Les Algorithmes Cryptographiques Symétriques

Omar Cheikhrouhou
Omar.cheikhrouhou@isetsf.rnu.tn

ISET SFAX, 2010-2011

Plan

- Principes
- Cryptographie traditionnelle
- Opérations de base:
  - Substitution
  - Transposition
  - Opérations algébriques
- Modes Opératoires :
  - Cryptage par flux
  - Cryptage par Bloc
- Algorithmes Cryptographiques Symétriques
  - DES
  - IDE
  - AES
- Fonctions de Hashage
  - MD5
  - SHA
- Avantages et Inconvénients

Introduction

- Les algorithmes cryptographiques modernes se basent sur des fonctions mathématiques qui dépendent d'une clés secrète
- La sécurité est au niveau clés non pas algorithmes cryptographiques
- Les algorithmes cryptographiques sont publiées est connu par tout le monde

Cryptographie traditionnelle

Opérations de base

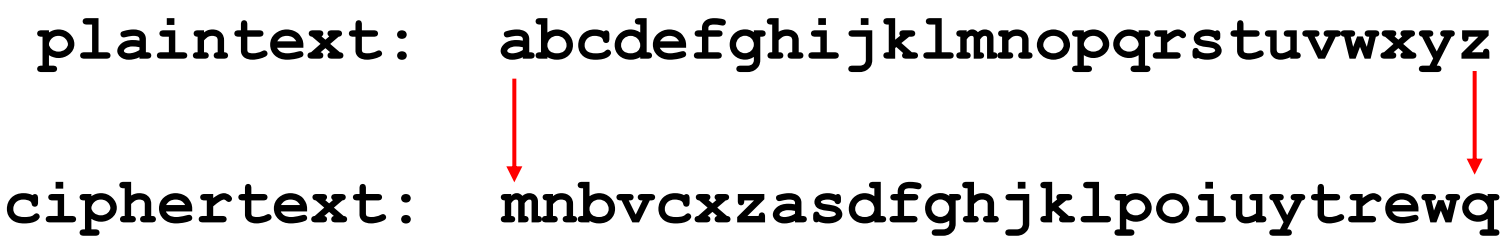
- Substitution: replacement de chaque élément (bit, lettre, groupe de bits ou de lettres) dans le texte clair par un autre élément.
- Transposition: réarrangement des éléments du texte clair.
- Opérations algébriques simples
- La plupart des systèmes utilisent plusieurs étapes de transposition et de substitution.

Chiffrement par substitution

- Cette méthode correspond à substituer un caractère ou un groupe de caractères par un autre dans le texte à chiffrer.
- Plusieurs types de crypto-systèmes par substitution :
  - *monoalphabétique* (code César) consiste à remplacer chaque lettre du message par une autre lettre de l'alphabet
  - *homophonique* permet de faire correspondre à chaque lettre du message en clair un ensemble possible d'autres caractères c'est un peu similaire aux méthodes employées par les mordus de SMS ;
  - *polyalphabétique* (code Vigenère) consiste à utiliser une suite de chiffrement, monoalphabétique réutilisée périodiquement ;
  - *polygrammes* consiste à substituer un groupe de caractères (polygramme) dans le message par un autre groupe de caractères.

Chiffrement par substitution simple

- Chaque symbole du *plaintext* est remplacé par un autre de manière unique



E.g.: Plaintext: bob. how are you. alice

ciphertext: nkn. akr moc wky. mgsbc

Exemple de cryptage par substitution simple

- Caesar's cipher
  - Remplacer chaque lettre par celle qui la succède de trois.
  - a devient d, b devient e, …, y devient b, z devient c
  - L'algorithme peut être décrit comme suit:
    - C = E(p) = (p+3) mod (26)
- La distribution fréquentielle des symboles est préservée dans le *ciphertext*
- Vulnérabilité aux attaques de cryptanalyse statistique : il suffit de calculer la fréquence d'apparition de chaque symbole dans le *ciphertext* et de le comparer aux fréquences d'apparition des lettres de l'alphabet dans une langue particulière.
  - Algorithme de cryptage et de décryptage connu.
  - Seulement 25 clés à essayer.
  - Le langage du message clair est connu et facilement identifiable.

Cryptanalyse du Chiffrement par substitution

- Dans le cas de l'utilisation d'un code par substitution, la cryptanalyse ou déchiffrement se fait par l'utilisation de données **statistiques** :
  - En anglais, les caractères les plus fréquemment utilisés sont : e, t, o, a, n, i…
  - Les combinaisons de deux lettres (***digrammes***) les plus fréquentes sont : th, in, er, re, et an.
  - Les combinaisons de trois lettres (***trigrammes***) : the, ing, and et ion.
  - ***Méthode empirique de cryptanalyse***: Il suffit pour retrouver le texte en clair de :
    - de rechercher les caractères, digrammes et trigrammes les plus fréquents du texte chiffré;
    - de faire des suppositions en les associant à ceux les plus fréquents d'un texte en clair (dans la langue choisi).
    - Par exemple dans un texte crypté appartenant à une banque il est probable de trouver des mots tel que financier, montant, solde…

Cryptanalyse du Chiffrement par substitution

- ***Comment finir la cryptanalyse ?***
  - Si certains mots commencent à émerger du texte chiffré, alors il y a de fortes probabilités que le code de chiffrement soit découvert.
  - Un code par substitution ne modifie pas les propriétés statistiques des caractères, digrammes et trigrammes substitués.
  - Il conserve **l'ordre des caractères** du texte en clair, mais masque ces caractères.

Cryptanalyse du Chiffrement par substitution

- Table des fréquences d'apparition des lettres pour un texte français

Lettre	Fréquence %	Lettre	Fréquence %
A	9.42	N	7.15
B	1.02	O	5.14
C	2.64	P	2.86
D	3.39	Q	1.06
E	15.87	R	6.46
F	0.95	S	7.90
G	1.04	T	7.26
H	0.77	U	6.24
I	8.41	V	2.15
J	0.89	W	0.00
K	0.00	X	0.30
L	5.34	Y	0.24
M	3.24	Z	0.32

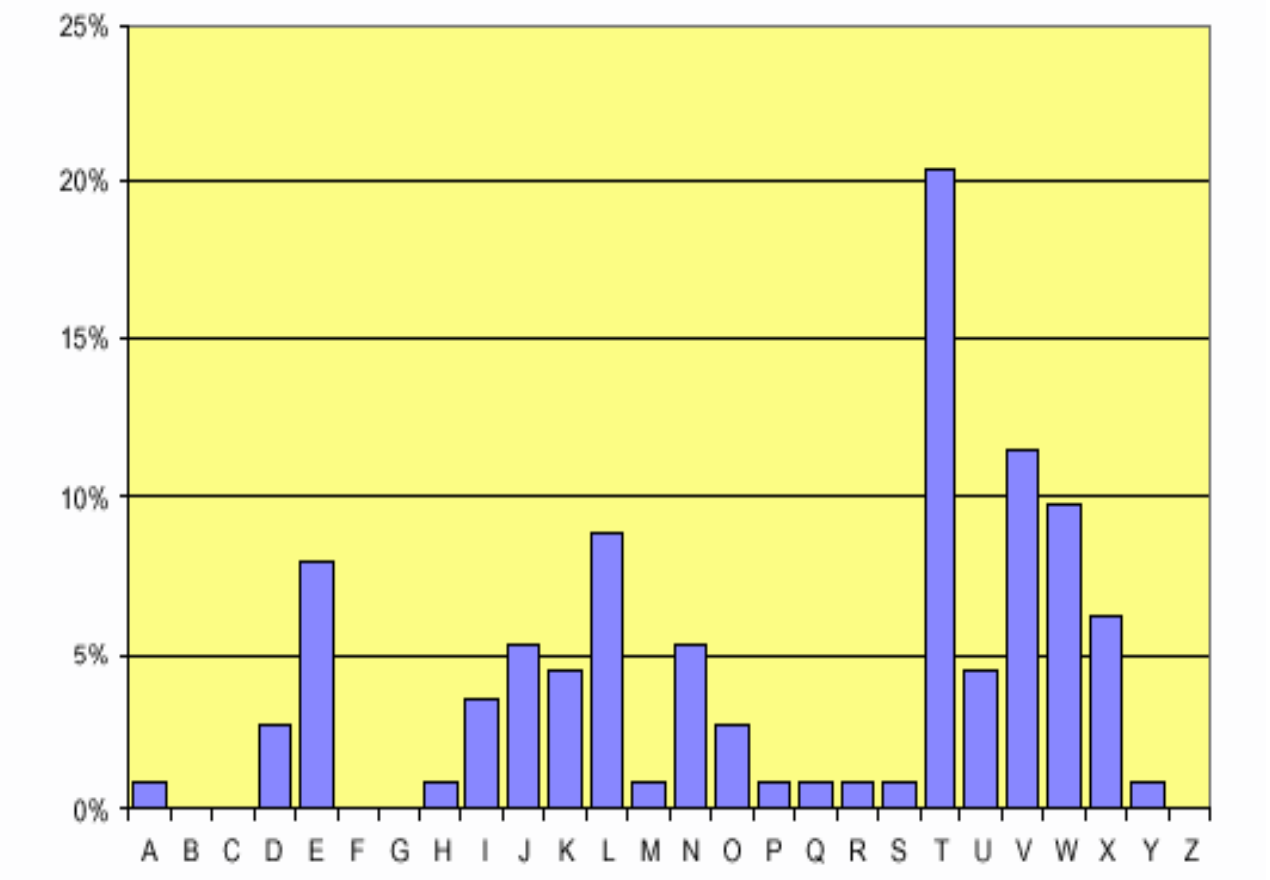
Cryptanalyse du Chiffrement par substitution

- Exemple: Texte chiffré

JTVMNKKTVLDEVVTLWTWITKTXUTLWJ
ERUTVTWTHDXATLIUNEWV.
JTVIEVWELOWENLVVNOEDJTVLTPTXYT
LWTWUTSNLITTVQXTVXUJXWEJEWTON
KKXLT.

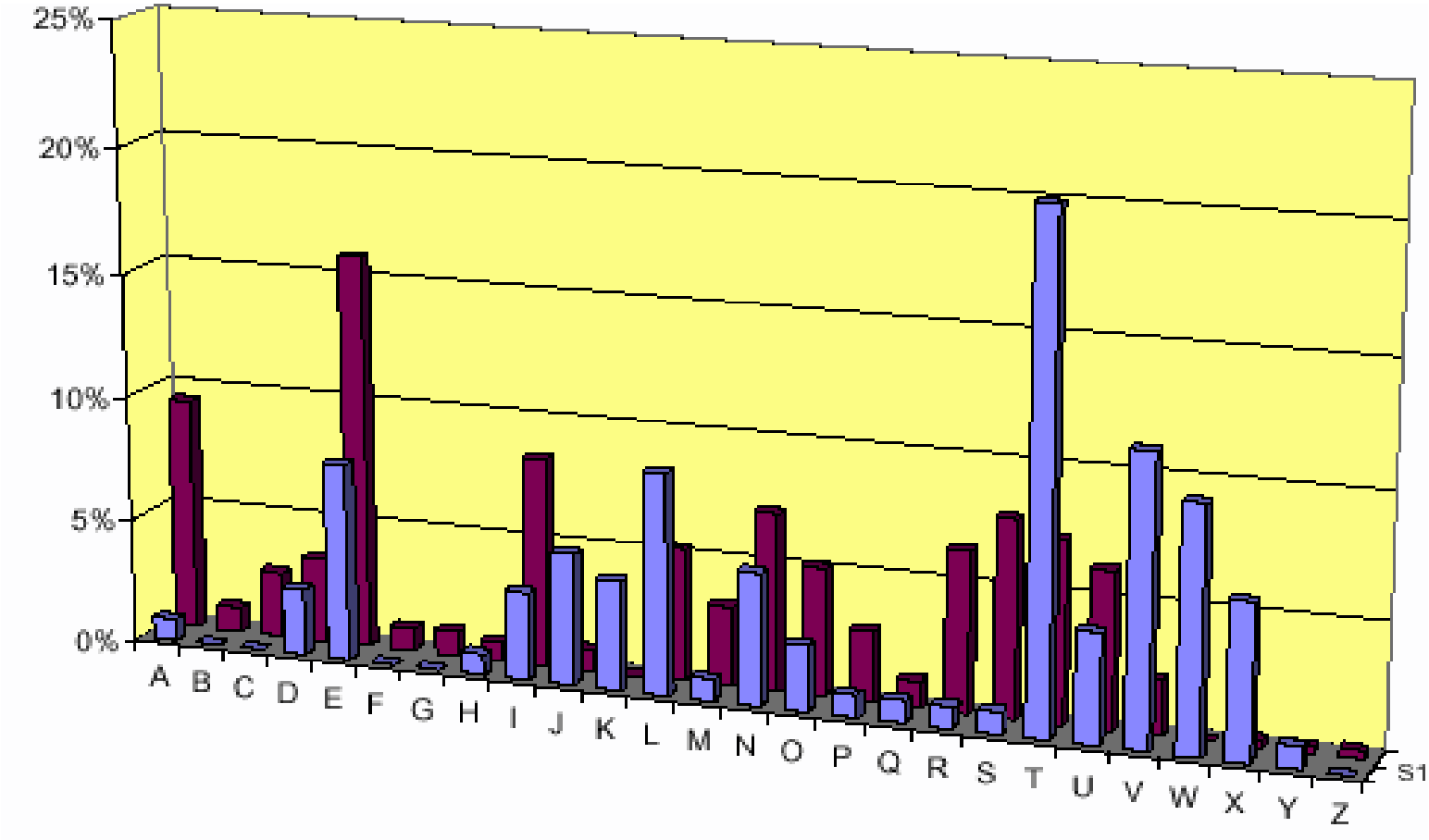
Cryptanalyse du Chiffrement par substitution

- Exemple: Analyse des fréquences de caractères du texte chiffré



Cryptanalyse du Chiffrement par substitution

- Exemple: Comparaison des fréquences entre texte clair et chiffré



Cryptanalyse du Chiffrement par substitution

- Exemple: Début du déchiffrement

JeVMNKKeVLDEVVeLWeWIeKeXUeLWJ
ERUeVeWeHDXAeLIUNEWV.
JeVIEVWELOWENLVVNOEDJeVLePeXYe
LWeWUeSNLIeeVQXeVXUJXWEJEWeON
KKXLe.

Cryptanalyse du Chiffrement par substitution

- Exemple: Suite du déchiffrement

lesMNKKesLDEsseLtetIeKeureLtlERreseteH

DuAeLIrNEts.

lesIEstELOtENLssNOEDlesLePeuYeLtetreS

NLIeesQuesurlutElEteONKKuLe.

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
				T							J	K	L				U	V	W	X	Y	Z	A	B	C

Cryptanalyse du Chiffrement par substitution

- Exemple: Poursuite du déchiffrement

lesMNKKesLDEsseLtetIeKeureLtlERreseteH
DuAeLIrNEts.
lesIEstELOtENLssNOEDlesLePeuYeLtetreS
NLIeesQuesurlutElEteONKKuLe.

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
				T							J	K	L				U	V	W	X	Y	Z	A	B	C

Cryptanalyse du Chiffrement par substitution

- Exemple: poursuite du déchiffrement

les MNmmes nDEssent et Iemeurent
lERres et eHDux en IrNEts.
Les IEstEnOtENns sNOEDles ne Peuvent etre
SNLIees Que sur lutElEte ONmmune.

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
				T							J	K	L				U	V	W	X	Y	Z	A	B	C

Cryptanalyse du Chiffrement par substitution

- Exemple: Fin du déchiffrement

« Les hommes naissent et demeurent
libres et égaux en droits.
Les distinctions sociales ne peuvent être
fondées que sur l'utilité commune. »

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

Cryptanalyse du Chiffrement par substitution

- **Idée d'amélioration** : Substitution **polyalphabétique**: utilisation de deux ou plus alphabets de chiffrement.
- Cette méthode opère sur des blocs de taille *t*
- A chaque symbole du bloc on applique une substitution simple différente

Exemple:

Alphabet clair : abcdefghijklmnopqrstuvwxyz

Alphabet chiffré 1: MOTSECRUVWXYZABDFGHIJKLNPQ

Alphabet chiffré 2: QPNLKJIHGFDBAZYXWVURCESTOM

Texte clair :

vinum et musica laetificant cor

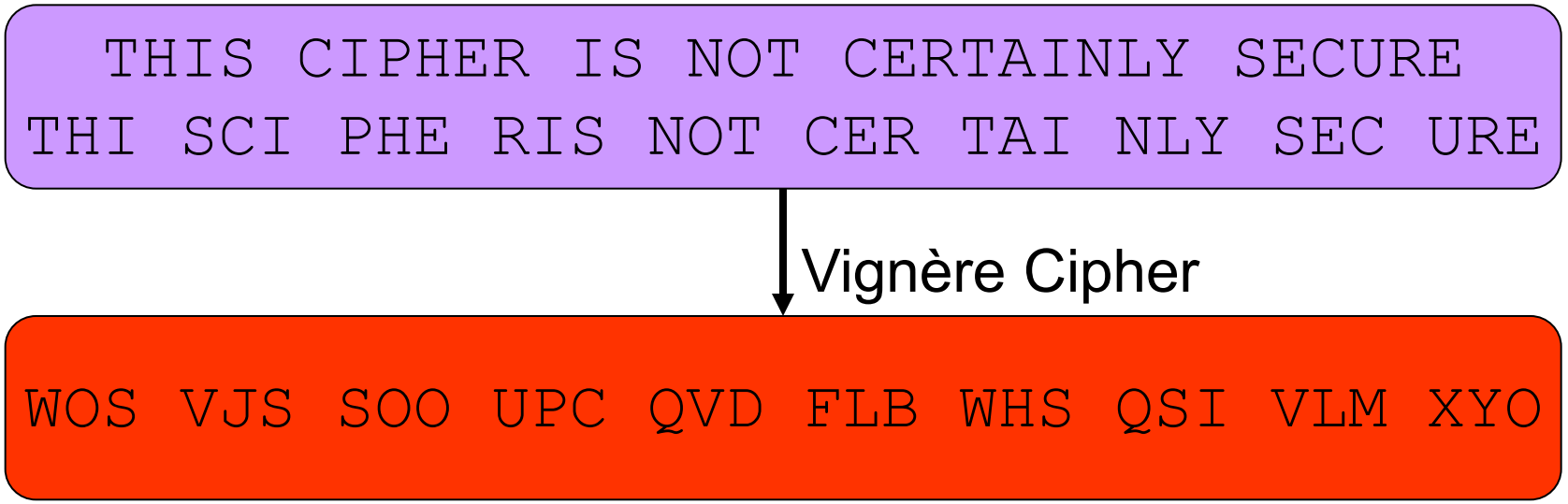
Texte chiffré :

KGACZ KI AJUVNM BMKIGCGTQAR TYG

Chiffrement par substitution polyalphabétique

• Vignère cipher (exemple):

- Il opère sur des blocs de taille 3
- Le premier symbole du bloc est remplacé par le troisième symbole à droite
- Le deuxième symbole du bloc est remplacé par le septième symbole à droite
- Le troisième symbole du bloc est remplacé par le dixième symbole à droite



- **Le chiffre de Vigenère**
- Le carré de Vigenère :
  - 26 alphabets : chiffrement de César
- Clé de chiffrement : un mot clé identifiant les alphabets à utiliser

Chiffrement par substitution polyalphabétique

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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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
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

Chiffrement par substitution polyalphabétique

- L'idée de Vigenère est d'utiliser un code de César, mais où le décalage utilisé change de lettres en lettres.
- Pour coder un message,
  - on choisit une clé qui sera un mot de longueur arbitraire.
  - On écrit ensuite cette clé sous le message à coder, en la répétant aussi souvent que nécessaire pour que sous chaque lettre du message à coder, on trouve une lettre de la clé.
  - On remplace les lettres par leur rang dans l'alphabet (attention on commence à 0).

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																								

  - A chaque lettre on additionne les deux rangs et on prend le reste de cette somme dans la division euclidienne par 26 et on trouve ainsi la lettre codée correspondante.

Exemple

Exemple : on veut coder CHIFFRE DE VIGENERE, avec la clé MEXICO.

clair	C	H	I	F	F	R	E	D	E	V	I	G	E	N	E	R	E
rang	2	7	8	5	5	17	4	3	4	21	8	6	4	13	4	17	4
clé	12	4	23	8	2	14	12	4	23	8	2	14	12	4	23	8	2
reste du(rang+clé) par 26	14	11	5	13	7	5	16	7	1	3	10	20	16	17	1	25	6
codé	O	L	F	N	H	F	Q	H	B	D	K	U	Q	R	B	Z	G

M	E	X	I	C	O
12	4	23	8	2	14

CHIFFRE DE VIGENERE se code donc par OLFNHFQ HB DKUQRBZG.

Application

1) Coder EUPHEMISME par cette méthode en prenant pour clé OVIDE.

clair																	
rang																	
clé																	
reste du(rang+clé) par 26																	
codé																	

2) Décoder le mot OELUZOLEMK qui a été codé avec la clé ZEUGMA. Expliquer le sens du mot trouvé et en donner un exemple.

Cryptanalyse de la substitution polyalphabétique

- **Deux étapes:**
  - trouver la longueur du mot-clé ;
  - faire l'analyse fréquentielle sur chacun des alphabets
- **Faiblesse**
  - **Taille de la clé** : le codage d'un mot peut être le même, en particulier celui d'un digramme.
  - Il est possible de faire une **analyse fréquentielle** afin de déterminer la taille de la clé.

Substitution homophonique

- Au lieu d'associer un seul caractère crypté à un caractère en clair on dispose d'un ensemble de possibilités de substitution de caractères dans laquelle on choisit aléatoirement.

Transposition: Principe

- La transposition représente la permutation des symboles d'un *plaintext*
- Conserve la distribution des symboles
- La cryptanalyse statistique est possible

Exemple de cryptage par transposition

Rail fence technique

- Le texte clair est réécrit comme une séquence de lignes, puis réordonnée comme une séquence de colonnes

```
Key:        4 3 1 2 5 6 7
Plaintext: a t t a c k p
           o s t p o n e
           d u n t i l t
           w o a m x y z

Ciphertext: TTNA APTM TSUO AODW COIX KNLY PETZ
```

- Cryptanalyse possible vue que l'algorithme préserve la fréquence de distribution des lettres du texte original.

Opérations algébriques simples

- Composition des fonctions ($f \circ g$)
- XOR
- Remarque:
  - La substitution ajoute du **désordre** (*confusion*) au processus de cryptage. L'objectif est de rendre la relation entre le ciphertext et la clé la plus compliquée que possible
  - La transposition ajoute de la **diffusion** au processus de cryptage. L'objectif est de réarranger les bits du *plaintext* afin de détruire toute forme de redendance

Exercice 1

- Retrouver le clair du message codé à l'aide de l'algorithme de César (La clé est 3) «FRGDJHGHFHVDU ».

Clair	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

Exercice 1

- Solution:
  - Comme son nom l'indique, l'algorithme à translation de César correspond à une translation de 3 lettres (clé) pour passer du message original au message crypté.

Clair	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
Crypte	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

  - Ainsi, la lettre F d'un message crypté correspondra à la lettre C du message clair.
  - Soit le texte clair « CODAGE DE CESAR »

Exercices

- **Exercice 2**
  - Chiffrer avec le chiffre de Vigenère le texte suivant "textesecretadecoder" en utilisant comme clé le mot ***crypto***
  - Pour le même texte en clair on obtient le texte chiffré suivant "brqksmzcspxiqxtcxzr" .Quel est la clé ?
- **Exercice 3**
  - Soit d=6 et la permutation (6,5,4,3,2,1). Chiffrer le message "CRYPTOGRAPHIE PAR TRANSPOSITION".
- **Exercice 4**
  - L'attaque «web spoofing » est une attaque contre la confidentialité?
  - Quelles sont les techniques de l'attaque «Password Guessing»
  - Donnez des exemples d'attaques de déni de service

Résumé

- Services de sécurité: authentification, confidentialité, intégrité, non répudiation…
- Mécanismes: chiffrement, signature, mot de passe, empreinte, carte à puce, contrôle d'accès…
- Chiffrement:
  - Symétrique (une seule clé)
  - Asymétrique (une clé publique et une clé privée)
- Chiffrement par flux ou par bloc
- Opérations:
  - Substitution mono-alphabétique/ polyalphabétique/ homophonique
  - Transposition
  - Opérations algébriques simple
- Chiffrement de césar
- Chiffrement de Vigenère

Le carré de Vigenère

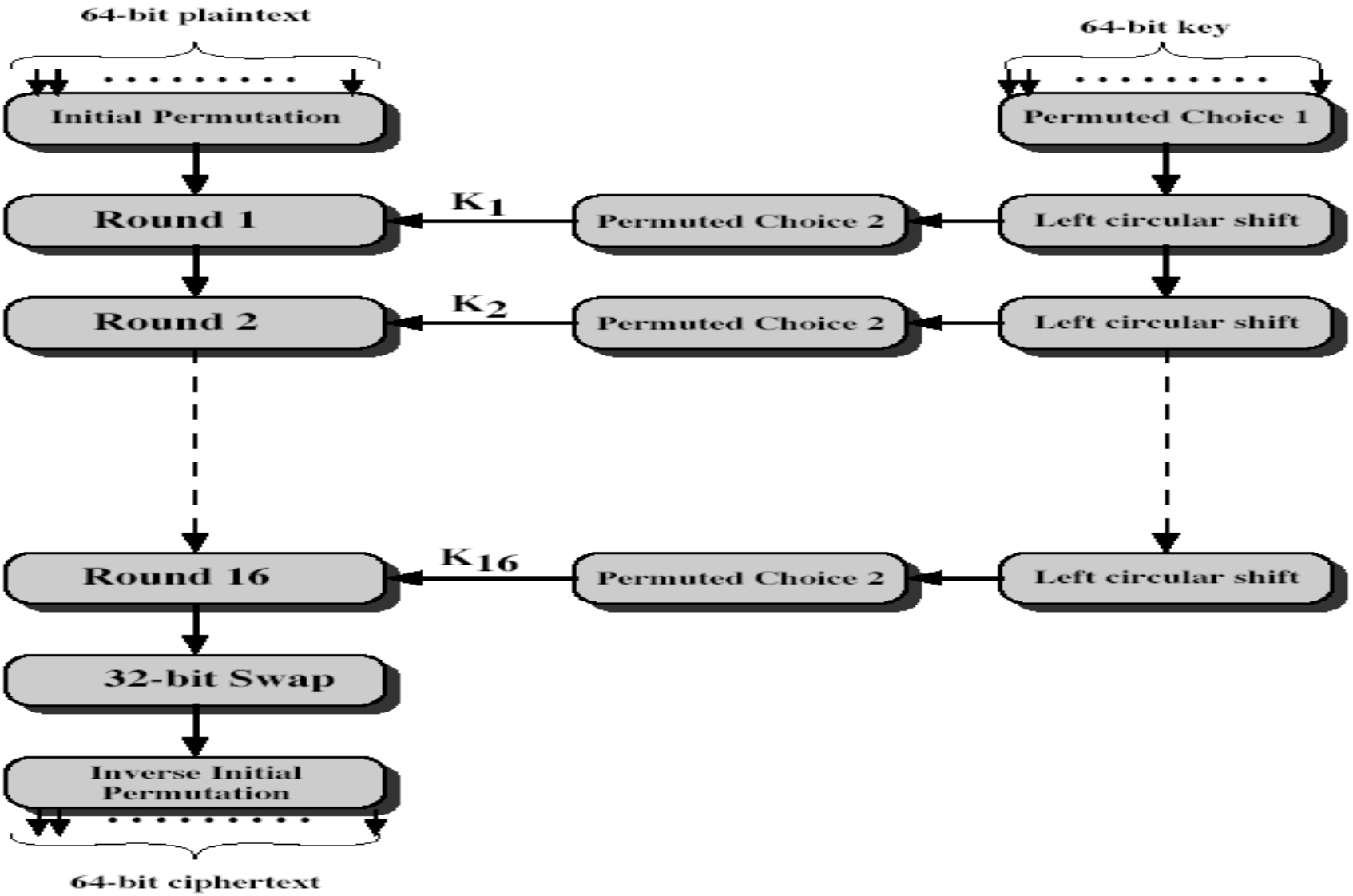
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T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

Algorithmes Cryptographiques Symétriques

DES
IDE
AES

DES

Chiffrement DES



IDE

AES

- AES

Avantages et Inconvénients

Modes Opératoires

- La méthode par laquelle le texte clair est traité
- Cryptage par flux (stream cipher)
  - Opère sur un flux continu de données
  - Mode adapté pour la communication en temps réel
  - RC4 (longueur de clé variable, généralement 128 bits)
- Cryptage par bloc (Block Cipher)
  - Opère sur des blocs de données de taille fixe (généralement 64 bits)
    - Electronic Code Block (ECB)
    - Cipher Block Chaining (CBC)
  - Implémentation logicielle en générale
  - Exemples: DES (Clé: 56 bits codée sur 64 bits); 3DES (EDE (Encrypt-Decrypt-Encrypt), Trois clés distincts ou seulement deux); IDEA (128 bits); AES longueur de clé variable: 128, 192, 256)

Stream Cipher

- traite les éléments d'entrée de façon continue, produisant un élément de sortie (crypté), à la fois.
  - La clé est aussi longue que le *stream* de données.
  - Étapes:
    - Définition de l'état initial du *key stream*
    - Définition de la fonction état suivant: *next-state function*
    - Combinaison du *key stream* courant avec la clé K et les caractères précédents. La fonction de sortie doit aussi modifier l'état interne.
    - Crypte chaque caractère x_i du texte clair avec un caractère z_i du *key stream (exemple xor)*

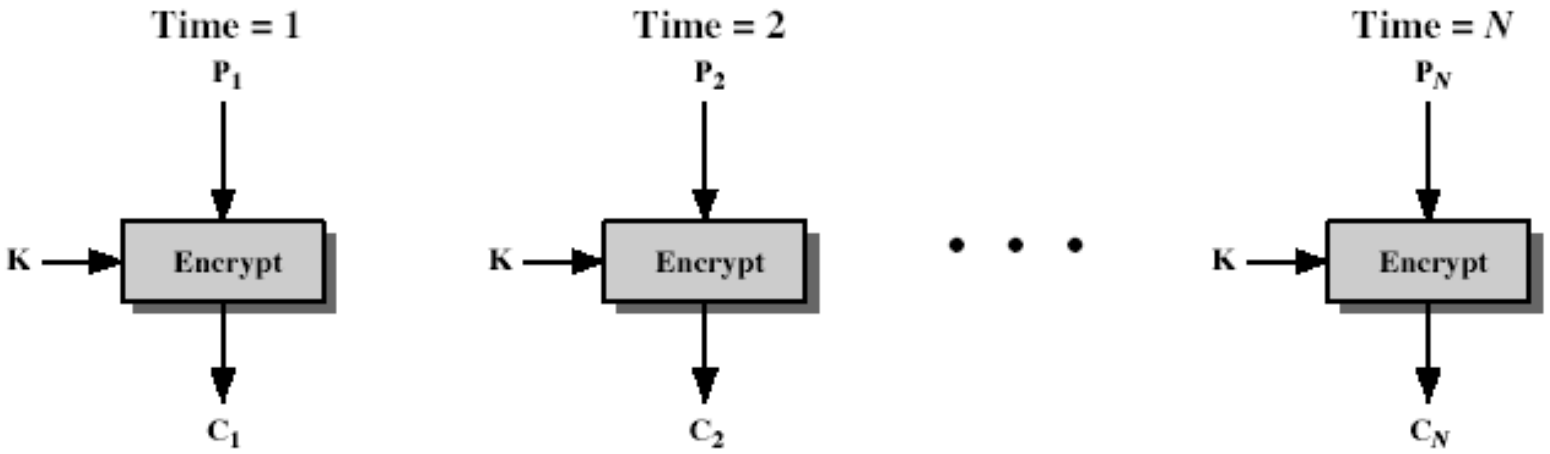
Stream Cipher (suite)

- Pour un texte clair $P=x_1x_2x_3x_4x_5\ldots$ et une clé $I=I_1I_2I_3I_4I_5\ldots$ il existe une fonction de cryptage E_I et des algorithmes de cryptage E_{I_i} tel que:
  - $C = E_I(P)$
  - $C = E_{I_1}(x_1)E_{I_2}(x_2)\ldots$
  - $I_i = f(k, x_1, x_2, x_{i-1})$
- Les valeurs $I_1, I_2, I_3, I_4, \ldots$ sont appelées *key streams*
- *Synchronous cypher:* Le *key stream* ne dépend pas du texte clair. La période du *key stream* est égale à d tel que: $I_{i+d}=I_i$
- *Self-synchronizing*: le *key stream* dépends de n caractères clairs précédents.

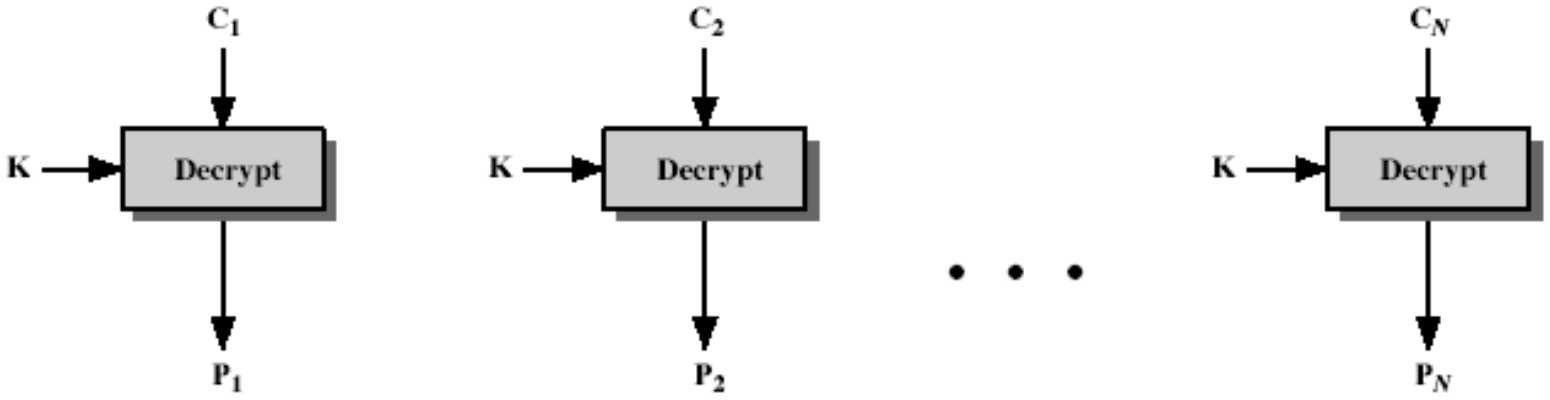
Block Cipher

- *Block Cypher*: Le texte est divisé en différents blocks de taille fixe. Un block est traité à la fois, produisant un block de données cryptées.
- Sans mémoire. La même fonction et la même clé est utilisée pour crypter les blocks successifs.
- Mode d'utilisation:
  - Electronic Code Block (ECB): Chaque block de données est crypté indépendamment, et les blocks cryptés ne sont pas liés
    - ➔ non sécurisé pour les messages longs à cause de la répétition du code
  - Cipher Block Chaining (CBC): Le résultat d'une étape est utilisé pour modifier les données d'entée de la prochaine étape
    - ➔ besoin d'un vecteur d'initialisation connu d'avance.

Electronic Code Block (ECB)



(a) Encryption



(b) Decryption

Cipher Block Chaining (CBC):