Sécurité Informatique

Chapitre 1 :

Techniques de cryptographie Classiques

Guellil zouaoui

plant

- Introduction
- Cryptographie symétrique
  - Cryptographie Classique
  - Techniques de la Substitution
  - Techniques de la Transposition

Introduction

- **Le réseau: système support avec ses caractéristiques matérielles (switch, routeurs,…) et logicielles (protocoles)**

- **Le système d'information: systèmes d'exploitation et applications diverses et variées**

- **La sécurité informatique: Ensemble de moyens mis en œuvre pour éviter ou minimiser les défaillances naturelles dues à l'environnement ou au défaut du système d'information et les attaques malveillantes intentionnelles dont les conséquences sont catastrophiques .**

Sûreté Vs Sécurité

- Sûreté de fonctionnement (Safety)

- Sécurité de fonctionnement (Security)

Solutions

- Solutions pour le réseau système support: FireWall, VPN , Solutions sécurisées

- Solutions pour le système d'information: Approches de développement, Modèles de développement, Méthodes de développement, revue de code, analyse statique et dynamique du code, etc.…

Cryptography

C1 - Cryptology

is the science of cryptosystems (machines & technics) & cryptoanalysis.

C2 - Cryptography

is the science of secret writing with the goal of hiding the meaning of a message.

C3 - Cryptanalysis

is the science/art of breaking cryptosystems.

Cryptography branches :

Symmetric Algorithms :

two parties have an encryption and decryption method for which they share a secret key.

Asymmetric (or Public-Key) Algorithms

In public-key cryptography, a user possesses a secret key but also a public key.

Cryptographic Protocols

deal with the application of cryptographic algorithms.

Problem of confidentiality of hiding the contents of the message from an eavesdropper.
Preventing Oscar from making unnoticed changes to the message (message integrity)

Assuring that a message really comes from Alice (sender authentication).

Substitution 1/5

- **Principe général :** A chaque lettre ou groupe de lettres on substitue une autre lettre ou un autre groupe de lettres.
- **substitution mono alphabétique:** Pour chaque lettre de l'alphabet de base on se donne une autre lettre utilisée dans le texte chiffré.

Substitution 2/5 : *Mono (**Caesar**)*

- **On décale les lettres de 3 positions**

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

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

- Forme générale des chiffre par décalage sur l'alphabet à 26 lettres :
- $E_k(x)=x+k \bmod 26$
- $D_k(y)=y-k \bmod 26$
- Où k est la clés de chiffrement.
- Attack: force brute et analyse fréquentielle.

Substitution 3/5 : *Mono* (***Afine***)

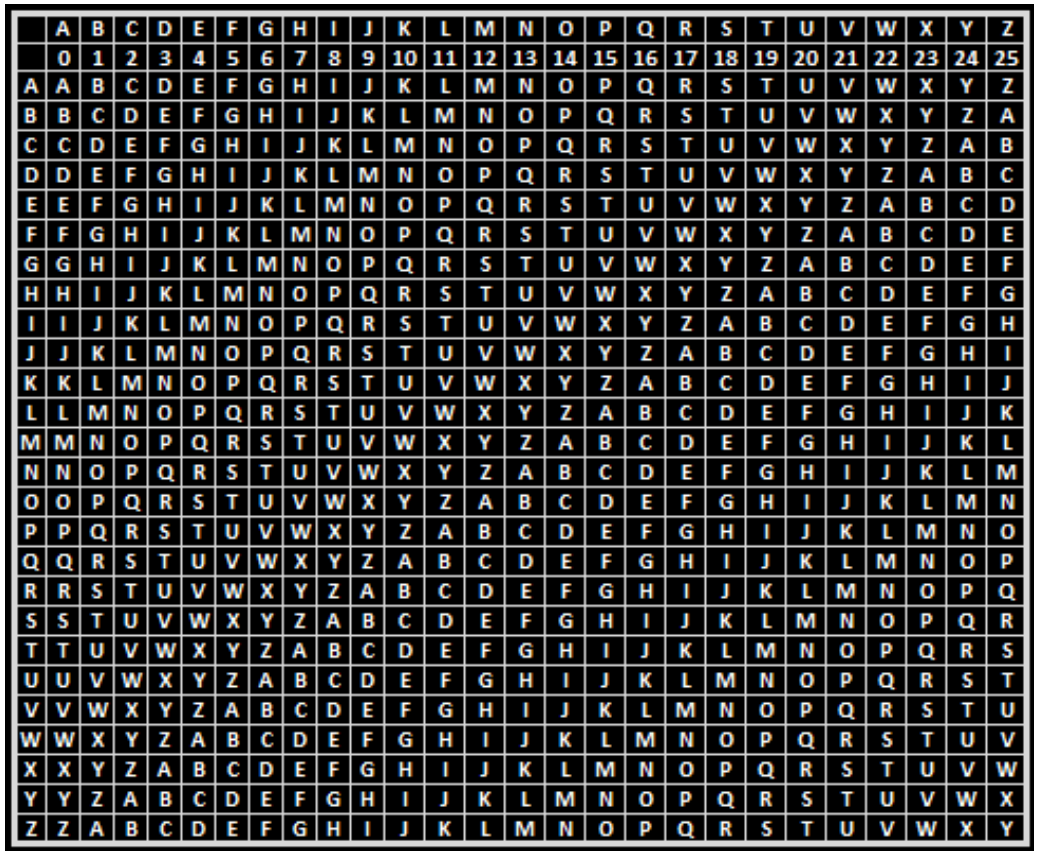
Definition 1.4.4 *Let x,y,a,b ∈ Z26*
Encryption: ek(x) = y ≡ a ▪ x+b mod 26.
Decryption: dk(y) = x ≡ a^{-1} ▪ (y−b) mod 26.
key: k = (a,b) has the restriction: gcd(a,26) = 1.

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

X est l'inverse modulaire de y dans Z_{26} si x*y *≡1 mode 26*
Quelle sont les clés possible dans Z_{26}

$$\begin{aligned}\text{key space} &= (\#\text{values for } a) \times (\#\text{values for } b)\\ &= 12 \times 26 = 312\end{aligned}$$

Chiffrement Vigenere (Poly)



	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
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

T	H	E		V	I	G	E	N	E	R	E		A	L	G	O	R	I	T	H	M					
C	H	L	E	F	C	H	L	E	F	C	H	L	E	F	C	H	L	E	F	C	H					
V	O	P		A	K	N	P	R	J	T	L		E	Q	I	V	C	M	Y	J	T					

Shift table.
Columns labeled from A to Z,
Column μ is alphabet shifted from μ.

Key word. *Used encrypt PT*

Mapping. *Repeat KW to match PT in length.*

Encrypt. *Encrypt current character $ using shift cipher with key is the mapped character to $.*

Exc 1.8. *write formel algorithm of VC*

Exc 1.9. *Apply VC to*
PT=THE VIGENERE ALGORITHM
Key =CHLEF

PT=VIGENERE Key =CHIFFRE

Exc 1.10. *Compute KS size for VC*

Substitution 4/5 *Poly (**Vegenere**)*

	0	1	2	3
	c	l	e	f
CL	2	11	4	5

$E_{CL}(x_n)=(x_n+CL\ (n \bmod 4)) \bmod 26$

t	e	x	t	e	s	e	c	r	e	t
19	4	23	19	4	18	4	2	17	4	19
2	11	4	5	2	11	4	5	2	11	4
21	15	1	24	6	3	8	7	19	15	23
v	p	b	y	g	d	i	h	t	p	x

Substitution 5/5 *Poly (**Playfair**)*

- **Substitutions de polygrammes :** Au lieu de substituer des caractères on substitue par exemple des digrammes (groupes de deux caractères)

Brute Force attack

First Attack: Brute-Force or Exhaustive Key Search

Oscar has the ciphertext from eavesdropping on the channel and a short piece of plaintext

Oscar decrypts the ciphertext with *all possible keys.*

Definition 1.2.1 Basic Exhaustive Key Search or Brute-force Attack
Let (x,y) denote the pair of plaintext and ciphertext, and let $K = \{k_1, ..., k_K\}$ *be the key space of all possible keys* k_i*. A brute-force attack now checks*
for every $k_i \in K$ **if** $d_{k_i}(y) = x$**?.**
If the equality holds, a possible correct key is found;
if not, proceed with the next key.

If testing all the keys on many modern computers takes too much time, the cipher is *computationally secure against a brute-force attack.*

Exc 1.2 / D*etermine the key space of the substitution cipher.*

Space key size

When choosing the replacement for the first letter A, we randomly choose one letter from the 26 letters of the alphabet (in the example above we chose k).

Replacement for the next alphabet letter B was randomly chosen from the remaining 25 letters, etc.

Thus there exist the following number of different substitution tables:
key space of the substitution cipher = $26 \cdot 25 \cdot \cdots \cdot 3 \cdot 2 \cdot 1 = 26! \approx 288$

Letter Frequency Analysis

Second Attack: Letter Frequency Analysis

the brute-force attack from above treats the cipher as a black box,
i.e., we do not analyze the internal structure of the cipher.

analytical attack.

Weakness of the cipher is that each PT symbol always maps to the same CT symbol.
That means that the statistical properties of PT are preserved in CT.
observe that the letter q occurs most frequently in the text.

From this we know that q must be the substitution for one of the frequent letters in the English language.

For practical attacks, the following properties of language can be exploited:

1. Determine the frequency of every CT.
2. The frequency distribution, often even of relatively short pieces of encrypted text, will be close to that of the given language in general.

2. Looking at pairs or triples, or quadruples, and so on of CT symbols. QU, WH

Letter Frequency Analysis

Detect frequent short words such as THE, AND, etc.
Once identified one of these words, immediately know the letters for the entire text.

Table 1.1 Relative letter frequencies of the English language

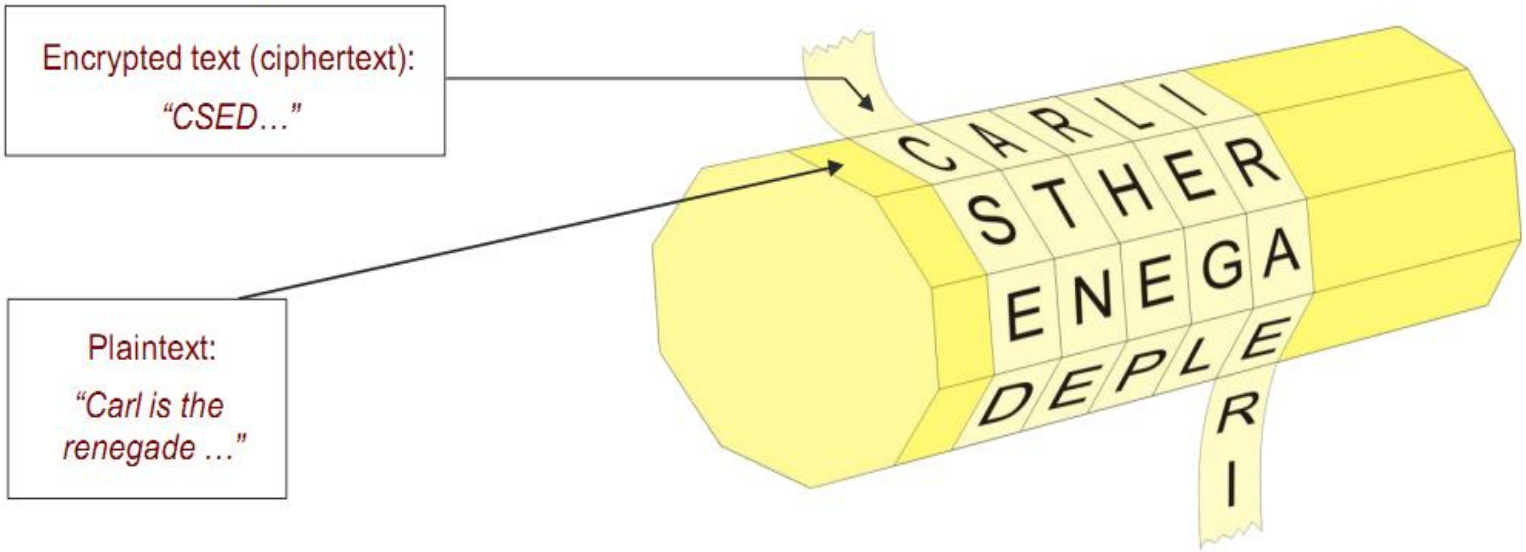
Letter	Frequency	Letter	Frequency
A	0.0817	N	0.0675
B	0.0150	O	0.0751
C	0.0278	P	0.0193
D	0.0425	Q	0.0010
E	0.1270	R	0.0599
F	0.0223	S	0.0633
G	0.0202	T	0.0906
H	0.0609	U	0.0276
I	0.0697	V	0.0098
J	0.0015	W	0.0236
K	0.0077	X	0.0015
L	0.0403	Y	0.0197
M	0.0241	Z	0.0007

Exc 1.3. Ciphertext:
iq ifcc vqqr fb rdq vfllcq na rdq cfjwhwz hr bnnb hcc hwwhbsqvqbre hwq vhlq
Try to decrypt CT by using analytical attack methodes

Good ciphers should hide the statistical properties of the encrypted PT.
PT symbols should appear to be random.
Large key space alone is not sufficient for a strong encryption function.

Transposition *(**Scytal**)*

- Transposition (plaintext characters are re-sorted)



Cryptographie classique (Limite)

- mode utilisé durant la période avant les ordinateurs
- Espace de clés réduit.
- Expose les propriétés statistiques du texte.

Chiffre symétrique moderne

- Le **principe de Kerckhoffs :**la sécurité d'un cryptosystème ne doit reposer que sur le secret de la clef.
- Claude Shannon : « l'adversaire connaît le système »
- Diffusion : cacher les propriétés statistiques
- Confusion : cacher la relation entre la clé et les messages cryptés

Chiffre symétrique moderne

- Diffusion : Diffusion means that if we change a single bit of the plaintext, then (statistically) half of the bits in the ciphertext should change, and similarly,…
- Confusion : Confusion means that each binary digit (bit) of the ciphertext should depend on several parts of the key, obscuring the connections between the two.

chiffrement à clé symétrique

- Il existe deux types :
- Le chiffrement par blocs : l'opération de chiffrement s'effectue sur des blocs de texte clair (ex : le DES avec des blocs de 64 bits).
- Le chiffrement par flots (ou par stream ou de flux) : l'opération de chiffrement s'opère sur chaque élément du texte clair (caractère, bits). On chiffre un bit/caractère à la fois. La structure d'un chiffrement par stream repose sur un générateur de clés qui produit une séquence de clés k1, k2, ..., ki.

BIT/STREAM & BLOCK/BLOCK

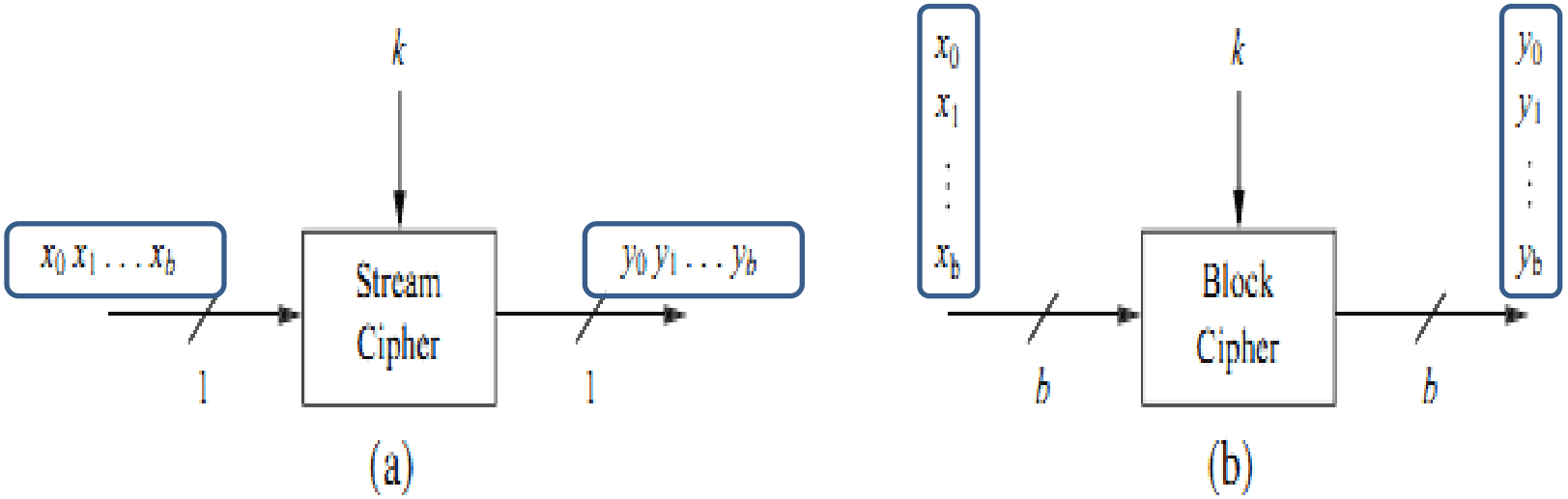


Fig. 2.2 Principles of encrypting b bits with a stream (a) and a block (b) cipher

Encryption and Decryption with SC

Definition 2.1.1 Stream Cipher Encryption and Decryption
The plaintext, the ciphertext and the key stream consist of individual bits,
i.e., $x_i, y_i, s_i \in \{0, 1\}$.
Encryption: $y_i = e_{s_i}(x_i) \equiv x_i + s_i \mod 2$.
Decryption: $x_i = d_{s_i}(y_i) \equiv y_i + s_i \mod 2$.

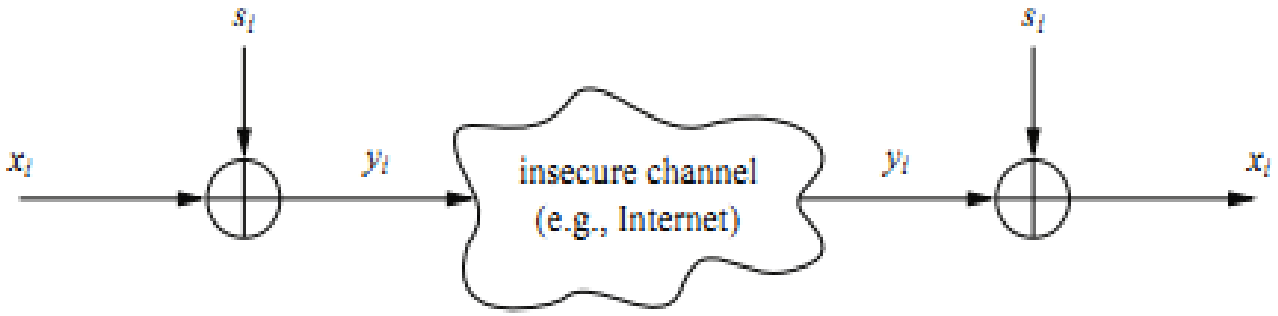


Fig. 2.4 Encryption and decryption with stream ciphers

LFSR : Linear Feedback Shift Register

Registre à d´écalage à rétroaction linéaire

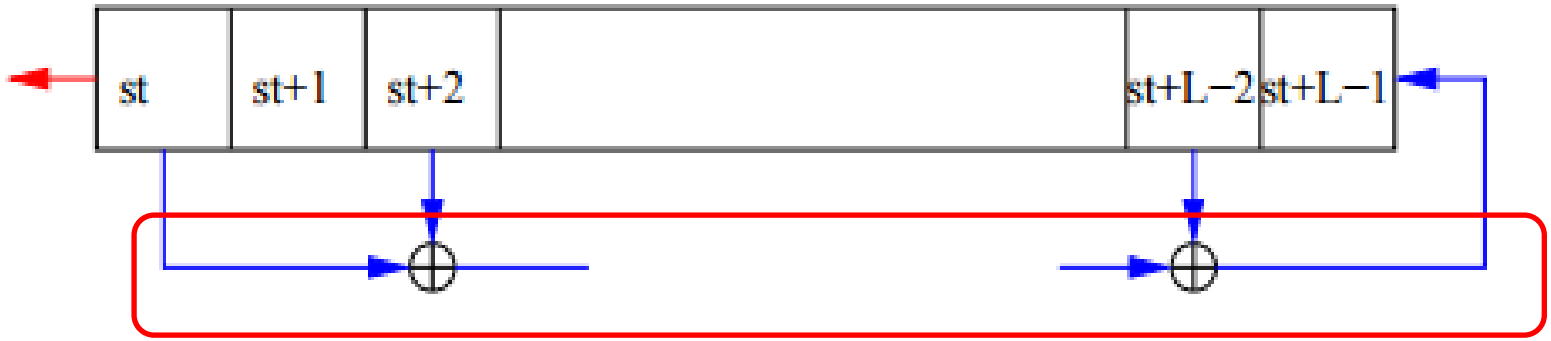
est la donnée de :

1. Un registre de L cases contenant chacune un bit $s_t,\ldots,s_{t+L-1}$;
2. Une fonction de rétroaction calculant un bit s_{t+L} par combinaison linéaire de certains bits du registre

$$s_{t+L} = f(s_t, s_{t+1}, .., s_{t+L-1})$$

$$s_{t+L} = \sum_{i=1}^{L} c_{L-i+1} s_{t+i-1}$$

Au top t d'horloge, le bit s_t sort du registre, tous les bits sont décalés d'un rang vers la gauche, et le bit s_{t+L} entre dans le registre.



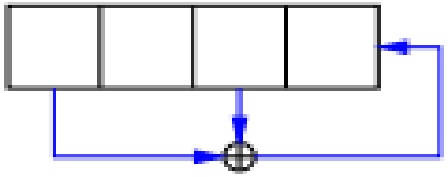
Polynome de rétroaction

Définition On appelle polynome de rétroaction d'un LFSR de longueur L, le polynome

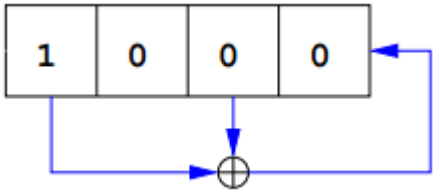
$$P(x) = 1 + \sum_{i=1}^{L} c_i x^i$$

ou chaque c_i est le coefficient utilisé dans le calcul de la combinaison lineaire

Exemple Le LFSR de longueur 4 ci-dessous a pour polynome de rétroaction $P(x) = 1 + x^2 + x^4$.



Exemple de suite chiffrante produite par un LFSR, avec état initial **1000**



t	q_t	s_t
0	1000	
1	0001	1
2	0010	0
3	0101	0
4	1010	0
5	0100	1
6	1000	0

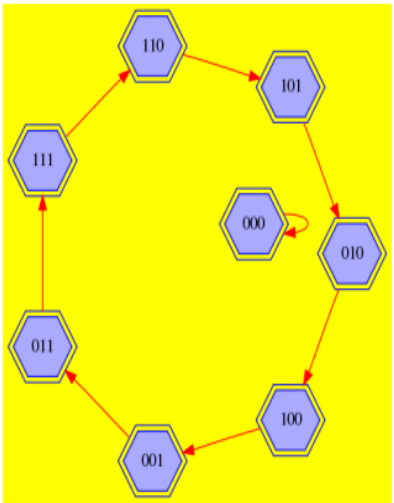


FIG.: Cycles des états d'un LFSR de longueur 3 et de polynôme de rétroaction $1 + x + x^3$