Sécurité et Réseaux
Licence 3 Informatique

Cours 1 et 2: 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 (Mercredi de 09h15-10h45)
  - 3h de TD/TP
    - 3 groupes
      - 2 groupes le Mercredi (13h15 et 16h30) et 1 groupe le Jeudi à 10h
- 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 2022

Semaine	Semaine	Cours	TD	commentaires
S1	17/01	1	1 (TD3)	
S2	24/01	2	2	
S3	31/01	3	3	
S4	14/02	4	4	
S5	21/02	5	5	
S6	28/02	6	6	
S7	14/03	7	7	
S8	21/03	8	8	
S9	28/03	9	9	
S10	04/04	10	10	
S11	11/04	11	11	
S12	18/04	12	12	

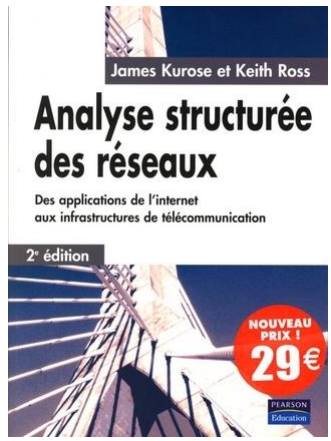
4

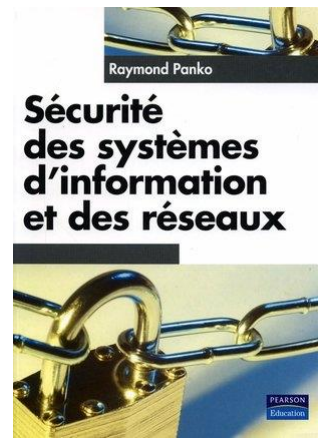
Evaluation

- Modalité de calcul de la note finale de l'U.E.
  - Il faudra au moins 3 notes
    - Examen final (si pas de confinement)
    - TPs à rendre
    - Participation

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, EIGRP, OSPF

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 claire avec Telnet et FTP
  - Steghide, nmap, dirb, nikto,wp scan, etc.
  - Wireshark
  - Secure Shell: SSH, SCP et SFTP
  - CISCO Packettracer
  - DHCP et DNS

9

Partie I: la sécurité des réseaux

Introduction

10

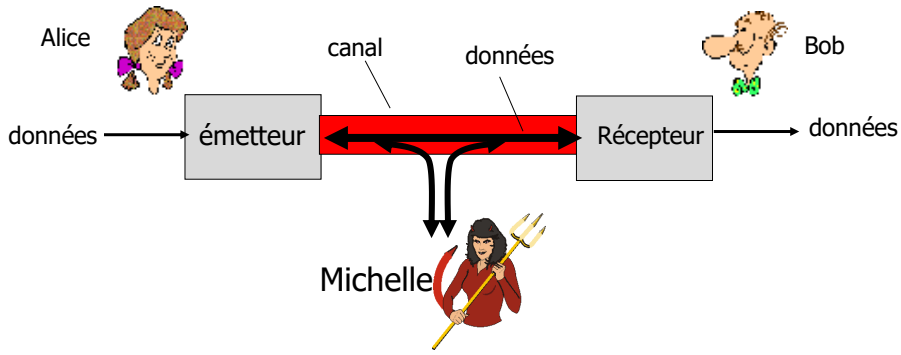
Les services de sécurité

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

11

Confidentialité

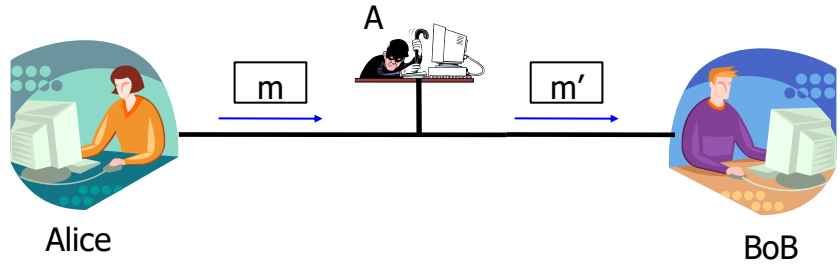
- Seul le récepteur patenté du message peut lire le message, celui-ci reste secret (ou inexploitable) pour tous les autres utilisateurs
  - **Empêcher les utilisateurs malicieux de lire une information confidentielle**



12

Intégrité

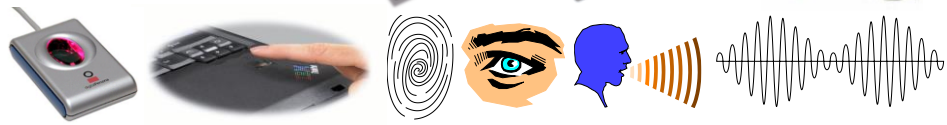
- Quand le récepteur reçoit le message ***m***, il peut vérifier que celui-ci est intact, c'est-à-dire égal au message que l'émetteur a envoyé
  - **L'information n'est pas été altérée durant son transfert**
  - Objective: empêcher un modification par des utilisateurs malicieux



13

Authentification

- 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



14

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

15

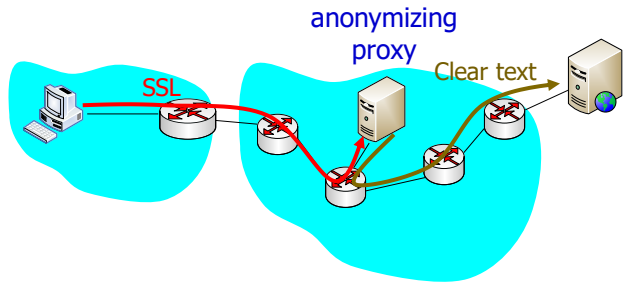
Non-répudiation

- 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

16

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



17

2. Cryptographie

Introduction

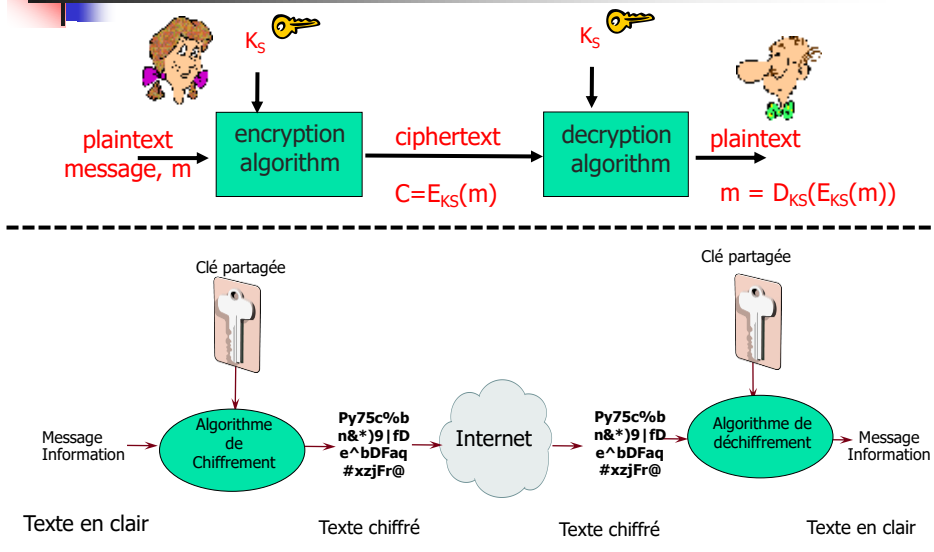
18

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

19

Chiffrement symétrique



20

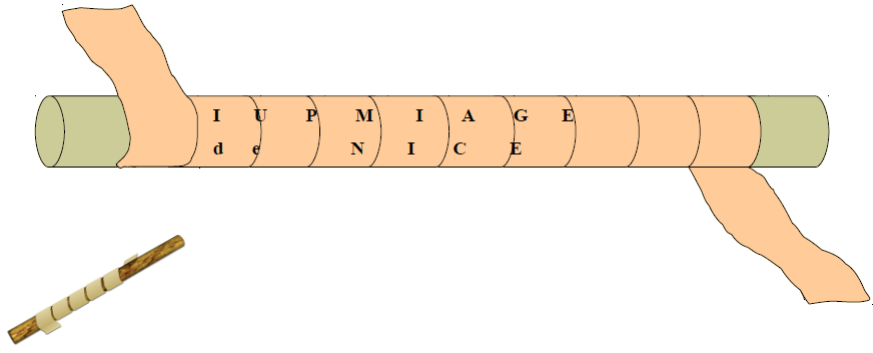
Cryptanalyse

- 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

21

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



22

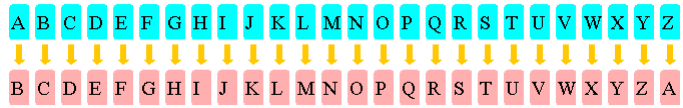
Chiffrement symétrique

- 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

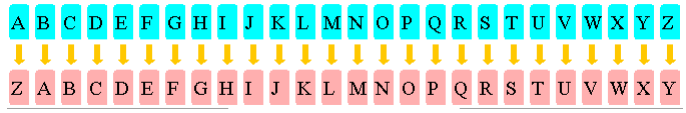
23

Substitution

- Substitution: Ex1: chiffrement par décalage



- Substitution alphabétique inversée

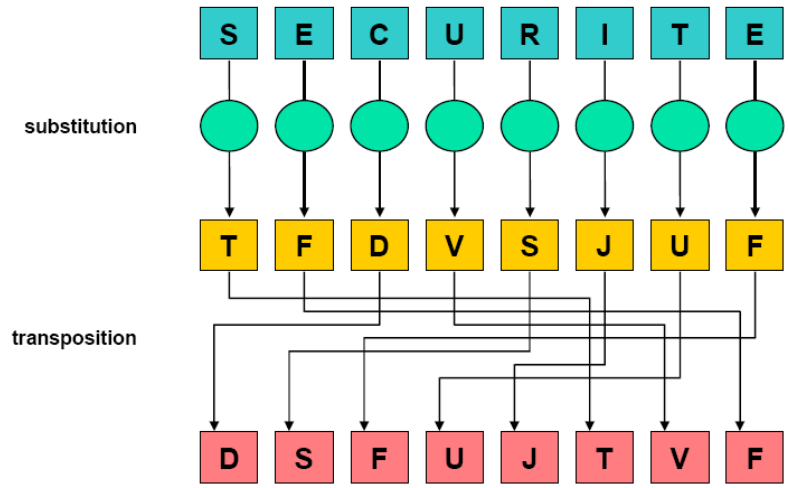


- Substitution, Ex3: utilisation de tables d'association

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

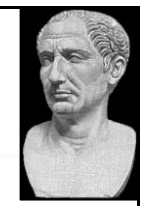
24

Substitution et transposition



25

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

  UHQGHCYRXVDSUHVOHFRXV

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

26

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
```

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

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

27

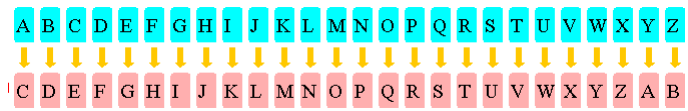
Cryptanalyse du code de César

- 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 FGEJKHHTGT"

28

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 FGEJKHHTGT"
  - A ➔ C
  - FACILE DE DECHIFFRER



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

29

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
```

30

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.

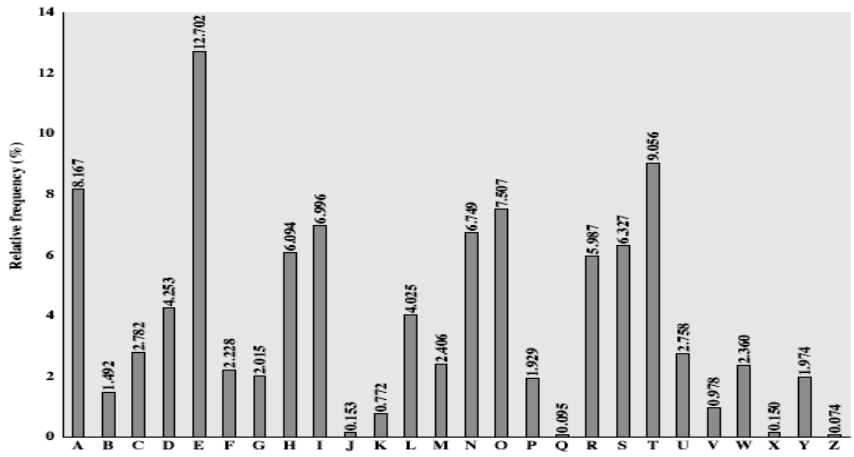
31

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),…

32

Fréquence des lettres en anglais



Code de vigenère

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

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: ausecoursnoussommesdecouverts

  key: monarchieausecoursnoussommesd

  ciphertext: ...

36

Chiffrement "playfair"

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

37

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**	**WX**	**Y**	**Z**

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

38

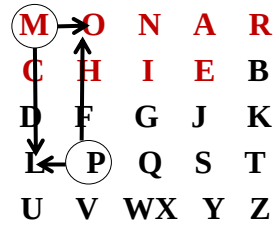
Chiffrement

- 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

39

Déchiffrement

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

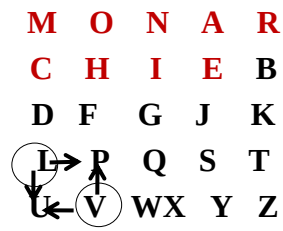


- PM➔ ligne de P et colonne de M : intersection = L ; colonne de P et ligne de M : intersection = 0

40

Déchiffrement

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

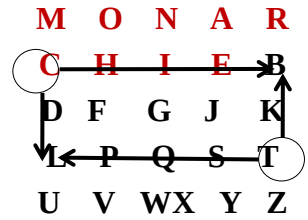


- PM➔ ligne de P et colonne de M : intersection = L ; colonne de P et ligne de M : intersection = O
- VL ➔ ligne de V et colonne de L : intersection = U; colonne de V et ligne de L : intersection = P

41

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

42

Déchiffrement

- 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	WX	Y	Z

- 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)

43

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…

44

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

45

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 : **DACNSEROSSEULEPOZRUVER**

46