Introduction à la Cryptographie

Master TNSI (S8 FI & S10 FA)
2016 - 2017

Christophe Wilbaut

ISTV - LAMIH

christophe.wilbaut@univ-valenciennes.fr

Introduction

- **Volume horaire**

COURS	=>	12h
TD (**FA**)	=>	6h
TP	=>	6h

- Ce cours …
  - Est une **introduction** à la cryptographie
  - Vise à apporter les éléments de base (vocabulaire, protocoles existants) sur le **transfert de données sécurisé**
- Ce cours **n'est pas** …
  - Un **module avancé** sur les techniques de cryptographie (domaine scientifique)

Plan du Cours

- **Introduction Générale à la Cryptographie**
  - Objectifs / Applications
  - Vocabulaire
  - Exemples Historiques
  - Protocoles de Confidentialité
  - Techniques de contournement ?

Plan du Cours

- Introduction Générale à la Cryptographie
- **Protocoles à Clé Publique**
  - Quelques éléments mathématiques
  - Protocole RSA
  - Crypto système de El Gamal
  - Protocole de Merkle - Hellman

Plan du Cours

- Introduction Générale à la Cryptographie
- Protocoles à Clé Publique
- **Protocoles à Clé Secrète**
  - Quelques éléments mathématiques
  - Techniques de codage par blocs
  - Protocole DES
  - Protocole IDEA
  - Protocole AES

Chapitre 1 :
Introduction Générale à la Cryptographie

Introduction Générale à la Cryptographie

- **Exemples Historiques**
  - **La scytale spartiate**

KTMIOILMDLONKRIIRGNOHGWT

Introduction Générale à la Cryptographie

- **Exemples Historiques**
  - Le cryptogramme de César
    - Décalage des lettres de l'alphabet vers la droite ou la gauche
    - La **clé** = le décalage (entier entre 0 et 25)
    - Exemple :

clair	A	B	C	D	E	F	G	H	I	J	K	L	M
chiffré	C	D	E	F	G	H	I	J	K	L	M	N	O

clair	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
chiffré	P	Q	R	S	T	U	V	W	X	Y	Z	A	B

Clair : Veni, Vidi, Vici => **Clé C** => **Chiffré :** XGPK XKFK XKEK

Introduction Générale à la Cryptographie

- **Exercice** (Cryptogramme de César)
  1. Chiffrer CHIFFREZ MOI avec la clé G
  2. Déchiffrer NCJA EZTD PLDJ avec la clé L
  3. Déchiffrer MH SHQVH TXH FHVW DFTXLV (clé ?)

  1. INOLL XKFSU O
  2. Crypto is easy
  3. JE PENSE QUE CEST ACQUIS => CLE D (3)

Introduction Générale à la Cryptographie

- **La Permutation de Lettres**
  - Généralisation du cryptogramme de César
  - **Clé** = permutation sur 26 lettres (26 ! clés)
  - Exemple :

clair	A	B	C	D	E	F	G	H	I	J	K	L	M
chiffré	R	G	E	C	V	J	U	A	S	P	O	I	M

clair	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
chiffré	B	W	D	T	Z	X	F	H	Y	K	L	N	Q

Clair : Veni, Vidi, Vici => **Chiffré :** YVBS YSCS YSES

Introduction Générale à la Cryptographie

- **La Permutation de Lettres**
  - Améliore le cryptogramme de César
  - Point faible : une lettre toujours chiffrée de la même manière
  - **Cryptanalyse :** fréquence d'apparition des lettres

Exemple, en Français

E	A	S	I	N	T	R	L
17,3%	8,4%	8,1%	7,4%	7,1%	7,0%	6,6%	6,0%

Introduction Générale à la Cryptographie

- **La Permutation de Lettres** (Cryptanalyse)

E	A	S	I	N	T	R	L
17,3%	8,4%	8,1%	7,4%	7,1%	7,0%	6,6%	6,0%

– Message à déchiffrer

TD VYEVTF OSU EMETYV R PU MTV KMPOOMRY YF TD YFMTF MP KSKYUF RY DY AVSTOOYV OMUO RSPFY ESPV DY ZYFYV RMUO DY AYP LPMUR OSU VYCMVR YFMUF FSKBY EMV JMOMVR OPV DY RYOOTU FSPFY OSU MFFYUFTSU Q EMVPF YUHJMTUYY YU PU TUOFMUF OSU WTOMCY RYWTUF R PU VSPCY TUFYUOY EPTO YGHYOOTWYKYUF EMDY EYURMUF LPYDLPYO KTUPFYO OMUO …

Introduction Générale à la Cryptographie

- **La Permutation de Lettres** (Cryptanalyse)

E	A	S	I	N	T	R	L
17,3%	8,4%	8,1%	7,4%	7,1%	7,0%	6,6%	6,0%

Y	M	U	O	F	P	T	V
16,56	9,98	9,55	8,70	7,64	6,58	6,58	6,37

TD VYEVTF OSU EMETYV R PU MTV KMPOOMRY YF TD YFMTF MP KSKYUF RY DY AVSTOOYV OMUO RSPFY ESPV DY ZYFYV RMUO DY AYP LPMUR OSU VYCMVR YFMUF FSKBY EMV JMOMVR OPV DY RYOOTU FSPFY OSU MFFYUFTSU Q EMVPF YUHJMTUYY YU PU TUOFMUF OSU WTOMCY RYWTUF R PU VSPCY TUFYUOY EPTO YGHYOOTWYKYUF EMDY EYURMUF LPYDLPYO KTUPFYO OMUO …

Introduction Générale à la Cryptographie

- **La Permutation de Lettres** (Cryptanalyse)
  - Essai : (Y, M) $\rightarrow$ (E, A)

TD VEEVTF OSU EAETEV R PU ATV KAPOOARE EF TD EFATF AP

KSKEUF RE DE AVSTOOEV OAUO RSPFE ESPV DE ZEFEV RAUO DE

AEP LPAUR OSU VECAVR EFAUF FSKBE EAV JAOAVR OPV DE

REOOTU FSPFE OSU AFFEUFTSU Q EAVPF EUHJATUEE EU PU

TUOFAUF OSU WTOACE REWTUF R PU VSPCE TUFEUOE EPTO

EGHEOOTWEKEUF EADE EEURAUF LPEDLPEO KTUPFEO OAUO …

Introduction Générale à la Cryptographie

- **La Permutation de Lettres** (Cryptanalyse)

TD VEEVTF OSU EAETEV R PU ATV KAPOOARE EF TD EFATF AP

KSKEUF RE DE AVSTOOEV OAUO RSPFE ESPV DE ZEFEV RAUO DE

AEP LPAUR OSU VECAVR EFAUF FSKBE EAV JAOAVR OPV DE

REOOTU FSPFE OSU AFFEUFTSU Q EAVPF EUHJATUEE EU PU

TUOFAUF OSU WTOACE REWTUF R PU VSPCE TUFEUOE EPTO

EGHEOOTWEKEUF EADE EEURAUF LPEDLPEO KTUPFEO OAUO …

Introduction Générale à la Cryptographie

- **La Permutation de Lettres** (Cryptanalyse)
  - Essai : (Y, M, D) → (E, A, L)

TL VEEVTF OSU EAETEV R PU ATV KAPOOARE EF TL EFATF AP

KSKEUF RE LE AVSTOOEV OAUO RSPFE ESPV LE ZEFEV RAUO LE

AEP LPAUR OSU VECAVR EFAUF FSKBE EAV JAOAVR OPV LE

REOOTU FSPFE OSU AFFEUFTSU Q EAVPF EUHJATUEE EU PU

TUOFAUF OSU WTOACE REWTUF R PU VSPCE TUFEUOE EPTO

EGHEOOTWEKEUF EALE EEURAUF LPELLPEO KTUPFEO OAUO …

Introduction Générale à la Cryptographie

- **La Permutation de Lettres** (Cryptanalyse)

TL VEEVTF OSU EAETEV R PU ATV KAPOOARE EF TL EFATF AP

KSKEUF RE LE AVSTOOEV OAUO RSPFE ESPV LE ZEFEV RAUO LE

AEP LPAUR OSU VECAVR EFAUF FSKBE EAV JAOAVR OPV LE

REOOTU FSPFE OSU AFFEUFTSU Q EAVPF EUHJATUEE EU PU

TUOFAUF OSU WTOACE REWTUF R PU VSPCE TUFEUOE EPTO

EGHEOOTWEKEUF EALE EEURAUF LPELLPEO KTUPFEO OAUO …

Introduction Générale à la Cryptographie

- **La Permutation de Lettres** (Cryptanalyse)
  - Essai : (Y, M, D, T) → (E, A, L, I)

IL VEEVIF OSU EAEIEV R PU AIV KAPOOARE EF IL EFAIF AP

KSKEUF RE LE AVSIOOEV OAUO RSPFE ESPV LE ZEFEV RAUO LE

AEP LPAUR OSU VECAVR EFAUF FSKBE EAV JAOAVR OPV LE

REOOIU FSPFE OSU AFFEUFISU Q EAVPF EUHJAIUEE EU PU

IUOFAUF OSU WIOACE REWIUF R PU VSPCE IUFEUOE EPIO

EGHEOOIWEKEUF EALE EEURAUF LPELLPEO KIUPFEO OAUO …

Introduction Générale à la Cryptographie

- **La Permutation de Lettres** (Cryptanalyse)

IL VEEVIF OSU EAEIEV R PU AIV KAPOOARE EF IL EFAIF AP

KSKEUF RE LE AVSIOOEV OAUO RSPFE ESPV LE ZEFEV RAUO LE

AEP LPAUR OSU VECAVR EFAUF FSKBE EAV JAOAVR OPV LE

REOOIU FSPFE OSU AFFEUFISU Q EAVPF EUHJAIUEE EU PU

IUOFAUF OSU WIOACE REWIUF R PU VSPCE IUFEUOE EPIO

EGHEOOIWEKEUF EALE EEURAUF LPELLPEO KIUPFEO OAUO …

Introduction Générale à la Cryptographie

- **La Permutation de Lettres** (Cryptanalyse)
  - Essai : (Y, M, D, T, F) → (E, A, L, I, T)

IL VEEVIT OSU EAEIEV R PU AIV KAPOOARE ET IL ETAIT AP

KSKEUT RE LE AVSIOOEV OAUO RSPTE ESPV LE ZETEV RAUO LE

AEP LPAUR OSU VECAVR ETAUT TSKBE EAV JAOAVR OPV LE

REOOIU TSPTE OSU ATTEUTISU Q EAVPT EUHJAIUEE EU PU

IUOTAUT OSU WIOACE REWIUT R PU VSPCE IUTEUOE EPIO

EGHEOOIWEKEUT EALE EEURAUT LPELLPEO KIUPTEO OAUO …

Introduction Générale à la Cryptographie

- **La Permutation de Lettres** (Cryptanalyse)

IL VEEVIT OSU EAEIEV R PU AIV KAPOOARE ET IL ETAIT AP

KSKEUT RE LE AVSIOOEV OAUO RSPTE ESPV LE ZETEV RAUO LE

AEP LPAUR OSU VECAVR ETAUT TSKBE EAV JAOAVR OPV LE

REOOIU TSPTE OSU ATTEUTISU Q EAVPT EUHJAIUEE EU PU

IUOTAUT OSU WIOACE REWIUT R PU VSPCE IUTEUOE EPIO

EGHEOOIWEKEUT EALE EEURAUT LPELLPEO KIUPTEO OAUO …

……

Introduction Générale à la Cryptographie

- **Le chiffrement de Vigenère**
  - Exemple :

    CHIFFREDEVIGENERE avec la clé CRYPTOGRAPHIE

clair	C	H	I	F	F	R	E	D
clé	C	R	Y	P	T	O	G	R
décalage	2	17	24	15	19	14	6	17
chiffré	E	Y	G	U	Y	F	K	U

clair	E	V	I	G	E	N	E	R	E
clé	A	P	H	I	E	C	R	Y	P
décalage	0	15	7	8	4	2	17	24	15
chiffré	E	K	P	O	I	P	V	P	T

Introduction Générale à la Cryptographie

- **Le chiffrement de Vigenère** (Cryptanalyse)
  - Exemple :

KIIFSIRV A E NEEF HJYKR SPFCVI GI KRVMMSYI XSLC HZ ZVAX YI EBVY IJG
UPM JRHZGYNMIE RH QDPZRY YI C RUPMEBBZ HV PIOXV NRIIV RX
KIEQEIX CRUPIC YI WEIBQZXIR XJQSN E NIGG GZRK QMS
QZYPDQVGVZW TR JPX LA SPVRTEI WRAW DRKRVHMKGIIGV DYD HLEE
YY UVB CYZG EP ZZAKO GZAU HEIF PZW INZVKVF UP MC CVJHLVWDX
WHVZRK VQHIEFIN IENQZVZDYZ IE RYMSGR II EJVI NYI HRZ DFAI GEITI
YI UVB CYZG GZRKF QDPCRW LYZ FIYIJFMIEZG SWPZDYZQVAX V P
VDYVXVHV YIGHMN PV GVZRKR GDRHHMZQV CEMECYIGI EBVY
NLFUPEL DYVVRAXDIDR TVVRYPZPV FYY

Introduction Générale à la Cryptographie

- **Le chiffrement de Vigenère** (Cryptanalyse)
  - Exemple :
    - On considère le cas d'une clé de longueur 1

KIIFSIRV A E NEEF HJYKR SPFCVI GI KRVMMSYI … ***Ic* = 0.052**

    - Puis le cas d'une clé de longueur 2

KISRANEHYRPCI .. IFIVEEFJKSFV ... ***Ic* = 0.051**

    - Puis une clé de longueur 3

KFREEJRFI ... ISVNFYSCG ... IIAEHKPVI ... ***Ic* = 0.052**

    - Puis une clé de longueur 4

KSAEYPI ... IIEFKFG ... IRNHRCI ... FVEJSVK ... ***Ic* = 0.050**

Introduction Générale à la Cryptographie

- **Le chiffrement de Vigenère** (Cryptanalyse)
  - Exemple :
    - On considère le cas d'une clé de longueur 5

KINJ... IREY... IVEK... FAFR... SEHS... ***Ic* = 0.079**

=> On en déduit que la clé est (probablement) de longueur 5 $C_1C_2C_3C_4C_5$

- Reste à trouver les 5 lettres… on considère **chacun des 5 extraits**, et on compte le nombre d'occurrences des lettres (**fréquence d'apparition**)

Introduction Générale à la Cryptographie

- **Le chiffrement de Vigenère** (Cryptanalyse)
  - Exemple :
    - Reste à trouver les 5 lettres… on considère **chacun des 5 extraits**, et on compte le nombre d'occurrences des lettres (**fréquence d'apparition**)

1er extrait

KINJPGMXZYYPZIDYPZOIKIPWZJNZSDZPP … 16 **Z** (19.3%)

=> C1 = 'Z' – 'E' = **'V'**

2ème extrait

IREYFIMSZIIMGEPIMHXIIXIEXQIRQQWXV … 17 **I** (20.7%)

=> C2 = 'I' – 'E' = **'E'** **…**

Introduction Générale à la Cryptographie

- **Exercice**

Décoder le message suivant (dont la mise en forme a été supprimée) encodé par le protocole de Vigenère avec une clé de longueur 2. On détaillera les différentes étapes de la méthode utilisée.

QODBS WWOFO LOFMW MSZFK HSEES FWCSK JOFST SSBEE SVSCP KGOGC CXHKQ AISGO G

Exercices

- **Chiffrement de César**
  - Chiffrer PREMIER EXEMPLE avec la clé Y
  - Déchiffrer MZMV CV DFULCV UV TIPGKF avec la clé R
  - Décrypter KNS IZ UWJRNJW JCT
- **Chiffrement de Vigenère**
  - Chiffrer CAMARCHE avec la clé ROI
  - Déchiffrer le message suivant, avec la clé MASTER

XATBG YQBJT QVMUU EEZDD WEYEQ ELIPV GRWTW VROFW VVXEK RILJS

GGTVF ILYEF ZDWEM TUEMQ EUUSH TVLPA FLPRZ UAMFI GNW

Exercices

- **Cryptanalyse du chiffrement de Vigenère**

  Le cryptogramme suivant a été obtenu par le chiffrement de Vigenère (sur un alphabet de 26 lettres). Retrouvez la longueur de la clé.

  IRTGQ TFTEF KENVR TOVLI GETDN VCITR BXGLV HGKYX VTFPT XCSGC YBKJC TPKPP KEGAC CJPKK TTPRG IFVQR GEBPK KPTOF LICZR QTLGH URGIG KGCEV JPKK