

Sécurité et Réseaux

Licence 3 Informatique



Cours 1: Introduction

Osman SALEM

Maître de conférences - HDR

osman.salem@parisdescartes.fr



MATHÉMATIQUES ET INFORMATIQUE

Sciences

Université de Paris

1



Objectif de l'ECUE

- Renforcer vos connaissances en réseaux:
 - Réseaux Avancés: réseaux du semestre 5 + techniques avancées
 - Approfondir et compléter vos connaissances en réseaux:
 - Protocoles et services
 - Pas de retours sur ce que vous avez vu en réseaux (ARP, IP, adressage et subnetting)
 - Continuité et initiation à la configuration des équipements CISCO
 - Initiation à la Sécurité des réseaux
 - Vulnérabilités et attaques
 - Outils et systèmes cryptographiques: chiffrement symétrique
 - Protocoles de sécurité
 - Hacking: Catch The Flag and Hack The Box.

2



Organisation de l'enseignement

- Responsable: M. Osman SALEM
- 12 semaines avec :
 - 1h30 de cours (Vendredi de 11h15-12h45) : Curie A
 - 3h de TD/TP
 - 3 groupes
 - 1 groupe le Mardi et 2 groupes le Jeudi après-midi
- Quelques site utiles...
 - Moodle de l'UFR Math-Info
 - <https://moodle.parisdescartes.fr/>
 - Support du cours/TD/information diverses
 - Courriels pour rappeler les dates des partiel

3



Planning 2020

Semaine	Semaine	Cours	TD	commentaires
S1	17/01	1		
S2	24/01	2	1	
S3	31/01	3	2	
S4	07/02	4	3	
S5	14/02	5	4	
S6	28/02	6	5	Partiel 1
S7	06/03	7	6	
S8	13/03	8	7	
S9	20/03	9	8	
S10	27/03	10	9	
S11	03/04	11	10	Partiel 2
S12	10/04	12	11	
S13	17/04	13	12	Partiel 3

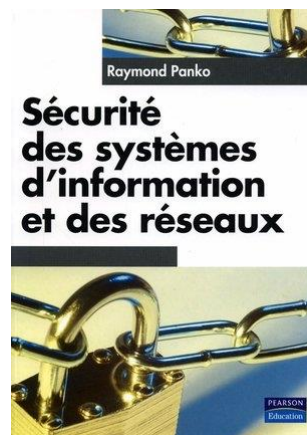
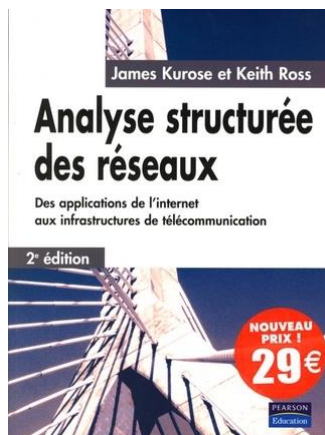
4

Evaluation

- Modalité de calcul de la note finale de l'U.E.
 - Contrôle Continu
 - Partiel 1
 - Partiel 2
 - Partiel 3

5

Bibliographie



6



Plan

- 2 Parties
 - Sécurité
 - Chiffrement symétrique
 - Intro au chiffrement asymétrique
 - Compromettre une machine: Intrusion
 - Réseaux
 - Prise en main des outils de configuration
 - Cisco Packet Tracer
 - Ou sur un switch réel

7



Plan

- Cours 1: Introduction à la sécurité
- Cours 2: Chiffrement symétrique: Scytale, Substitution, Transposition
- Cours 3: César, Vignère, Auto-Chiffrement, Playfair, Rail Fence
- Cours 4: Enigma, Stéganographie, Kerberos
- Cours 5: Introduction au chiffrement asymétrique
- Cours 6: Démonstration d'une intrusion
- Cours 7 : Initiation à la configuration des équipements CISCO
- Cours 8 : Configuration de Switch CISCO
- Cours 9: Configuration des Routeurs CISCO
- Cours 10: Configuration du protocole de routage RIP

8



Travaux dirigés et pratiques

- TDs et TPs
 - Exercices et problèmes illustrant les concepts présentés en cours
 - Questions et rappel de cours
 - Tous les exercices proposés ne seront pas traités en TD
- Outils
 - Mot de passe en clair avec Telnet et FTP
 - Wireshark
 - Secure Shell: SSH, SCP et SFTP
 - CISCO Packettracer
 - RADIUS, DHCP et DNS

9



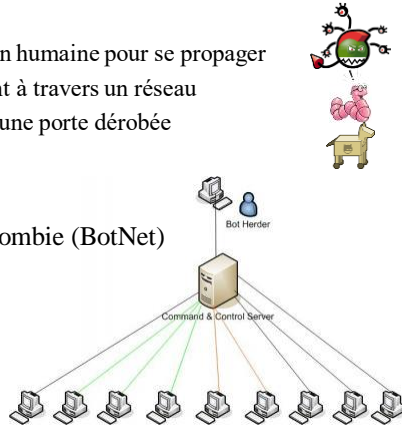
Partie I: la sécurité des réseaux

Introduction

10

Logiciel malveillant

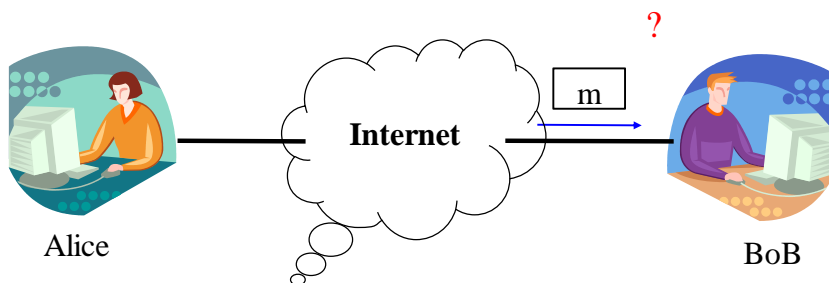
- Logiciel malveillant
 - Objectif: nuire au système
 - Virus, Vers, cheval de Troie
 - Virus: besoin d'une intervention humaine pour se propager
 - Vers: se reproduit en s'envoyant à travers un réseau
 - Cheval de Troie: installation d'une porte dérobée
 - Suppression des fichiers
 - Installation d'un logiciel espion
 - Transformer notre machine en zombie (BotNet)



11

Ce qui peut mal se passer...

- ...quand l'ordinateur de BoB reçoit ou s'attend à recevoir un message *m* ?



12

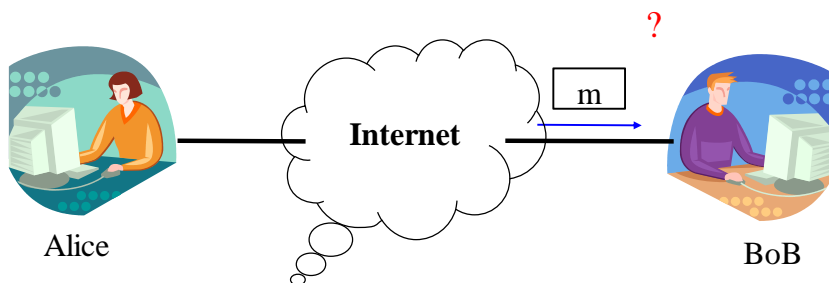
Qui sont Bob et Alice?

- ... dans la vie réelle, qui sont Alice et Bob ?
- Navigateur/serveur web pour le commerce électronique (achat on-line)
- Banque on-line client/serveur
- Serveurs DNS
- Routeurs qui transmettent leurs tables de routage

13

Ce qui peut mal se passer...

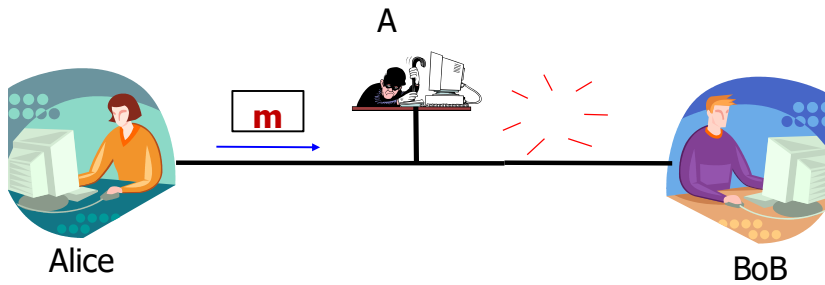
- ...quand l'ordinateur de BoB reçoit ou s'attend à recevoir un message *m* ?



14

Une perte de message

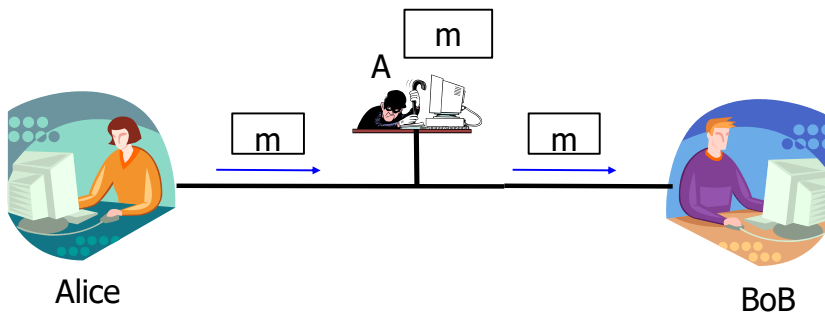
- Un adversaire **A** a fait disparaître le message **m** au cours de la transmission



15

Une interception de message

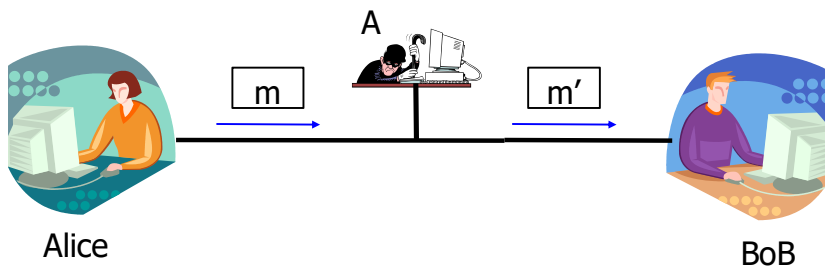
- Un adversaire A a constitué une copie de **m** quand il est passé



16

Une modification de message

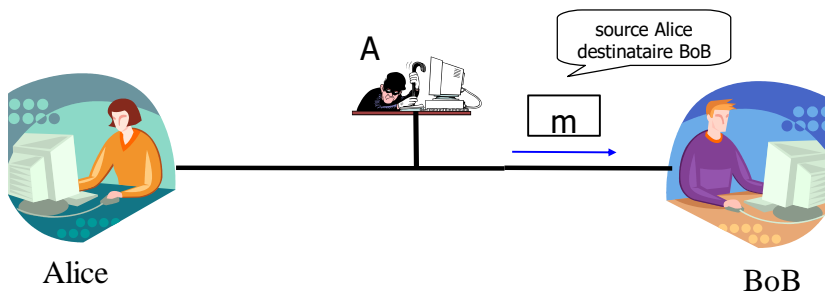
- Un adversaire A a modifié le contenu du message m qui est devenu m'



17

Une insertion de message

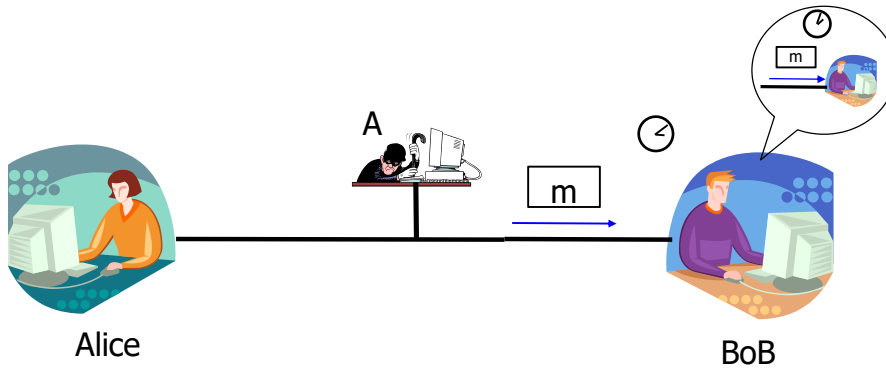
- Un adversaire A a fabriqué un message m , en prétendant que c'est Alice qui en est l'émetteur (**usurpation d'identité**)



18

Une duplication de message

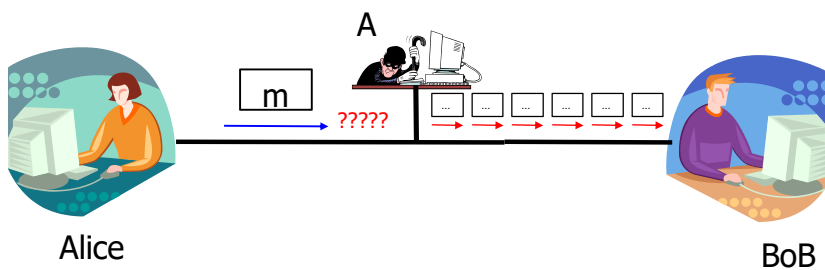
- Un adversaire A a envoyé de nouveau un message **m** qui avait été envoyé auparavant par Alice et reçu par BoB (“**rejeu**”)



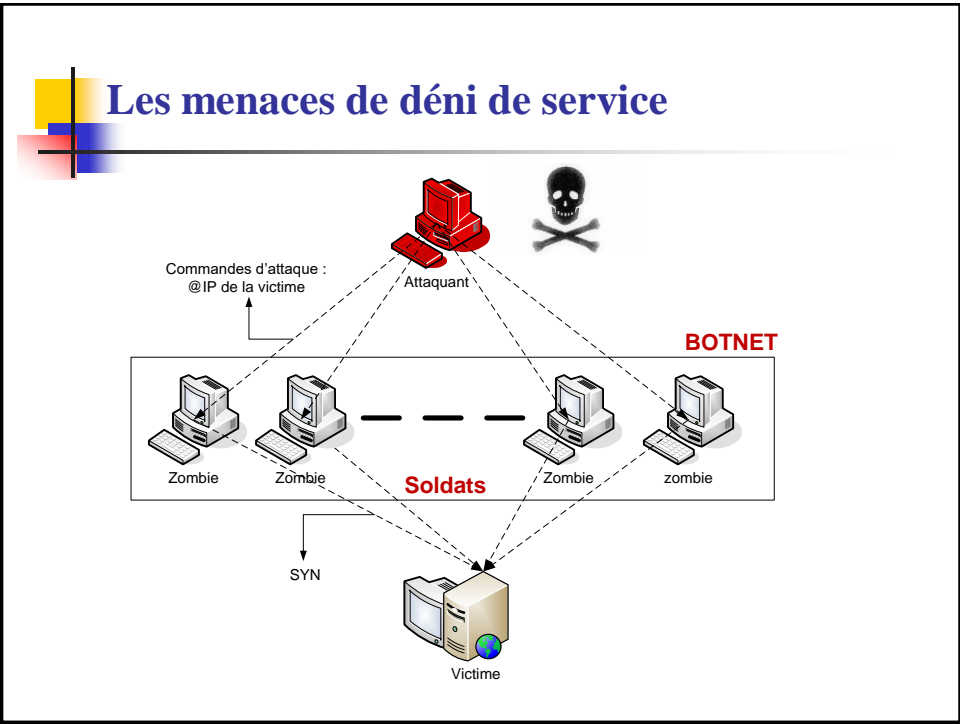
19

Un déni de service

- Un adversaire A peut bloquer le message **m** en submergeant BoB de messages



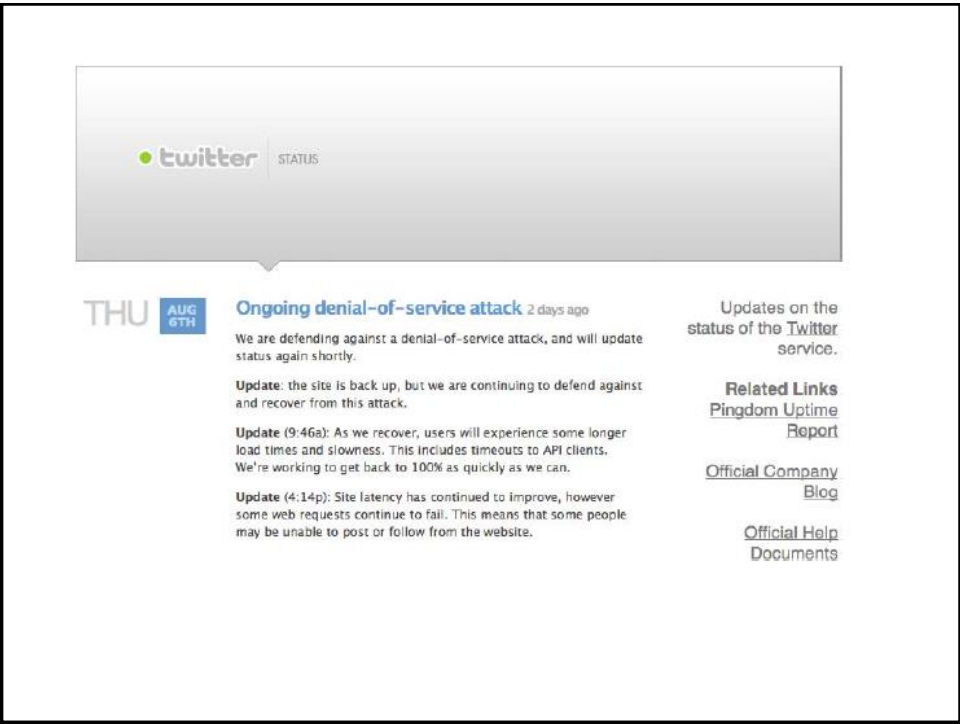
20



21



22



23

DDoS

- Distributed Denial of Service
 - Recently many servers were victims of DDoS

14 August 2012 Last updated at 10:26 GMT

Wikileaks website back online after DDoS cyber-attack

CNET › News › Security & Privacy › WikiLeaks endures a lengthy DDoS attack

WikiLeaks endures a lengthy DDoS attack

Under a barrage of more than 10GB per second in a DDoS attack, the document-leaking organization's Web site has been either inoperable or sluggish since the beginning of the month.

Federal prosecutors shut down file-sharing service Megaupload.com on Jan. 19 for distributing illegal content in one of the largest online piracy crackdowns in Internet history and arrested four individuals.

Opera

@Anon_Operation
Operation Payback

FBI,

had
mous
DoS

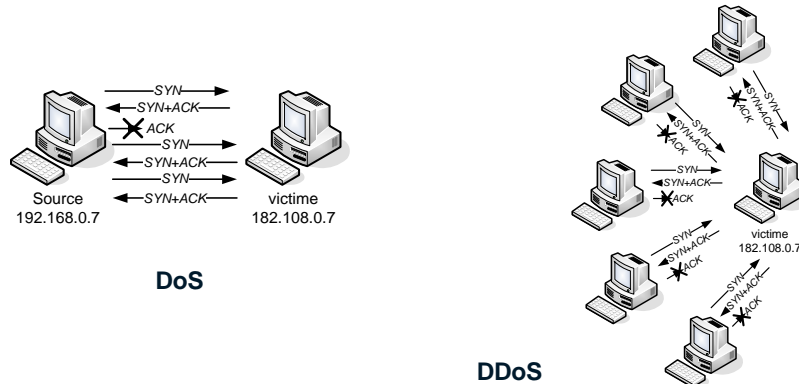
low
aws.
bout

24

24

DoS, DDoS: SYN Flooding

- SYN FLOOD: inondation SYN
 - Un attaquant harcèle le serveur avec TCP SYN (demande d'ouverture d'une connexion)
 - Mais il ne répond pas au message final
 - TCP instaure une connexion semi-ouverte pour quelques minutes (~75s)
 - Les messages SYN peuvent engorger le module TCP



25

Mnémonique

- Qu'est ce qu'un **hacker** ? **Cracker** ?
 - Un hacker est une personne qui veut comprendre les choses ...
 - ... jusqu'au moindre détail
 - Comment devenir un Hacker ?
 - Crackers: exploitation des connaissances avec des mauvaises intentions
- Qu'est ce qu'un script kiddie ?
 - Outils d'exploitation de vulnérabilités facile à utiliser
- Pourquoi les autres essaient d'accéder d'une façon illégale à notre système ?
 - Curiosité, revanche, extorsion de fond, terrorisme, vol de ressources, vandalisme, etc.

26



Les différents types d'attaques

■ Attaques passives

- Analyse de trafic
- Interception de message

■ Attaques actives

- Perte de message
- Modification de message
- Insertion de message
- replay
- déni de service

27



Méthodes d'attaques

■ Ecoute passives

- Obtenir une copie de l'information sans autorisation
- Login et Mot de Passe

■ Usurpation d'identité

- Transmission de messages avec autres identité

■ Modification

- Changement du contenu

28



Méthodes d'attaques

- Rejeu
 - Enregistrement du trafic et re-injection
 - Ex: retransmission du message de paiement
- Exploitation
 - Utilisation d'une vulnérabilité d'un logiciel pour obtenir un accès
- MITM: Man In The Middle
 - Interception de communications entre différents partenaires

29



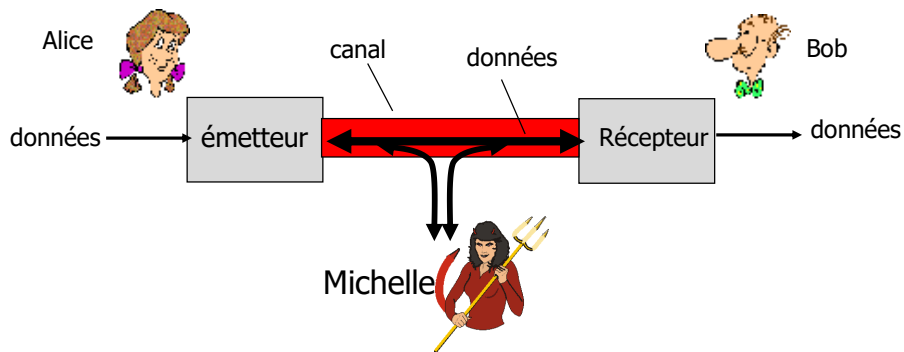
Les services de sécurité

- | | |
|--------------------|--------------------|
| ■ Confidentialité | ■ Disponibilité |
| ■ Intégrité | ■ Contrôle d'accès |
| ■ Authentification | ■ Non-répudiation |
| ■ Anti-rejeu | ■ Anonymat |

30

Confidentialité

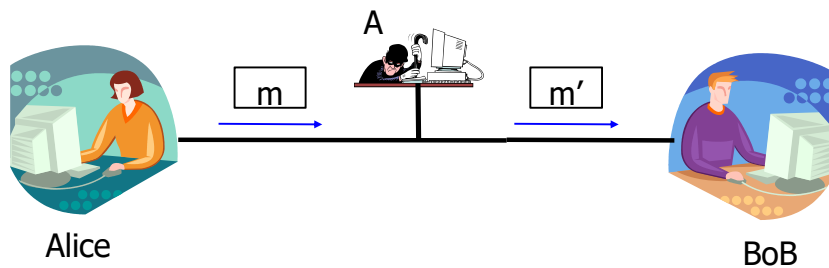
- Seul le récepteur patenté du message peut lire le message, celui-ci reste secret (ou inexploitable) pour tous les autres utilisateurs
 - **Empêcher les utilisateurs malicieux de lire une information confidentielle**



31

Intégrité

- Quand le récepteur reçoit le message m , il peut vérifier que celui-ci est intact, c'est-à-dire égal au message que l'émetteur a envoyé
 - **L'information n'est pas été altérée durant son transfert**
 - Objective: empêcher un modification par des utilisateurs malicieux



32

Authentication

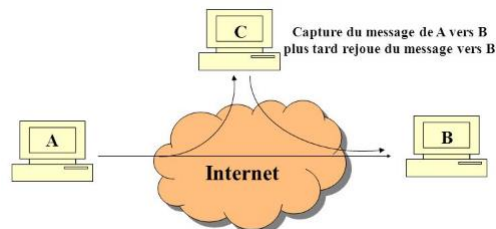
- Quand le récepteur reçoit le message **m**, il peut vérifier que c'est bien l'émetteur **Alice** qui l'a envoyé
 - La preuve s'appuie sur un **secret** que connaît l'utilisateur
 - Mot de passe
 - La preuve s'appuie sur un **objet** unique que possède l'utilisateur
 - La preuve s'appuie sur une caractéristique **physique** de l'utilisateur
 - Techniques biométriques
 - Empreintes digitale, rétine de l'œil, vocale
 - Forme du visage
 - Etc.
 - Pas très précis



33

Anti-rejeu

- Quand le récepteur reçoit le message **m**, il peut vérifier si celui-ci est bien un nouveau message (le message **m** n'a pas déjà été émis et reçu...)



34



Disponibilité

- Propriété d'un système à être accessible et utilisable par tout utilisateur autorisé
 - Accessible lorsqu'un utilisateur autorisé en a besoin

35



Contrôle d'accès

- Mécanisme destiné à gérer les droits d'accès aux ressources et aux données
- Les utilisateurs ne peuvent accéder qu'aux ressources et données pour lesquels ils disposent spécifiquement des droits
- Les utilisateurs ne peuvent pas accéder aux ressources et données pour lesquels ils ne disposent pas des droits

36

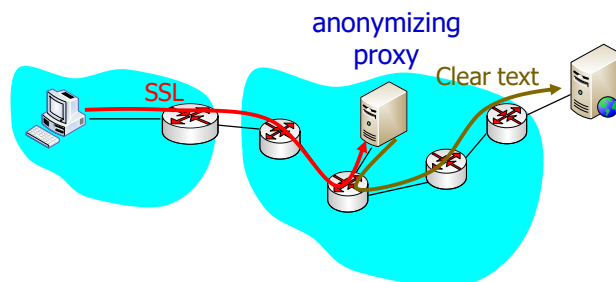
Non-répudiation

- Quand le récepteur reçoit le message **m**, il peut être certain que l'émetteur du message a effectivement envoyé un message
- Le récepteur peut montrer la preuve à une tierce partie, preuve que l'émetteur ne peut pas nier
- Quand le récepteur reçoit le message **m**, l'émetteur du message peut être certain que **m** a été effectivement reçu
- L'émetteur peut montrer la preuve à une tierce partie, preuve que le récepteur ne peut pas nier

37

Anonymat

- L'identité de l'émetteur est cachée au récepteur
- Quand le récepteur reçoit le message **m**, il n'a aucune indication quant à l'émetteur du message
- Ex: Proxify.com



38

2. Cryptographie

Introduction

39



La cryptographie

- Elle est caractérisée par
 - Le type des opérations de chiffrement utilisées
 - substitution / transposition / produit
 - Le nombre des clés utilisées
 - Clé unique partagée / paire de clés ou clés publiques
 - La façon dont le message en clair est traité
 - Par bloc / en flux

40



La sécurité apportée par la cryptographie

- Sécurité inconditionnelle
 - Quelles que soient les ressources de calcul disponibles, le message chiffré ne peut pas être cassé car il contient des informations insuffisantes pour reconstruire de manière unique le message en clair correspondant
- Sécurité "liée au coût des calculs"
 - Avec des ressources de calcul limitées (par exemple, le temps des calculs est égal à l'âge de l'univers), le message chiffré ne peut pas être cassé

41



Chiffrement symétrique

- Emetteur et récepteur *partagent* une même clé secrète
- Tous les algorithmes de chiffrement classiques appartiennent à cette famille
- C'était l'unique méthode de chiffrement avant les années 1970 et l'invention des systèmes à clés publiques

42

Cryptographie: définition

- C'est la science qui étudie les principes, méthodes et techniques mathématiques pour réaliser la sécurité de l'information
- Pour une utilisation sûre, il faut
 - Un algorithme de chiffrement solide "**E**" (Encryption ou chiffrement)
 - Une clé secrète "**K**" connue seulement de l'émetteur et du récepteur

$$C = E_K(M)$$

$$M = D_K(C) = D_K(E_K(M))$$

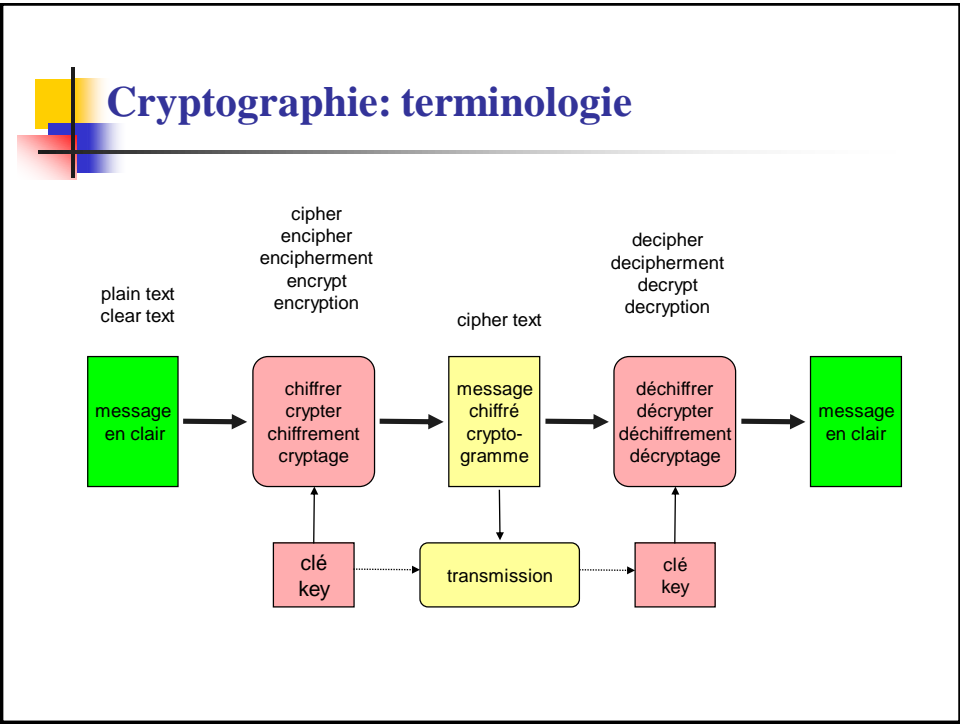
Ex: message en clair: *Bob, je t'aime. Alice*
 message chiffré: *CPC, KF U'BJNF. BMJDF*

43

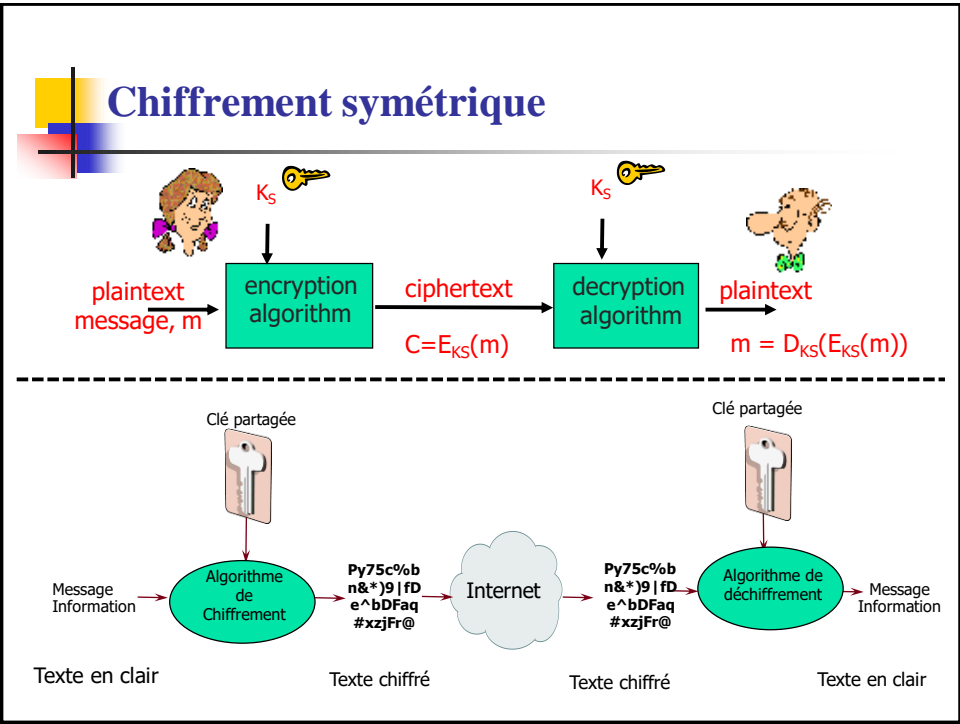
Cryptographie : synonymes

- **Message en clair** = message original = *plaintext*
- **Message chiffré** = ciphertext – *message original*
- **(algorithme de) Chiffrement** = cipher - algorithme de transformation du message en clair en message chiffré
- **Clé** = key – information utilisée dans l'algorithme de chiffrement et connue des seuls émetteur et récepteur
- **Chiffrer, crypter** = *encipher, encrypt* - convertir le message en clair en message chiffré
- **Déchiffrer, décrypter** = *decipher, decrypt* – restaurer le message en clair à partir du message chiffré
- **Cryptographie** = étude des principes et méthodes de chiffrement
- **Cryptanalyse** = *codebreaking* - étude des principes et méthodes de déchiffrement sans connaissance des clés
- **Cryptologie** = domaine complet comprenant la cryptographie et la cryptanalyse

44



45



46

Cryptanalyse

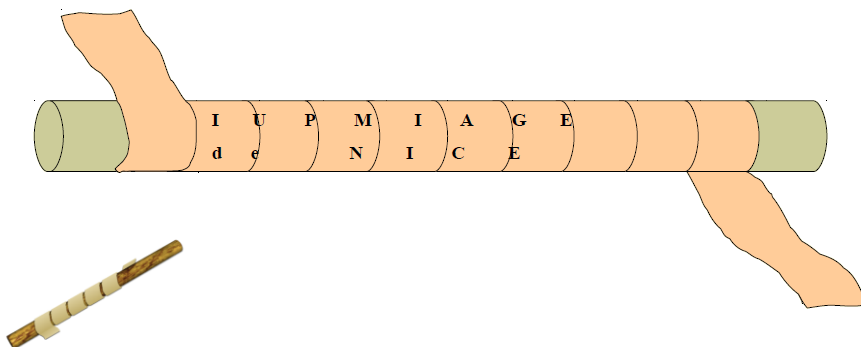
- La sécurité d'un système de chiffrement doit reposer sur
 - le secret de la clé de chiffrement
 - et non pas sur celui de l'algorithme
- Le **principe de Kerkhoff** suppose en effet que l'attaquant connaît l'algorithme utilisé
 - L'algorithme est connu
 - La clé est **secrète**
- Il faut donc une solution sûre pour transmettre la clé de l'émetteur au récepteur => rôle des **protocoles d'échange de clés**

47

Chiffrement symétrique



- Grèce antique: la **scytale** utilisée à Sparte (**Spartiates**)
 - Algorithme : texte écrit sur un ruban enroulé autour d'un bâton
 - Clé : diamètre du bâton



48



Chiffrement symétrique

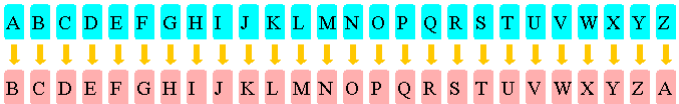
- Les algorithmes de chiffrement symétrique se fondent sur **une clé unique** pour chiffrer et déchiffrer un message
 - Clé unique partagée
- **Basée sur 2 mécanismes**
 - Substitution
 - Permutation

49

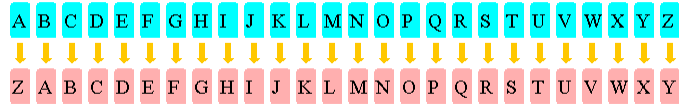


Substitution

- Substitution: Ex1: chiffrement par décalage



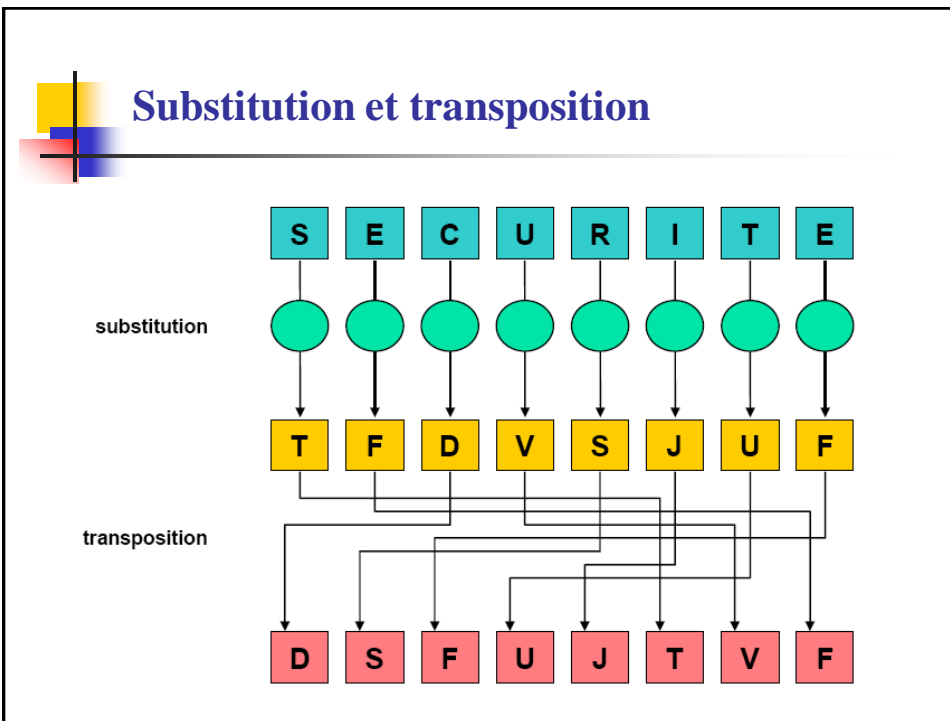
- Substitution alphabétique inversée



- Substitution, Ex3: utilisation de tables d'association

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

50



51

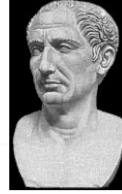
Méthode classique de substitution

- Les lettres du message en clair sont remplacées par d'autres lettres, des chiffres ou d'autres symboles
- Si le message en clair est vu comme une suite de données binaires, ce sont des séquences de bits qui seront remplacées par d'autres séquences de bits

<u>input</u>	<u>output</u>	<u>input</u>	<u>output</u>
000	110	100	011
001	111	101	010
010	101	110	000
011	100	111	001

52

Le code de César



- Plus ancien code de substitution connu
- Inventé par Jules César
- Utilisé pour des affaires militaires
 - Chaque lettre est remplacée par celle qui est située trois (par exemple) lettres après dans l'alphabet
- Exemple

Rendezvousapreslecours

UHQGH CYRXVDSUHVOHFRXUV

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

<http://www.bibmath.net/crypto/substi/cryptcesar.php3>

53

Mécanisme du code de César

- Une transformation

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
- En associant une valeur numérique à chaque lettre

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
- $C = E_3(m) = (m + 3) \bmod (26)$
 $m = D_3(C) = (C - 3) \bmod (26)$

54



Cryptanalyse du code de César

- 26 possibilités de codage
 - "A" est transformé en "A", "B", ... ou "Z"
- Ce code est facilement cassé par attaque brute
 - Il suffit d'essayer les 26 solutions !
- Pour cela, il faut pouvoir reconnaître le message en clair
- Essayez "HCEKNG FG FGEJXHHTGT"

55



Cryptanalyse du code de César

- 26 possibilités de codage
 - "A" est transformé en "A", "B", ...ou "Z"
- Ce code est facilement cassé par attaque brute
 - Il suffit d'essayer les 26 solutions !
- Pour cela, il faut pouvoir reconnaître le message en clair
- Essayez "HCEKNG FG FGEJXHHTGT"
 - A → C
 - FACILE DE DECHIFFRER

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
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
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

<http://www.bibmath.net/crypto/substi/cryptcesar.php3>

56



Codage monoalphabétique

- Meilleur qu'un simple décalage des lettres
- Les lettres sont codées "au hasard"
- Cela revient à un code dont la clé serait longue de 26 lettres
- Exemple
 - clair: **abcdefghijklmnopqrstuvwxyz**
 - chiffré: **DKVQFIBJWPESCXHTMYAUOLRGZN**
 - Message en clair: **etsinousreplacionsleslettres**
 - Message chiffré: **FUAWXHOAYFTSDWHXASFYSFUUYFA**

57



Sécurité apportée par un code monoalphabétique

- Nous avons $26! \geq 4 \times 10^{26}$ clés
- Avec un tel nombre de clés, on pourrait croire que le système est sûr
- Il y a malheureusement un problème : les langues naturelles ont des caractéristiques bien connues !

58



Cryptanalyse

- Les méthodes de chiffrement par substitution ne changent pas la fréquence des lettres
- Découverte des scientifiques arabes au IX^e siècle
 - Al-Kindi
- Il suffit de calculer la fréquence des lettres dans le message chiffré et de comparer avec les fréquences connues
- Idée: examiner la fréquence des lettres d'un message chiffré.

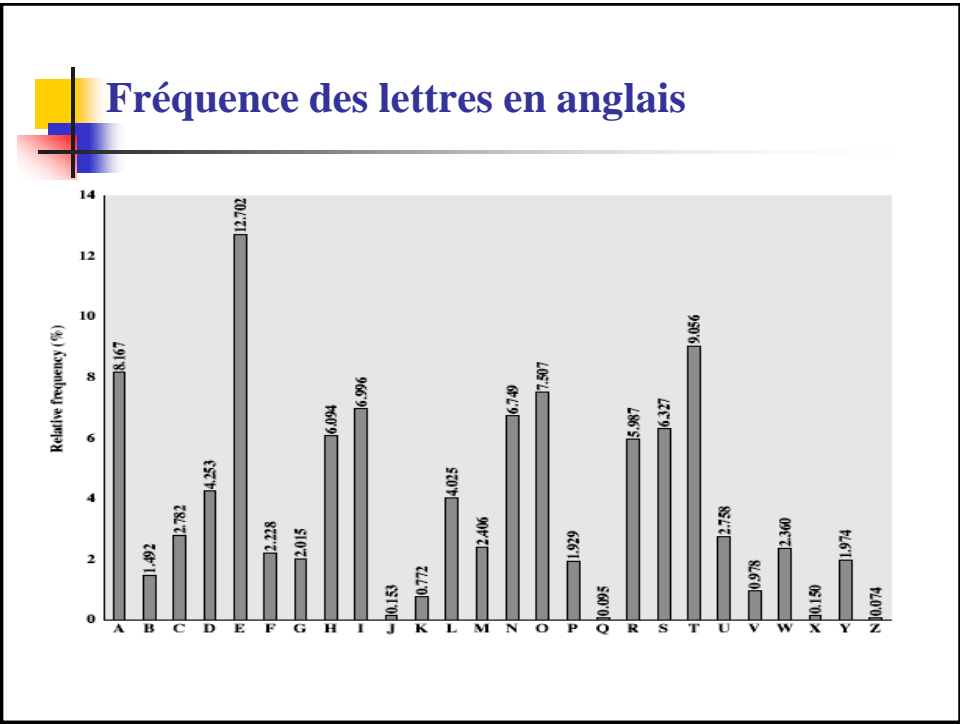
59



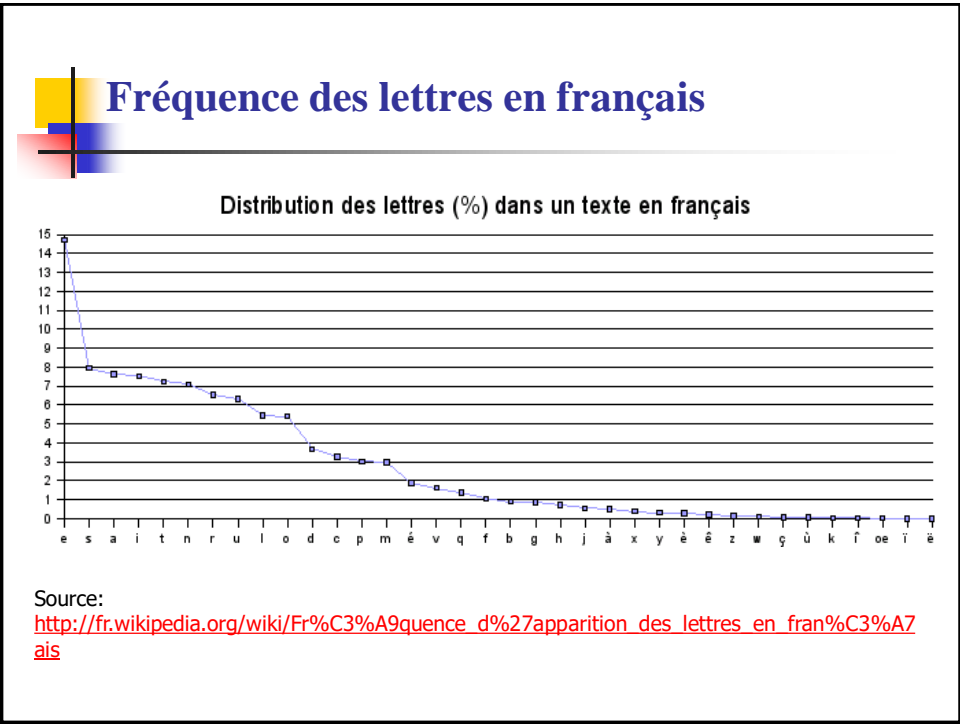
Statistiques de la langue et Cryptanalyse

- Les lettres ont des fréquences d'apparition différentes :
 - En anglais, "E" est la lettre la plus fréquente, suivie par "T", "A", "O", "I", "N", "S", "H", "R"
 - Certaines lettres "Z", "J", "K", "Q", "X" sont rares
 - Il existe des tables de fréquences des digrammes (deux lettres consécutives), trigrammes (trois lettres consécutives),...
- En **français**, "**E**" est la lettre la plus fréquente, suivie par "**S**", "**A**", "I", "T", "N", "R", "U", "L", "O",
 - Certaines lettres "J", "X", "Y", "W", "K" sont rares
 - Il existe des tables de fréquences des **digrammes** (deux lettres consécutives), **trigrammes** (trois lettres consécutives),...

60



61



62



Cryptanalyse

- Les méthodes de chiffrement par substitution ne changent pas la fréquence des lettres
- Il suffit de calculer la fréquence des lettres (des digrammes, des trigrammes) dans le message chiffré et de comparer avec les fréquences connues
- Pour le code de César (en français)
 - E, S, A les lettres les plus fréquentes, ES, EN, LE et DE sont les digrammes les plus fréquents, ENT, LES et ION les trigrammes les plus fréquents
 - Les raretés : y w k

63



Chiffrement "playfair"

- La substitution monoalphabétique ne suffit pas à apporter une sécurité suffisante
- Une approche "polyalphabétique" permet d'améliorer la sécurité
- Exemple : playfair

64



Matrice de lettres

- Une matrice 5X5 basée sur un mot-clé
- On place (sans espaces et sans duplication) les lettres du mot-clé
- On remplit le reste de la matrice avec les lettres restantes
- Par exemple avec le mot **MONARCHIE**

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

<http://www.apprendre-en-ligne.net/crypto/subst/playfair.html>

65



Chiffrement

- Le message en clair est chiffré en prenant les lettres deux par deux
 - Message en clair = **loup blanc**
 - Chaque groupe de 2 lettres est codé par la lettre à l'intersection de la ligne de la première et la colonne de la seconde puis à l'intersection de la ligne de la seconde et de la colonne de la première
 - Si les deux lettres tombent sur la même ligne, on remplace chacune par celle de droite ; Si les deux lettres tombent sur la même colonne, on remplace chacune par celle de dessous (avec rotation circulaire)
 - En cas de lettre double, et en cas de lettre unique (nombre total de lettres impair), une lettre "parasite" est insérée (w)
 - Exemple : LO UP BL AN CW
 - Chiffré en : PM VL CT RA IU

66



Déchiffrement

- Le message chiffré est lu en prenant les lettres deux
- par deux
 - Message chiffré = PM VL CT RA IU

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

- PM → ligne de P et colonne de M : intersection = L ; colonne de P et ligne de M : intersection = O

67



Déchiffrement

- Le message chiffré est lu en prenant les lettres deux
- par deux
 - Message chiffré = PM **VL** CT RA IU

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

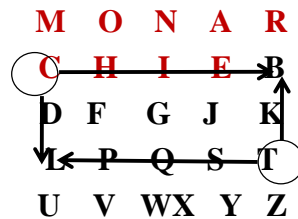
- PM → ligne de P et colonne de M : intersection = L ; colonne de P et ligne de M : intersection = O
- VL → ligne de V et colonne de L : intersection = U ; colonne de V et ligne de L : intersection = P

68



Déchiffrement

- Message chiffré = PM VL **CT** RA IU



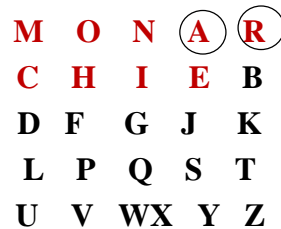
- PM → ligne de P et colonne de M : intersection = L ; colonne de P et ligne de M : intersection = 0
- VL → ligne de V et colonne de L : intersection = U ; colonne de V et ligne de L : intersection = P
- CT → ligne de C et colonne de T : intersection = B ; colonne de c et ligne de T : intersection = L

69



Déchiffrement

- Message chiffré = PM VL CT **RA** IU



- PM → ligne de P et colonne de M : intersection = L ; colonne de P et ligne de M : intersection = 0
- VL → ligne de V et colonne de L : intersection = U ; colonne de V et ligne de L : intersection = P
- CT → ligne de C et colonne de T : intersection = B ; colonne de c et ligne de T : intersection = L
- RA → sont sur la même ligne donc décalage vers la gauche ==AN
Puis IU donne C et W ou X (lettre parasite)

70



Sécurité apportée par ce code

- Nettement meilleure qu'un code monoalphabétique
- Possède 26x26 combinaisons au lieu de 26 avec un code monoalphabétique
- Nécessite la connaissance de plusieurs échantillons de messages chiffrés... mais peut tout de même être cassé !

71



Code de vigenère

- Le premier et le plus simple, utilise plusieurs codes de César
- La clé possède d lettres $K = k_1 k_2 \dots K_d$
- $i^{\text{ème}}$ lettre détermine le $i^{\text{ème}}$ alphabet à utiliser
- Exemple avec le mot-clé **MONARCHIE**
- key: monarchiemonarchiemonarchiem
- plaintext: ausecoursnousommesdecouverts
- ciphertext: MIFETQBZWZCHSFOTMWSPOLXLZXE

72



Code 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
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

73



Sécurité du code de Vigenère

- Une lettre du message en clair est transformée en plusieurs lettres différentes dans le message chiffré : cela brouille les fréquences
- Recherche des fréquences d'occurrence
 - Recherche de la longueur du mot clé en découpant le message chiffré en blocs de toutes les tailles possibles
- Les répétitions dans le message chiffré peuvent donner des indications

74



Auto-Chiffrement

- Pour éliminer la nature **périodique** du code précédent, la clé n'est utilisée qu'une seule fois, en préfixe du message
- Le message lui-même devient la suite de la clé
- Exemple avec **MONARCHIE**
plaintext: ausecoursnoussoyonsdecouverts
key: monarchieausecoursnoussoyonsd
ciphertext: ...

75



Les chiffrements par tranposition

- Permet de mieux cacher le message en changeant l'ordre des lettres
- Peut même être utilisé sans changer les lettres elles-mêmes ce que l'on pourra reconnaître puisque toutes les fréquences d'apparition seront conservées...

76



Chiffrement “Rail Fence”

- Ecrire le message en posant les lettres en diagonale sur un certain nombre de lignes
- Puis lire le message ligne par ligne
- exemple

```

r   n   e   v   u   a   r   s   e   o   r
     e   d   z   o   s   p   e   l   c   u   s

```

le message chiffré est : **RNEVUARSEOREDZOSPELCUS**

<http://www.apprendre-en-ligne.net/crypto/transpo/railfence.html>

77



Transposition de colonnes

- Un schéma plus complexe
- Ecrire le message en clair en ligne sur un nombre spécifié de colonnes
- Réordonner les colonnes conformément à la clé

```

Key:      4 3 1 2 5 6 7
          1 2 3 4 5 6 7
Plaintext: r e n d e z v
           o u s a p r e
           s l e c o u r
           s

```

le message chiffré est : **DACNSEROSSSEULEPOZRUV**

78



Chiffrements hybrides

- Les chiffrements utilisant substitutions et transpositions ne sont pas totalement sûrs à cause des caractéristiques statistiques des langues
- On peut imaginer d'en utiliser plusieurs en cascade pour rendre la tâche de l'adversaire plus difficile
 - deux substitutions sont plus complexes qu'une seule, mais cela reste une substitution
 - deux transpositions sont plus complexes qu'une seule, mais cela reste une transposition
 - Mais une substitution suivie par une transposition est beaucoup plus difficile
- Nous arrivons dans le monde du chiffrement moderne...

79



Machines à rotor

- Les machines à rotor ont été les machines les plus répandues, surtout pendant la seconde guerre mondiale
 - Enigma
- Elles implémentaient une méthode de substitution vraiment complexe et variable
- Avec une série de cylindres, chacun définissant une substitution, qui fait tourner et change après chaque lettre chiffrée
- Avec 3 cylindres, $26^3=17576$ alphabets

80

Machines à rotor

- Les travaux commencés par les polonais

[https://fr.wikipedia.org/wiki/Enigma_\(machine\)](https://fr.wikipedia.org/wiki/Enigma_(machine))

Dès 1931, le Service français de renseignement (surnommé le « 2e Bureau ») était parvenu à recruter une source (Hans-Thilo Schmidt) au sein même du bureau du chiffre du ministère de la Reichswehr. Il obtint de lui de premières copies de la documentation ; il les proposa à l'Intelligence Service britannique, qui se montra sceptique, et au service polonais, qui fut très intéressé. Une coopération s'instaura, qui allait durer jusqu'en 1939. Les Français continuèrent de fournir de nouveaux renseignements obtenus de la même source, et les Polonais montèrent une équipe qui parvint à reproduire la machine à partir de la documentation de plus en plus précise qui leur parvenait.

- Transmis à l'ambassade de Grande-Bretagne
 - deux jours avant l'invasion par l'Allemagne
- Les informations obtenues donnaient un net avantage dans la poursuite de la guerre
- Le conflit en Europe s'est considérablement écourté grâce à la cryptanalyse du code allemand

81

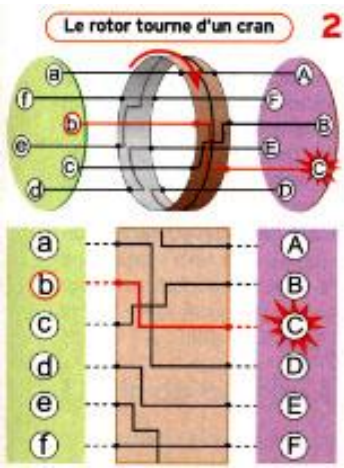
Enigma Machine



82



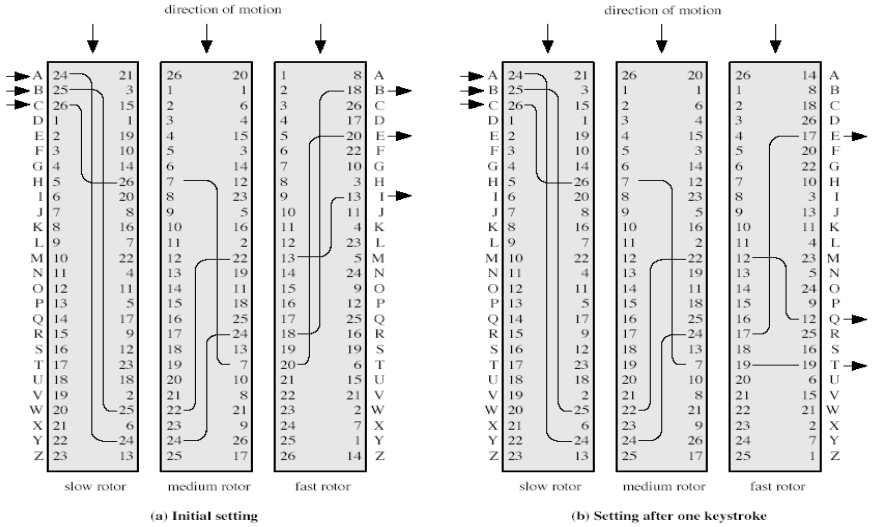
Un exemple de machine à rotor



83



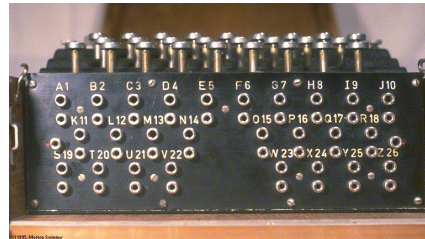
Un exemple de machine à rotor



84

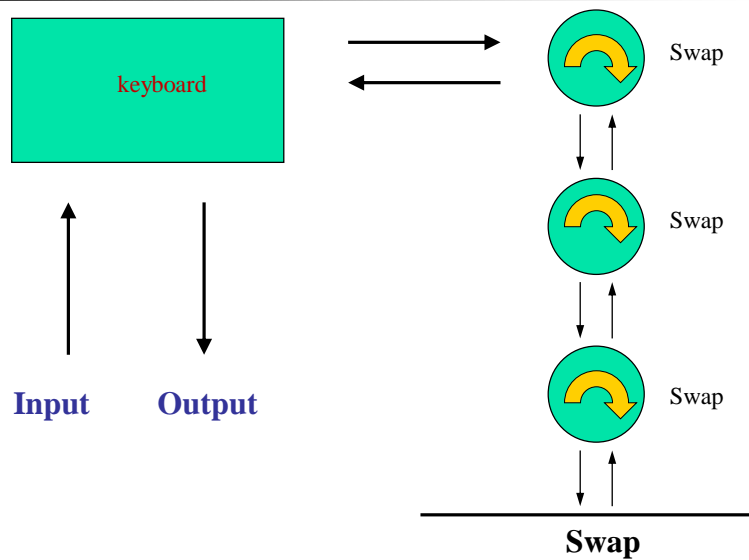
Plug Board

- Changement de lettres avant et après le passage par les cylindres



85

Procédure



86



Stéganographie

- Une alternative au chiffrement ; (du grec steganos, couvert et graphein, écriture)
- Cacher l'existence même des messages
- Utiliser un sous-ensemble de lettres ou de mots dans un message plus long
- Utiliser un pixel précis dans une séquence d'images vidéo...
- Inconvénients
 - Énorme overhead pour cacher peu d'informations

87



Intérêts de la stéganographie

- Communiquer en toute liberté même dans des conditions de censure et de surveillance
- Protéger ses communications privées là où l'utilisation de la cryptographie n'est normalement pas permise ou soulèverait des suspicions
- Contrebalancer toutes les législations ou barrières possibles empêchant l'usage de la cryptographie
- Publier ouvertement (mais à l'insu de tous) des informations qui pourront ensuite être révélées et dont l'antériorité sera incontestable et vérifiable par tous

88



Stéganographie (exemple 1)

■ Alfred de Musset écrit à George Sand :

Quand je vous jure, hélas, un éternel hommage
Voulez-vous qu'un instant je change de langage
Que ne puis-je, avec vous, goûter le vrai bonheur
Je vous aime, ô ma belle, et ma plume en délire
Couche sur le papier ce que je n'ose dire
Avec soin, de mes vers, lisez le premier mot
Vous saurez quel remède apporter à mes maux.



■ George Sand a répondu :

Cette grande faveur que votre ardeur réclame
Nuit peut-être à l'honneur mais répond à ma flamme.



*George Sand est le pseudonyme d' **Amandine Aurore Lucile Dupin**

89



Stéganographie (exemple 2)



- <http://lwh.free.fr/pages/algo/crypto/steganographie.htm>

90



Stéganographie (exemple 3)

- Cacher un fichier text dans un autre
 - `echo how are you doing > file.txt`
 - `echo password > file.txt:hidden.txt`
 - `dir file.txt`
 - `notepad file.txt:hidden.txt`
- Cacher une image dans un fichier text
 - `type image.jpg>file.txt:image.jpg`
 - `Mspaint file.txt:image.jpg`

91



Fonction de hachage : intégrité

- Fonction mathématique qui, à un ensemble de nombres en entrée, fait correspondre un ensemble de nombres de cardinal plus petit en sortie ;
 - La modification d'un élément en entrée engendre une modification de sa fonction de hachage en sortie.

M	h(M)
remarquez la fin de cette ligne,	4b:2c:65:c0:e8:ee:95:5f:eb:05:9f:3c:6d:2f:2f:0f:9a:26:00:b7
remarquez la fin de cette ligne!	9e:e9:22:99:11:7f:41:23:7c:ce:38:3a:d8:05:18:0c:4a:fc:ab:4c
??	75:cc:4b:e0:a9:7c:76:34:78:58:bf:04:db:3b:90:2b:45:6a:2b:c0

- Propriétés
 - Deux messages différents ont deux empreintes différentes
 - Connaissant h(M), il est impossible de trouver M

92



Fonction de hachage

- Fonctions de hachage :
 - si $H(x)$ est une telle fonction, pour tout y donné, il doit être **quasi-impossible** de trouver un x tel que $H(x)=y$;
 - si $y=H(x)$, et $x' \approx x$ à un tout petit détail près (ex : changer 1 bit), on doit avoir $y'=H(x')$ très \neq de y
 - Collision : si $H(y)=H(x)$ sachant $x \neq y$
 - Problème: hachage doit avoir un petit nb de collisions
 - Ex de fonctions de hachage: MD5, SHA-1, MD4, RIPEMD-160

93



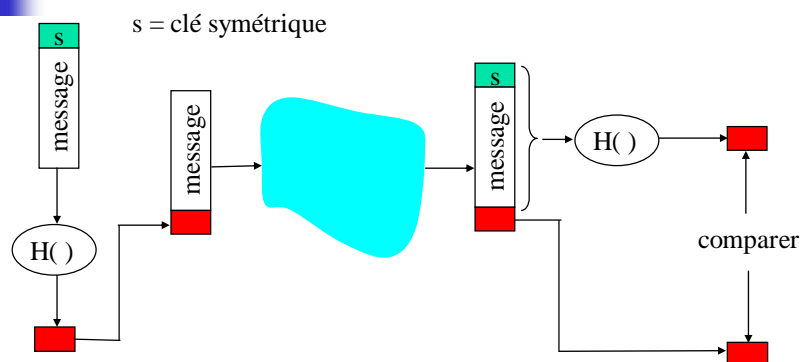
Hash Function Algorithms

- **MD5**
 - Digest sur 128-bit
- **SHA-1**
 - Digest sur 160-bit

94



MAC: Message Authentication Code



- Son rôle est d'assurer l'intégrité d'un message m
- $S = H(m, s)$, m est le message et s est la clé symétrique
- MAC (Message Authentication Code): ne fournit pas la propriété de non-répudiation

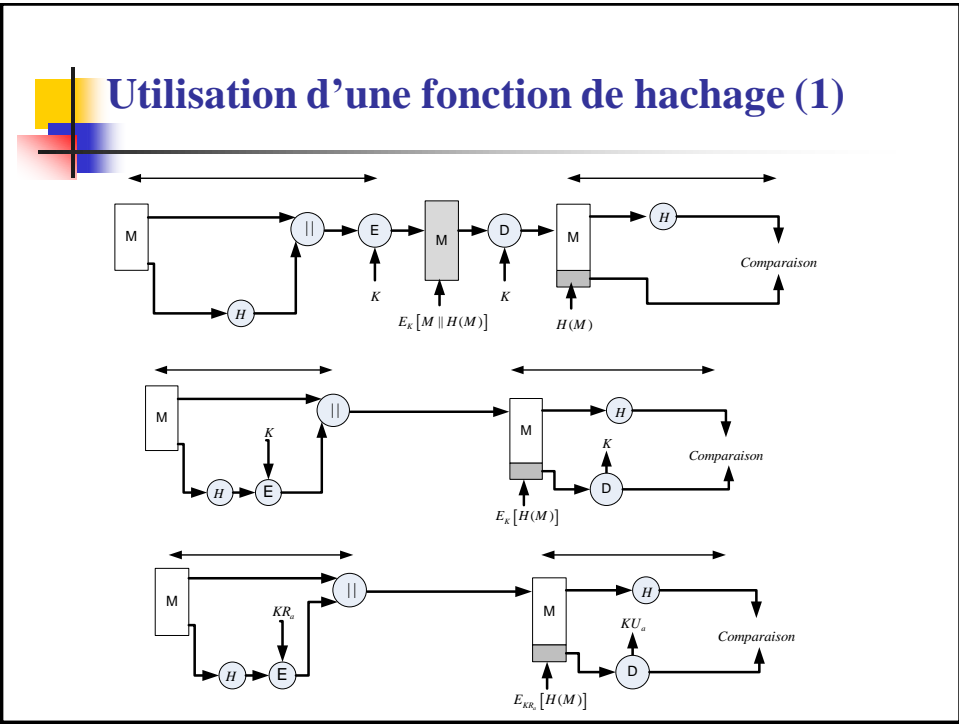
95



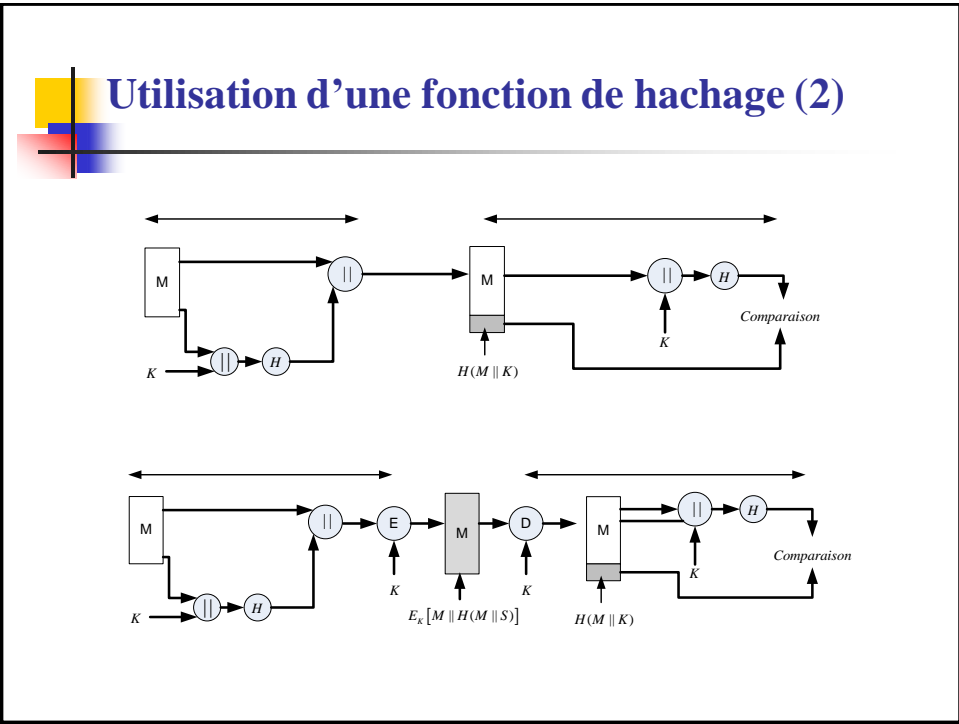
HMAC

- MAC standard
 - 1) Concaténation du secret avec le message
 - 2) Hachage de la concaténation
 - 3) Concaténation du secret avec le digest
 - 4) Hachage du résultat de la concaténation

96



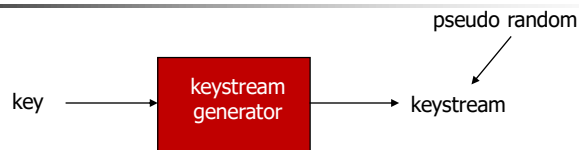
97



98



Chiffrement en continu



- Combinaison de bit de keystrem avec le bit du message en claire
- $m(i)$ = $i^{\text{ième}}$ bit du message
- $ks(i)$ = $i^{\text{ième}}$ bit de la clé
- $c(i)$ = $i^{\text{ième}}$ bit du message chiffré
- $c(i) = ks(i) \oplus m(i)$ (\oplus = ou exclusif)
- $m(i) = ks(i) \oplus c(i)$

99



Chiffrement par bloc

- Le message est divisé en bloc de k bits (64-bit par bloc).
- Chiffrement du k-bit du bloc en claire texte à k-bit bloc chiffré

Exemple avec k=3:

<u>input</u>	<u>output</u>	<u>input</u>	<u>output</u>
000	110	100	011
001	111	101	010
010	101	110	000
011	100	111	001

Quel est le message chiffré correspondant à 010110001111 ?

100

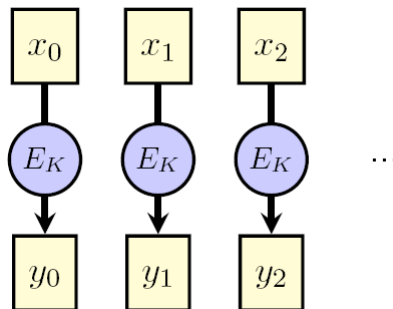
Chiffrement par bloc

- Les quatre principaux modes de chiffrement
 - ECB Electronic CodeBook
 - CBC Cipher Block Chaining
 - CFB Cipher FeedBack
 - OFB Output FeedBack

101

ECB : Electronic Code Book

- $C_i = E_k(M_i)$



- Le mode ECB n'assure aucune sécurité : ne pas l'utiliser.

102

Chiffrement par bloc (ECB)

Supposant le codage suivant:

input	output	input	output
A: 000	110	I: 100	011
K: 001	111	E: 101	010
N: 010	101	L: 110	000
O: 011	100	S: 111	001

Quel est le message chiffré correspondant à « le soleil »

L E S O L E I L
110 101 111 011 110 101 100 110

Texte chiffré:

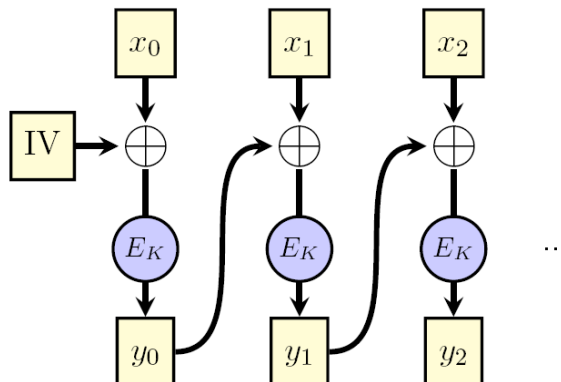
000 010 001 100 000 010 011 000
A N K I A N O A

Est-ce la fréquence de répétition des lettres est toujours la même avant et après le chiffrement ?

103

CBC : Cipher Block Chaining

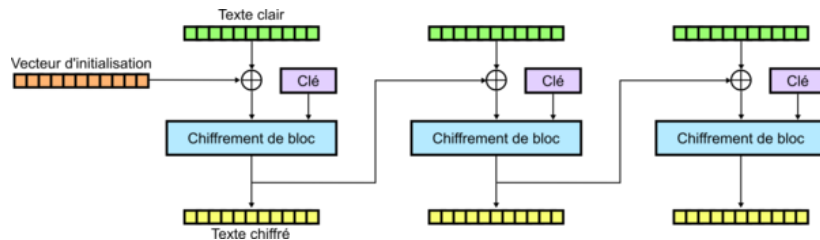
- $C_0 = IV$
 $C_i = E_k(M_i \oplus C_{i-1})$



104

Mode opératoire: Cipher Block Chaining

- Le message est découpé en blocs de taille fixe
- Chaque bloc est chiffré de manière corrélée avec le bloc précédent en utilisant l'opération **OU eXclusif** (XOR (\oplus)) entre le bloc de message i (M_i) et le résultat du chiffrement du bloc de Message M_{i-1}
 - à l'étape i ,
 - On calcule: $M_i \oplus C_{i-1}$
 - Puis on chiffre le résultat: $C_i = E(M_i \oplus C_{i-1})$
 - Et on transmet C_i
 - pour l'étape 1 :
 - On introduit une valeur d'initialisation (appelé seed ou initialisation Vector (IV)) pour effectuer le premier XOR.



105

Vecteur d'initialisation (IV)

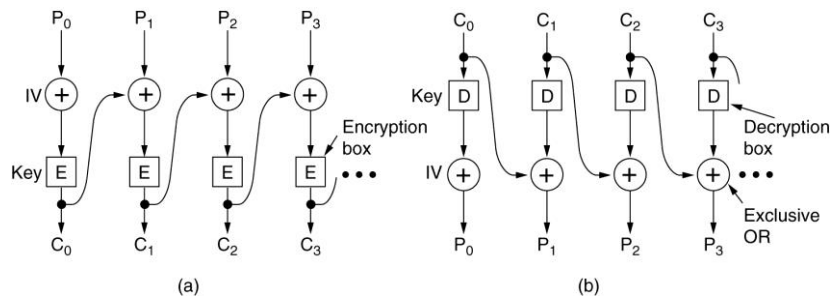
- Un vecteur d'initialisation (en anglais Initialization Vector ou IV) est un bloc de bits
 - Addition avec le premier bloc de données lors d'une opération de chiffrement
- Il est utilisé dans le cadre des modes d'opération d'un algorithme de chiffrement symétrique par blocs ou pour un chiffrement par flux comme RC4
- Dans certains cryptosystèmes, le vecteur est généré de manière **aléatoire** puis **transmis en clair** avec le reste du message

106



Cipher Block Chaining Mode

- Cipher block chaining (a) Encryption. (b) Decryption.



107



Chiffrement par bloc (CBC)

Supposant le codage suivant:

input	output	input	output
A: 000	110	I: 100	011
K: 001	111	E: 101	010
N: 010	101	L: 110	000
O: 011	100	S: 111	001

Par exemple:
IV: 000

Quel est le message chiffré correspondant à « le soleil »

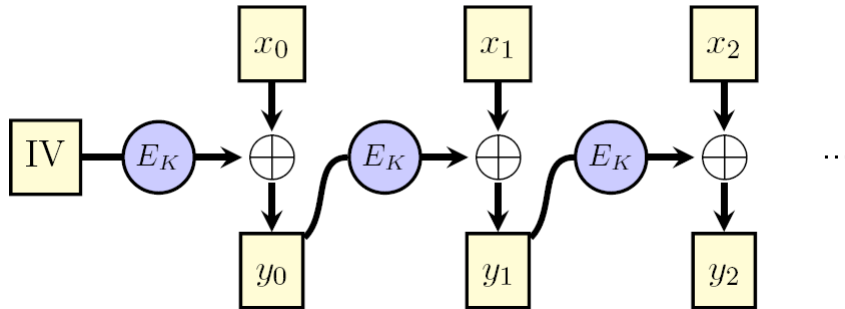
	L	E	S	O	L	E	I	L
IV:	110	101	111	011	110	101	100	110
Xor:	000	000	010	010	111	111	101	111
Texte chiffré	110	101	101	001	001	010	001	001

Est-ce la fréquence de répétition des lettres est toujours la même avant et après le chiffrement ?

108

CFB : Cipher FeedBack

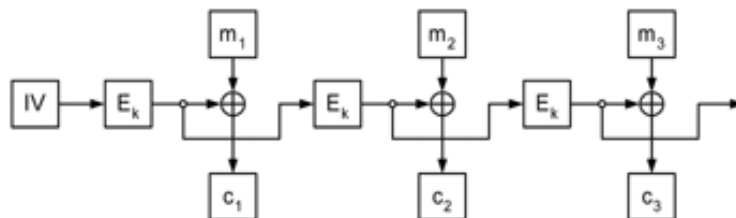
- $C_0 = IV$
 $C_i = M_i \oplus E_k(C_{i-1})$



109

OFB : Output FeedBack

- $Z_0 = IV$
 $Z_i = E_k(Z_{i-1})$
 $C_i = M_i \oplus Z_i$



110



Distribution des clés

- Les algorithmes de chiffrement symétriques nécessitent le partage d'une clé secrète
- Il faut donc assurer le transport sûr de cette clé
- Si la clé est compromise lors de la phase de distribution, toutes les communications le seront !

111



Distribution des clés

- Un utilisateur souhaitant communiquer avec plusieurs autres en assurant de niveaux de confidentialité distincts doit utiliser autant de clés qu'il a d'interlocuteurs
- Pour un groupe de N personnes utilisant un cryptosystème à clés secrètes, il est nécessaire de distribuer un nombre de clés égal à:

$$N * (N-1) / 2$$

112



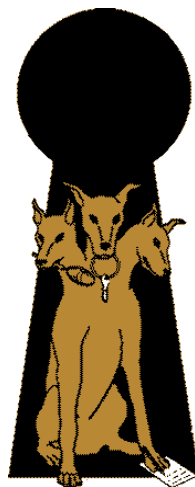
Schémas de distribution de clés

- Plusieurs variantes pour 2 partenaires
 - A choisit une clé et la transmet physiquement à B (valise diplomatique par exemple)
 - Une tierce partie (de confiance) C choisit un clé et assure la distribution à A et B
 - Si A et B ont déjà partagé une clé auparavant, ils peuvent utiliser l'ancienne clé pour chiffrer une nouvelle
 - Si A et B ont des communications sûres avec une tierce partie C, C peut relayer les clés entre A et B

113



Kerberos



114

Généralités

■ Principes

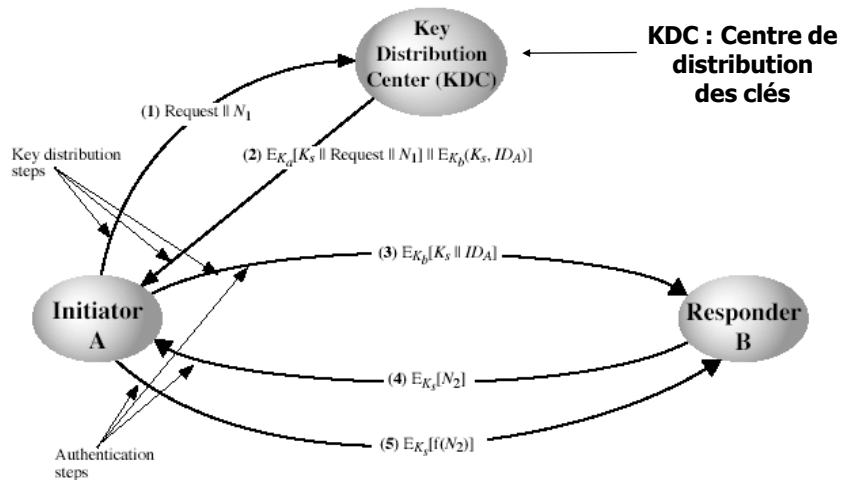
- Basé sur la notion de « Ticket »
- Cryptographie à clé secrète (symétrique)
- Authentification mutuelle
- Tickets limités dans le temps
- Mécanismes anti-rejeu (horodatage)
- Pas de transmission de mot de passe sur le réseau

■ Kerberos V5

- Standards IETF : RFCs 1510 et 1964

115

Scénario de distribution



116



Scénario de distribution

L'utilisateur A (resp. B) dispose d'une clé K_a (resp K_b) avec le KDC

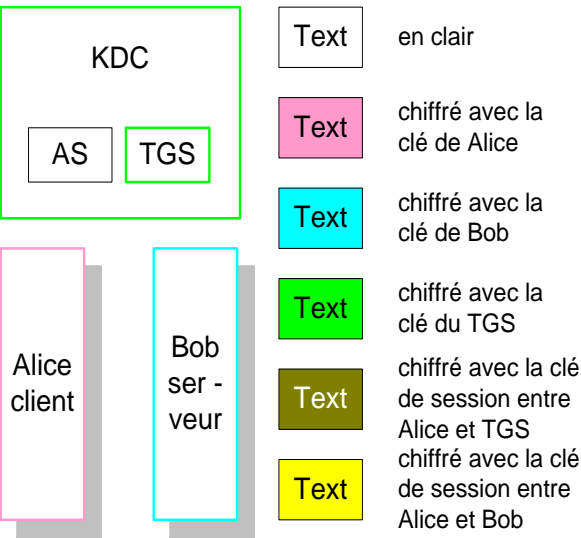
La requête envoyée par A au KDC contient les deux identités ID_a et ID_b

Le nombre aléatoire N_1 (resp. N_2) est destiné à la lutte anti rejeu

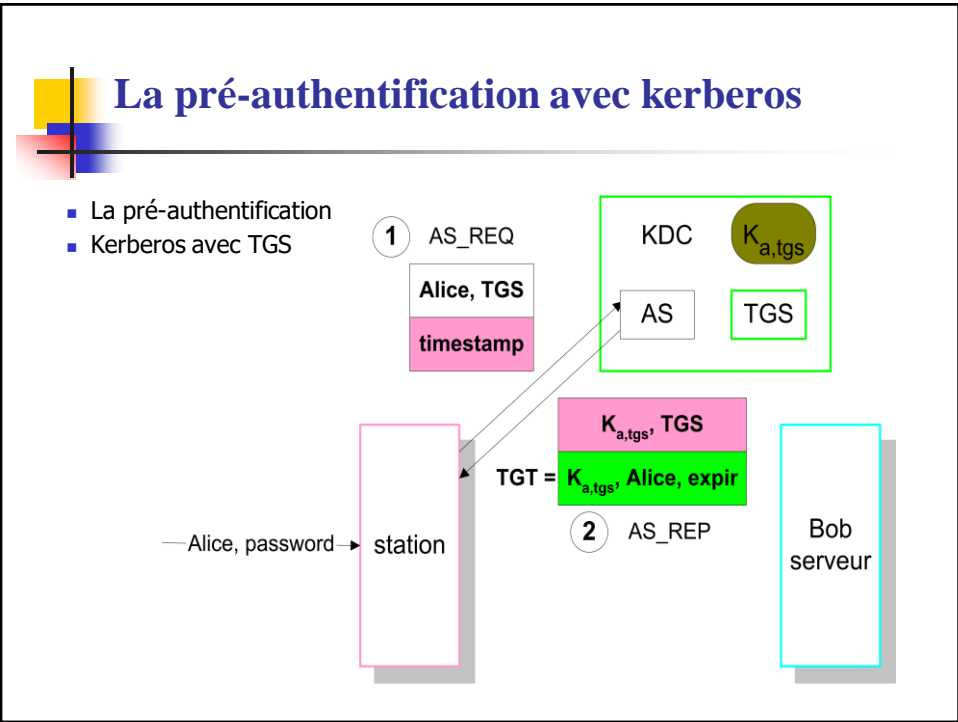
117



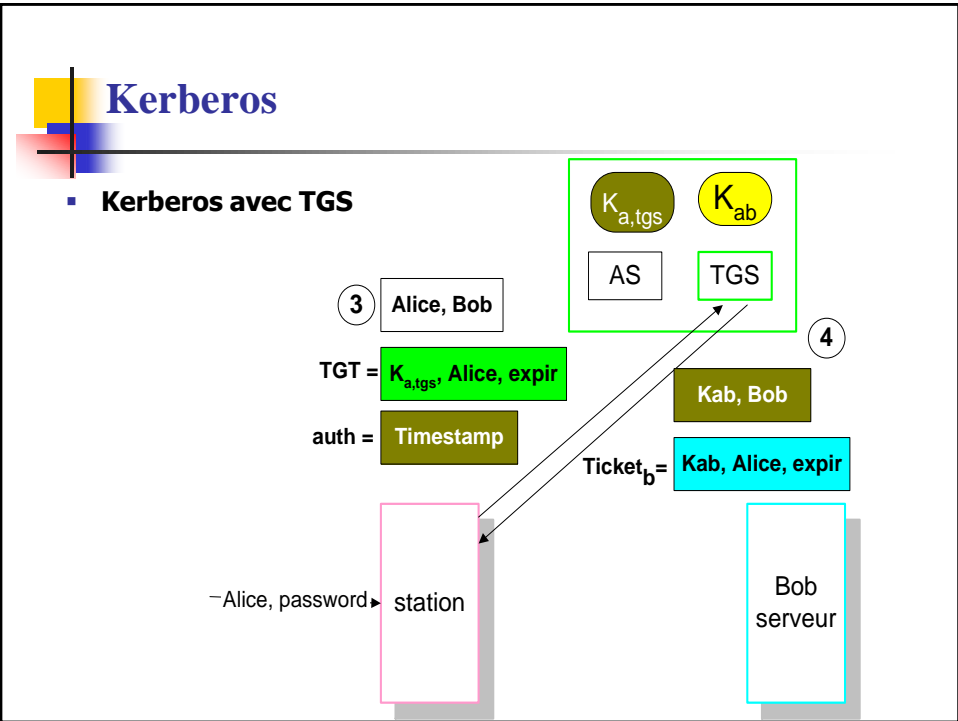
Kerberos



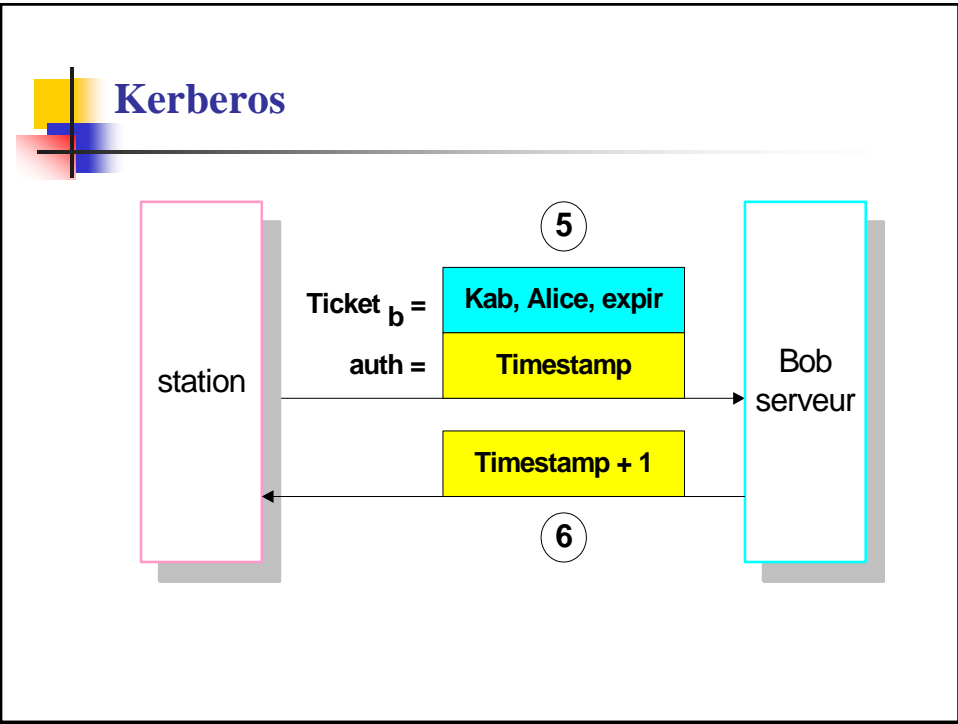
118



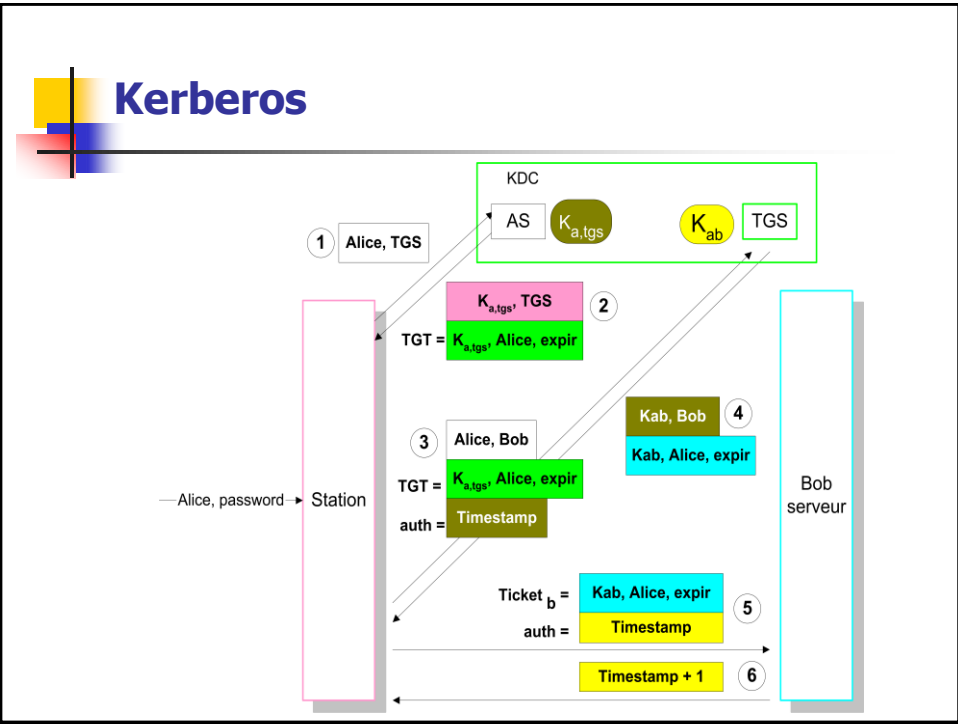
119



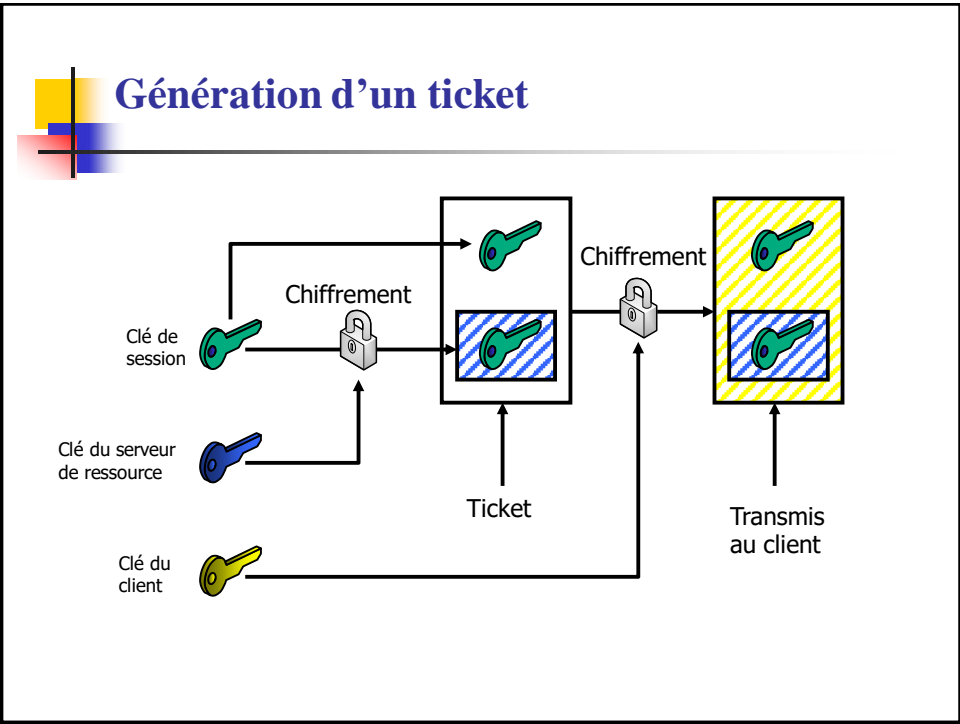
120



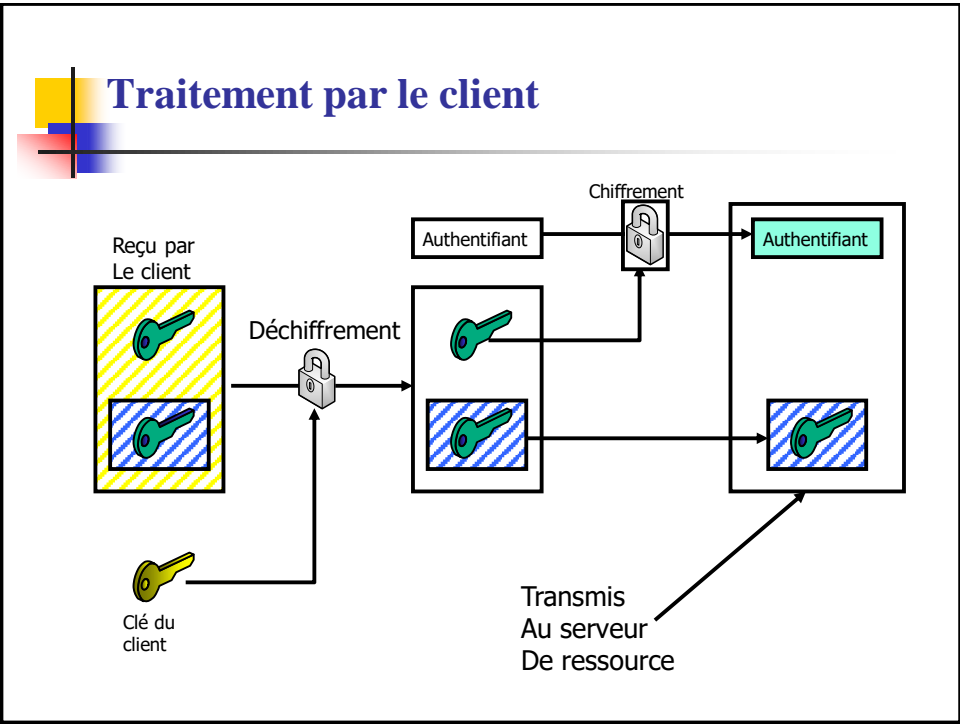
121



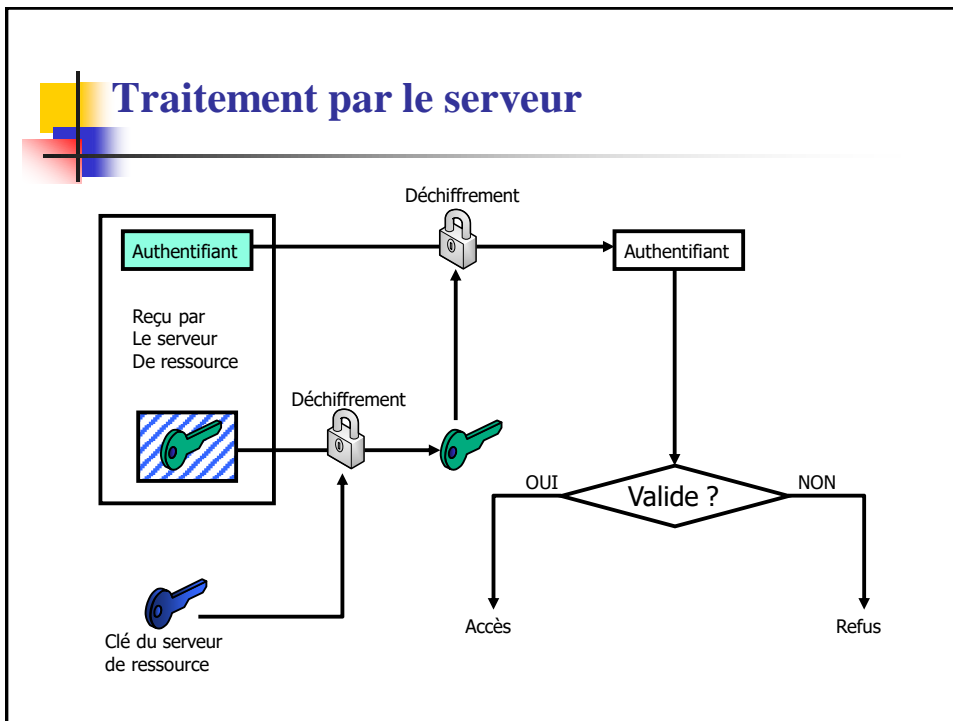
122



123



124



125

Accès à distance: FTP, telnet et SSH

- telnet (client et serveur)
 - yum install xinetd
 - yum install telnet-server telnet
 - nano /etc/xinetd.d/telnet
 - disable=no
 - /etc/init.d/xinetd restart
- ou
- service xinetd restart
- telnet 192.168.0.13
 - Login:
 - Password:
 - Escape character is '^'.

126



Accès à distance :FTP, telnet et SSH

- ftp (client et serveur)
 - Client en GUI: yum install gftp
 - Serveur: yum install vsftpd
 - Service vsftpd start
 - nano /etc/vsftpd/vsftpd.conf
 - anonymous_enable=YES => No (optionnal)
 - #local_enable=YES => uncomment this option
 - #write_enable=YES => uncomment this option
 - #anon_upload_enable=YES => uncomment this option (optional)

127



Accès à distance :FTP, telnet et SSH

SSH : Secure-Shell

- C'est un protocole sécurisée pour une connexion à distance
 - mot de passe n'est pas transmis en clair sur le réseau
 - session est chiffrée.
- SSH remplace *Telnet* et *FTP*
- Le protocole SSH est basé sur une architecture client/serveur
 - Un utilisateur qui veut se connecter exécute la commande «ssh» sur sa machine locale
 - Le client va se connecter à un **serveur** SSH sur une machine distante
 - Un serveur (sshd) est à l'écoute
 - port 22 et protocole TCP
 - La connexion est sécurisée, tout ce qui suit est chiffré

128



Accès à distance :FTP, telnet et SSH

- ssh
 - ssh *[user@]hostname*
[user@host]\$ ssh saphyr.ens.math-info.univ-paris5.fr
password: *****
[user@saphyr]\$ exit
logout
- ssh *[user@]hostname command*
- ssh *-l user hostname*
- ssh *-X user@hostB*

129



Les utilitaires SSH

- Transfert de fichiers
 - scp
 - Secure COPY
 - L'authentification est identique à celle de la commande ssh
 - Les deux processus communiquent par la connexion sécurisée
 - Sur la ligne de commande, des fichiers sont échangés
 - Syntaxe: *scp source destination*
 - sftp
 - L'authentification est identique à celle de la commande ssh
 - Les deux processus communiquent par la connexion sécurisée
 - Selon les commandes interactives saisies, des fichiers sont échangés
 - nb : semblable à ftp (mais celui-ci fait tout en clair !)
(de plus sftp utilise une seule connexion, le filtrage est facilité)
 - Syntaxe: *sftp source destination*

130

Transfert des fichiers

■ Secure copy

```
[user@host~]$ scp mylocalfile user@server:remotefile  
[user@host~]$ scp user@server:remotefile mylocalfile
```

■ Secure FTP

```
[user@host~]$ sftp user@server  
Sftp> dir  
File1 file2
```

sftp user@host

<i>sftp> lcd /tmp</i>	<i>[change local directory to /tmp]</i>
<i>sftp> cd /etc</i>	<i>[change remote directory to /etc]</i>
<i>sftp> get motd</i>	<i>[download /etc/motd to /tmp/motd]</i>
<i>sftp> ?</i>	<i>[view summary help]</i>
<i>sftp> bye</i>	<i>[terminate connection]</i>
<i>ls /tmp/motd</i>	<i>[prove you got the file]</i>

131

Accès à distance :FTP, telnet et SSH

■ ssh, scp sftp

- `scp [local path] [username]@[hostname]:[remote file path]`
- `scp hello.txt yourusername@localhost:scp-test.txt`
- `scp user@hostname:path filename`

■ Exemple : transfert de fichiers et de répertoires avec scp

```
{user$host}$ scp -r SubDir there.veryfar.net:Project  
{user$host}$ scp there.veryfar.net:Project/SubDir/photo.jpg .  
{user$host}$ scp ~/example.file user1@10.10.0.117:~/done/example.file.moved  
{user$host}$ scp data.tgz root@there.veryfar.net:
```

132



Les utilitaires SSH

- Exemple : transfert de fichiers et de répertoires avec sftp

```
{user$host}$ sftp root@there.veryfar.net
sftp> put data.tgz
Uploading data.tgz to /root/data.tgz
data.tgz          100%    18MB    17.7MB/s      00:01
sftp> get archive.tgz
Fetching /root/archive.tgz to archive.tgz
archive.tgz       100%    18MB     8.8MB/s      00:02
sftp> quit
{user$host}$
```