHFJTAPUDGBPIXDCIDGIJTHDXIAPEAJHTUUXRPRTPUXCSTRDBQPIIGTRTHVPJADXH"

Exercice 2. Chiffrement par substitutions

1. Chiffrer le message "IL FAUT TUER ASTERIX ET OBELIX" à l'aide du chiffrement par substitutions et de la clé suivante:

a	b	c	d	e	f	g	h	i	j	k	l	m
J	G	Q	K	U	Y	F	Z	E	N	D	L	B
n	o	p	q	r	s	t	u	v	w	x	y	z
V	R	W	H	O	I	P	C	T	S	M	A	X

2. Est-ce possible pour quelqu'un ne connaissant pas la clé de déchiffer le message suivant "WJOPRCPJPEI" ?

Exercice 3. Chiffrement de Vigenère

1. Chiffrer le message "IL FAUT TUER ASTERIX ET OBELIX" à l'aide du chiffrement de Vigenère et de la clé "GAULOIS"

2. Est-ce possible pour quelqu'un qui ne connait pas la clé de déchiffer le message suivant "ZTCAZJTGEFVRHSEOZKSCEKVROEALVXSXNOVRHTPTIZWVEGVVS" ? Déchiffrez le sachant qu'il a été chiffré avec la clé "OPATRE"

2 Arithmétique

Exercice 4. Euclide et Bezout

- Vérifier que GCD(45,56)=1
- Déterminer u et v tels que $45u + 56v = 1$
- Faire de même avec GCD(2025, 1237).

Exercice 5. Congruences Déterminez la véracité des expressions suivantes :

- $97 \equiv 12 \mod 17$
- $3462 \equiv 11 \mod 17$
- $11 \equiv 3462 \mod 17$
- si $a \equiv b \mod p$, alors $a + b \equiv 2b \mod p$
- si $a \equiv b \mod pq$, alors $a \equiv b \mod p$

Exercice 6. Chiffremenet modulaire

Dans cet exercice une lettre de l'alphabet est chiffrée en prenant son rang ℓ dans l'alphabet et en calculant $p = 5\ell + 2 \mod 26$.

- Chiffrer SECRET
- Calculer $5^{-1} \mod 26$ (*Inverse modulaire de 5, modulo 26*)
- En déduire l'opération de déchiffrement : trouver a et b tels que si $p = 5\ell + 2 \mod 26$, alors $\ell = ap + b \mod 26$.
- Déchiffrer MJSZTU

3 Ordres de grandeur

Exercice 7. Protection de mot de passe

Un système est protégé par un mot de passe. Après un essai infructueux le système attend une seconde avant d'accepter un nouvel essai. Combien de temps, en moyenne, faudra-t-il pour accéder au système dans les cas suivants:

1. Le mot de passe est un des 1 000 prénoms les plus fréquents.
2. Il est composé de 4 chiffres
3. Le mot de passe est un des ≈ 200000 mots que compte la langue française.
4. Le mot de passe est une combinaison de 8 caractères alphanumériques (minuscules, majuscules, chiffres, et 15 signes de ponctuation)

Exercice 8. La Bruteforce

Le facteur de travail d'un algorithme est le nombre d'instructions élémentaires nécessaire à son exécution. La puissance d'une machine est le nombre d'instructions qu'elle exécute par unité de temps. Nous allons estimer la puissance d'un PC actuel à environ 2000 Mips (millions d'instructions par seconde). Le facteur de travail d'un algorithme optimisé pour tester une clé de 128 bits de l'algorithme AES est d'environ 1200 instructions élémentaires. On dispose d'un couple clair/chiffré connu et on désire retrouver la clé utilisée par force brute, c'est-à-dire en testant toutes les clés les unes aprés les autres. Une clé est constituée d'un mot de 128 bits. On suppose que toutes les clés sont équiprobables.

1. En combien de temps une machine de 2000 Mips teste-t-elle une clé ?
2. Combien y a-t-il de clés possibles ? Quel est le nombre moyen de clés à tester avant de trouver la bonne ?
3. A quel temps moyen de calcul cela correspond-il si on suppose qu'un seul PC effectue la recherche ? Si les 1 milliard de PC de l'Internet sont mobilisés à cette tâche ?