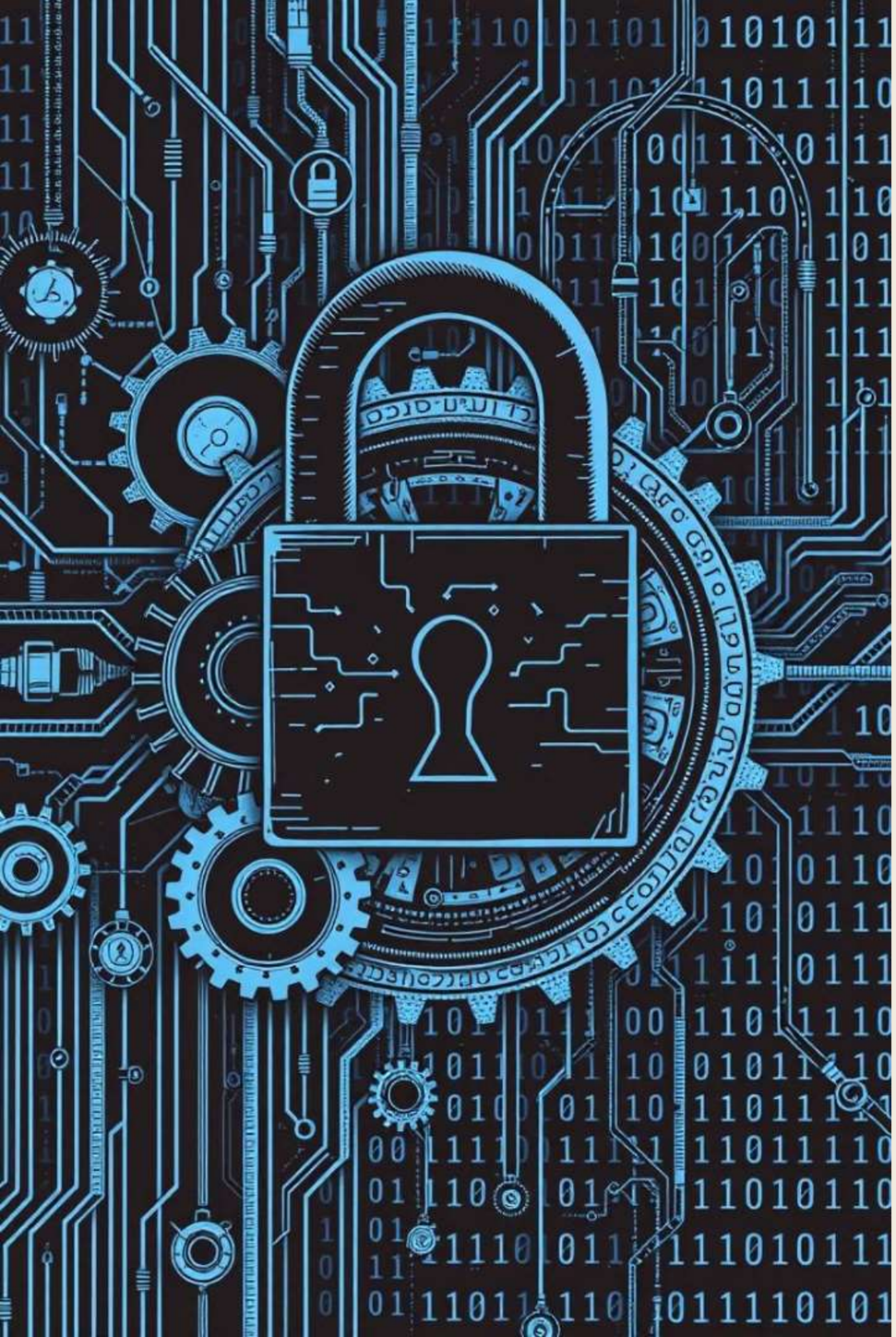
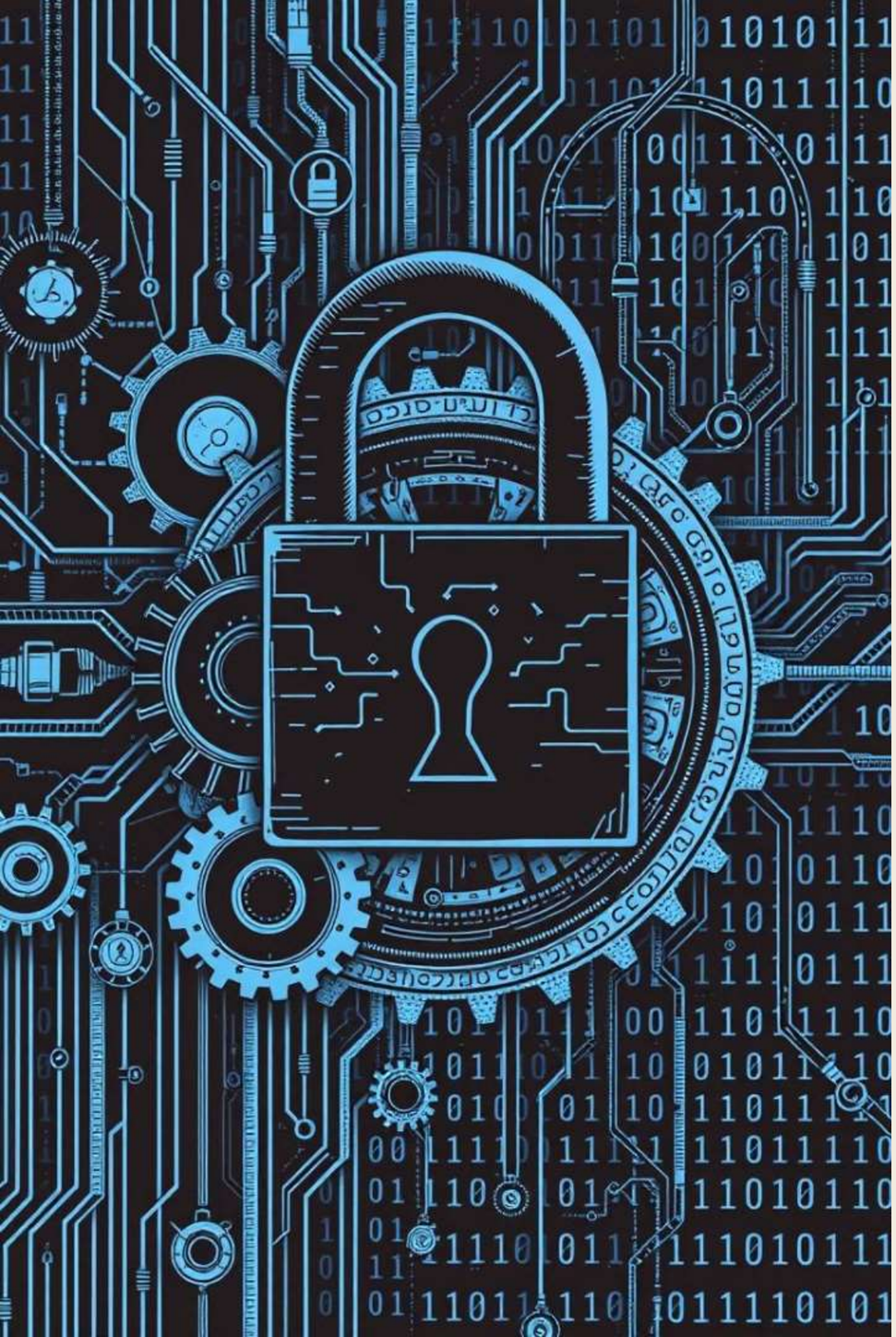


Cours
Introduction à la Sécurité Informatique
ING3 IAA

Bienvenue à ce cours sur la sécurité informatique.
Préparez-vous à explorer des concepts complexes et des technologies révolutionnaires qui sous-tendent la sécurité numérique moderne.

Dr F.Khalifa
Université USTOMB
2024-2025



Introduction à la Sécurité Informatique

Chapitre 2: Cryptographie Classique

1. Introduction
2. Chiffrement de César
3. Chiffrement par substitution mono alphabétique
4. Chiffrement par substitution poly alphabétique
5. Chiffrement de Vigénaire
6. Chiffrement de HILL
7. Chiffrement affine

Dr F.Khalifa

Université USTOMB

2024-2025

Chapitre 2: Cryptographie Classique

Introduction

Un expéditeur (Alice) veut envoyer un message à un destinataire (Bob)en évitant les oreilles indiscrète et/ou les attaques malveillantes des intrus.
Pour cela Alice se met d'accord avec Bob sur un cryptosystéme qu'ils vont utiliser. Ce choix n'a pas besoin d'être secret.

L'information qu'Alice souhaite transmettre à Bob est le texte clair.
Le processus de transformation d'un message, M, pour qu'il devient incompréhensible est appelé le chiffrement ou la codage.
On génère ainsi un message chiffré, C, obtenu grâce à une fonction de chiffrement, E, par :
$C = E(M)$.
Le processus de reconstruction du message clair à partir du message chiffré est appelé le déchiffrement ou décodage et utilise une fonction de déchiffrement, D. $D(C) = D(E(M)) = M$

Chapitre 2: Cryptographie Classique

Vocabulaire de base dans la cryptographie

Texte en clair : c'est le message à protéger (à chiffrer).

Texte chiffré : (cryptogramme) , c'est le résultat du chiffrement du texte en clair.

Chiffrement : c'est la méthode ou l'algorithme utilisé pour transformer un texte en clair en texte chiffré.

Déchiffrement : c'est la méthode ou l'algorithme utilisé pour transformer un texte chiffré en texte en clair.

Clé : c'est le secret partagé utilisé pour chiffrer le texte en clair en texte chiffré et pour déchiffrer le texte chiffré en texte en clair. On peut parfaitement concevoir un algorithme qui n'utilise pas de clé, dans ce cas c'est l'algorithme lui-même qui constitue la clé, et son principe ne doit donc en aucun cas être dévoilé.

Chapitre 2: Cryptographie Classique

Vocabulaire de base dans la cryptographie

Cryptosystème : algorithmes + clés

Cryptographie : cette branche regroupe l'ensemble des méthodes (algorithmes) qui permettent de chiffrer et de déchiffrer un texte en clair afin de le rendre incompréhensible pour quiconque n'est pas en possession de la clé à utiliser pour le déchiffrer.

Cryptanalyse : c'est l'art de révéler les textes en clair qui ont fait l'objet d'un chiffrement sans connaître la clé utilisée pour chiffrer le texte en clair.

Cryptologie : il s'agit de la science qui étudie les communications secrètes. Elle est composée de deux domaines d'étude complémentaires : la cryptographie et la cryptanalyse.

Chapitre 2: Cryptographie Classique

Chiffrement par substitution mono alphabétique

Le chiffrement par décalage : arithmétique modulaire

Il est défini par les données suivantes : $M = C = K = Z/26Z$
Pour $0 \leq K \leq 25$ et $0 \leq x \leq 25$, on définit:

$$E(x,K) = x + K \bmod 26$$

$$D(y,K) = y - K \bmod 26 .$$

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Chapitre 2: Cryptographie Classique

Chiffrement par substitution mono alphabétique

Le chiffrement par décalage:

Le chiffrement de César

Basé sur une substitution mono-alphabétique
Il a été utilisé dans l'armée romaine durant la guerre des Gaules
Méthode : Décalage alphabétique de 3 caractères (k=3).

Exemple message en clair : ABCDEFGHIJKLMNOPQRSTUVWXYZ
message chiffré : DEFGHIJKLMNOPQRSTUVWXYZABC

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Chapitre 2: Cryptographie Classique

Chiffrement par substitution poly alphabétique

Le Chiffrement de Vigenère: principe

Pour toute clef K de taille m :$K = (k_1, \cdots, k_m)$ (où $k_i \in \mathbb{Z}/26\mathbb{Z}$ pour chaque $i = 1, \cdots, m$), on définit :
Le chiffrement par :

$$E(x_1, x_2, \cdots, x_m, K) = (x_1 + k_1, x_2 + k_2, \cdots, x_m + k_m) \bmod 26$$

et le déchiffrement par :

$$D(y_1, y_2, \cdots, y_m, K) = (y_1 - k_1, y_2 - k_2, \cdots, y_m - k_m) \bmod 26$$

où les opérations sont effectuées dans $\mathbb{Z}/26\mathbb{Z}$.

En utilisant la correspondance $0 \leftrightarrow a$, $1 \leftrightarrow b$, ..., $25 \leftrightarrow z$, on décrit chaque clef K du chiffrement de Vigenère par une chaîne de caractères de longueur m appelée mot-clef. Le chiffrement de Vigenère traite m caractères alphabétiques à la fois : chaque bloc du texte clair est équivalent à m caractères alphabétiques.

Chapitre 2: Cryptographie Classique

Chiffrement par substitution poly alphabétique

Le Chiffrement de Vigenère: Exemple

Chiffrer le texte suivant avec la méthode de Vigenère avec le mot-clef :
« CIPHER »
message en clair : THISCRYPTOSYSTEMISNOTSECURE

La clef correspondant au mot-clef (CIPHER) est
(2, 8, 15, 7, 4, 17)
message chiffré : VPXZGIAXIVWPUBTTMJPWIZITWZT

Chapitre 2: Cryptographie Classique

Chiffrement par substitution poly alphabétique

Le Chiffrement de Hill

On choisit un alphabet de n lettres et une taille m pour les blocs, par exemple m = 2. Alors
P = E = (Z/26Z)2, (en général (Z/nZ)2).

La clé de codage est une matrice carrée de taille « m » inversible K ∈ GLm(Z/nZ), pour n = 26 et m = 2

$$\begin{bmatrix} C_k \\ C_{k+1} \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} P_k \\ P_{k+1} \end{bmatrix} \text{ Mod } 26$$

Pour le chiffrement on a : $C_1 \equiv (ap_1 + bp_2) \bmod 26$

$C_2 \equiv (cp_1 + dp_2) \bmod 26$

Chapitre 2: Cryptographie Classique

Chiffrement par substitution poly alphabétique

Le Chiffrement de Hill

Exemple :
Alice prend comme clef de cryptage la matrice $\begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix}$ pour chiffrer le message « USTO »
Après avoir remplacé les lettres par leur rang dans l'alphabet (a=1, b=2, etc.), elle obtiendra

Lettres	U	S	T	O
Rang (Pk)	20	18	19	14
Rangs chiffrés(Ck)	18	18	19	
Lettres chiffrés	S	S	T	L

C_1 =9*20+4*18 (mod26) = 252 mod 26 = 18
C_2 =5*20+7*18 (mod26) = 226 mod 26 = 18

C_3 =9*19+4*14 (mod26) = 227 mod 26 = 19
C_4 =5*19+7*14 (mod26) = 193 mod 26 = 11

Chapitre 2: Cryptographie Classique

Chiffrement par substitution poly alphabétique

Le Chiffrement de Hill

Déchiffrement :

Pour le déchiffrement Hill le principe est le même que pour le chiffrement: on prend les lettres deux par deux, puis on les multiplie par la matrice inverse

$$A^{-1} = (\det A)^{-1} \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

$$\det(A) = ad-bc$$

La matrice utilisée dans le déchiffrement est la matrice inverse
Le déterminant : (A=ad-bc)

une matrice A à coefficients dans Z/mZ est inversible si, et seulement si, son déterminant est inversible modulo m (c'est-à-dire pgcd(det A, m) = 1).

Chapitre 2: Cryptographie Classique

Chiffrement par substitution poly alphabétique

Le Chiffrement de Hill
Exemple de Déchiffrement :

Par exemple, considérons la matrice A= $\begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix}$

Le det A =43 mod 26 =17

Comme 17^{-1} mod 26 =23

La matrice inverse de A est : $\begin{pmatrix} 5 & 12 \\ 15 & 25 \end{pmatrix}$

Déchiffrer le message : UWGMWZRREIUB → UW| GM| WZ| RR| EI| UB | → (20,22)|(6,12)|(22,25)|(17,17)|(4,8)

20*5+22*12 mod 26 = 0

20*15+22*25 mode 26 =6 ---→ AG

6*5+12*12 mod 26 = 18

6*15+12*25 mode 26 =14 ---→ SO

Chapitre 2: Cryptographie Classique

Chiffrement par substitution poly alphabétique

Le Chiffrement Affine

L'idée est d'utiliser comme fonction de chiffrage une fonction affine du type y = (ax + b) mod 26, où a et b sont des constantes, et où x et y sont des nombres correspondant aux lettres de l'alphabet (a=0,b=1,…)

-On remarque que si a=1, alors on retrouve le chiffre de César et b est le décalage.
-On remarquera aussi que si b=0, alors "a" est toujours chiffré « a".

-Clé = $\mathbf{K\ (K_1, K_2)}$
-Chiffrement : $\mathbf{E(x,K) = K_1x + K_2 \bmod 26}$
-Déchiffrement $\mathbf{D(y,(K_1, K_2)) = K_1^{-1}(K_2 - b) \bmod 26}$

Chapitre 2: Cryptographie Classique

Chiffrement par substitution poly alphabétique

Exemple avec le Chiffrement Affine

chiffrer le mot « SECRET » avec la clé K=(3,7) :
SECRET = (18.4.2.17.4.19)
(3*18+7) mod 26 = 9
(3*4+7) mod 26 = 19
(3*2+7) mod 26 = 13
(3*17+7) mod 26 = 6
(3*4+7) mod 26 = 19
(3*19+7) mod 26 = 12

Le chiffré du mot « SECRET » est : «JTNGTM »

Déchiffrer le mot «JTNGTM» avec la clé K=(3,7) :
JTNGTM = (9, 19, 13, 6, 19, 12)
(3^{-1} * 9-7) mod 26 = 9*2 mod 26 = 18
(9*(19-7)) mod 26 = 4
(9*(13-7) mod 26 = 2
(9*(6-7) mod 26 = 17
(9*(19-7) mod 26 = 4
(9*(12-7) mod 26 =19

Le déchiffré du mot « JTNGTM » est : «SECRET »

Conclusion

En conclusion, la sécurité informatique est essentielle pour protéger les données, les systèmes et les infrastructures face aux nombreuses menaces et attaques de plus en plus sophistiquées. Au cours de ce module, nous avons exploré les concepts fondamentaux de la sécurité, tels que les principes de confidentialité, d'intégrité et de disponibilité, ainsi que les différentes menaces comme les malwares, le phishing, et les attaques par déni de service (DDoS). Nous verrons dans les chapitres qui suivent.les mécanismes de protection, tels que les pare-feu, le chiffrement et les systèmes de détection d'intrusion.