UNIVERSITÉ DE STRASBOURG S5b

Cryptographie : Algorithmes et protocoles

- Cryptologie
- Historique
- Algorithmes de chiffrement
- Standards de cryptographie
- L'aspect juridique

UNIVERSITÉ DE STRASBOURG S5b

Cryptologie

Combinaison de 2 techniques

- **Cryptographie**

  Art de générer des messages secrets

- **Cryptanalyse**

  Art de révéler des messages secrets

Chiffrement par substitution

- **Code de César : la clé est un entier n, et on réalise un décalage modulo 26 de n caractères du texte**

B O N J O U R

H U T P U A X

→*Clé = 6*

Et **Y L K P L F O** *?*

B O N S O I R

Code de Vigenère

- **Substitution à base d'une clé secrète (ex : 2 4 5 7 1)**

B O N J O U R

D S S Q P W V

C Q Q W T J T → ?

Chiffrement par transposition

- **Principe de la transposition matricielle**

Voici un message chiffré :

IAETLSSLCPEEDSEIERTU
ASLRLTNGTEMERMEFDUSEE

Voici un message clair :

ILESTFACILEDEPERMUTER
LESLETTRESDUNMESSAGE

I	L	E	S	T	F
A	C	I	L	E	D
E	P	E	R	M	U
T	E	R	L	E	S
L	E	T	T	R	E
S	D	U	N	M	E
S	S	A	G	E	

Chiffrement par double transposition

Voici un message clair :

ILESTFACILEDEPERMUTER

LESLETTRESDUNMESSAGE

Voici un message doublement transposé :

ISDTLMDALSUTEUECEAN

RSTPISGMELEELTEESERREF

Voici le message transposé :

IAETLSSLCPEEDSEIERTU

ASLRLTNGTEMERMEFDUSEE

I	A	E	T	L	S	
S	L	C	P	E	E	
D	S	E	I	E	R	
T	U	A	S	L	R	
L	T	N	G	T	E	
M	E	R	M	E	F	
D	U	S	E	E		

Chiffrement par transposition (niveau 2:)

Voici un message clair :

ILESTFACILEDEPERMUTER
LESLETTRESDUNMESSAGE

Voici un message transposé :

ILAECESIPTLEFERDMUTEL
RESLTDETUSRNEMESSAGE

Voici un autre message transposé :

ILAECESIPTTLEELFERRES
DMLTDSUETUSSRNAEMGEE

Comment ?

UNIVERSITÉ DE STRASBOURG S5b

Chiffrement par transposition et substitution

- La combinaison des deux techniques prévient l'attaque par mot connu

Voici un message clair :

ILESTFACILEDEPERMUTER

LESLETTRESDUNMESSAGE

Voici un message transposé et substitué :

LDHWOVVOFSHHGV……

Voici le message transposé :

IAETLSSLCPEEDSEIERTU

ASLRLTNGTEMERMEFDUSEE

Hachage ou résumé

- **Utilisation:**
  - **Intégrité de données**
  - **Signature électronique**
- **Algorithmes performants et non réversibles**
- **Les algorithmes**
  - **MD5 (Message Digest 5)** ***MIT***
    - **→ 128 bits**
  - **SHA-1** ***(Secure Hash Alg.) NIST***
    - **→ 160 bits**

SHA-1 Opérations

- Le message est complété pour être découpé en M^i multiples de 512 bits
- Chaque M^i est décomposé en 16 mots de 32 bits de M^i_0 à M^i_{15}
- On prend 5 valeurs initiales de hachage (entiers 32 bits)
- Pour chaque M^i , lors de 80 itérations, ces 5 entiers vont évoluer en intégrant les M^i_j du message pour arriver au condensé sur 5 * 32 = 160 bits
- Secure Hash Standards (NIST 2002)

http://csrc.nist.gov/publications/fips/fips180-2/fips180-2withchangenotice.pdf

valeurs initiales (p.13)

déroulement (p. 15)

Algorithme SHA-1

N Blocs de 512 bits $M^{(i)}$ décomposé en 16 $M_t^{(i)}$

$H_0^{(0)}$=…, $H_1^{(0)}$=…, $H_2^{(0)}$=…, $H_3^{(0)}$=…, $H_4^{(0)}$=… (5*32=160 bits)

Pour i de 1 à N

- a=$H_0^{(i-1)}$, b=$H_1^{(i-1)}$, … c, d, e
- Pour t de 0 à 79
  - a=…, b=…, c=…, d=…, e=…, T=…$W_t \leftarrow M_t^{(i)}$
- $H_0^{(i)}$=a+$H_0^{(i-1)}$, $H_1^{(i)}$=b+$H_1^{(i-1)}$, …

$H^{(N)}$ est le résultat du hachage

UNIVERSITÉ DE STRASBOURG S5b

MAC Message Authentification Code

- Fonction de hachage à sens unique
- Condensé à clé secrète
- Garantit l'intégrité d'un document en empêchant le recalcul du résumé
- Garantit l'identité de l'émetteur et l'authenticité du document

UNIVERSITÉ DE STRASBOURG S5b

Chiffrement symétrique

- **Méthodes de chiffrement à clé secrète**
  - **Algorithmes**
    - **DES (Data Encryption Standard)** ***IBM 1968 56 bits***
    - **3-DES Triple DES (112 bits)**
    - **RC4, RC5 (Rivest Code)(128..256 bits)**
    - **AES Advanced Encryption System** *Rijndael (*Rijmen et Daemen *Belgique) Concours NIST 2000 avec clés de 128, 192 ou 256 bits*

\+ **Opérations simples performantes et rapides**

\- **Administration des clés : Génération, Distribution, Partage et Stockage**

Chiffrement symétrique

Temps estimé pour casser les clés ***(source non vérifiée)***

	1995	2000	2005
40 bits	68 s	9 s	1 s
56 bits	53 j	7 j	19 h
64 bits	37 ans	7 ans	1750 j.
128 bits	6,7 e17 mil.	6,4 e16 mil.	1,1 e16 mil.

http://www.distributed.net/rc5/index.php.fr

UNIVERSITÉ DE STRASBOURG S5b

L'algorithme DES

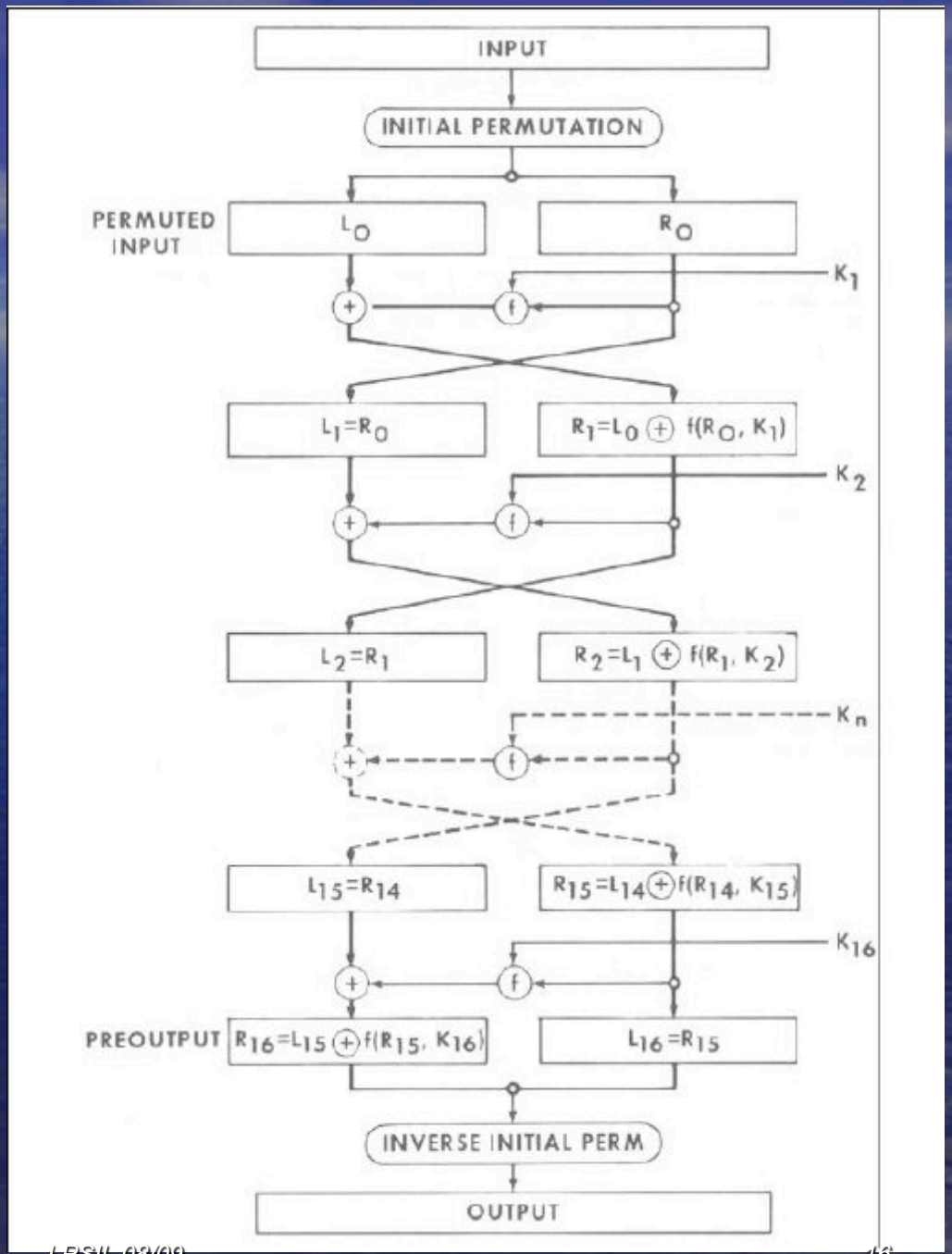
- Algorithme de chiffrement/déchiffrement de blocs de taille fixe soit 64 bits avec une clé de 64bits
- Chaque octet de la clé comporte un bit de parité pour vérifier l'intégrité de la clé de 56 bits
- 16 rondes traitent deux sous-blocs de 32 bits en utilisant un clé partielle de 48 bits
- Data Encryption Standards (NIST 1999)

  http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf

UNIVERSITÉ DE STRASBOURG S5b

L'algorithme DES

- L_i et R_i deux moitiés du bloc de 32 bits
- A partir d'une clé K, on obtient 16 K_i par décalages et permutations successives dont on extrait 48 bits
- ⊕ addition modulo 2
- f fonction qui additionne 2 arguments sur 48 bits et en extrait 32 bits
- Fonctions de conversion 32 ←→ 48 bits
- 16 itérations pour obtenir le résultat final
- Les opérations de chiffrement/déchiffrement sont performantes car elles sont limités à additions, décalages, sélections (matériel)



Chiffrement asymétrique

- **Architecture PKI (Public Key Infrastructure)**
- **Association d'une clé publique et d'une clé privée**
- **Un message chiffré avec la clé publique ne peut être déchiffré qu'avec la clé privée et inversement**
- Algorithmes
  - **DH (Diffie-Helman) (1975)**
    → clés de 512…2048 bits
  - **RSA (Rivest, Shamir, Adleman) 1977**
    → clés de 512…2048 bits
  - **ECC Eliptic Curve Crypto**
    → clés de 57 … 237 bits

UNIVERSITÉ DE STRASBOURG S5b

L'algorithme RSA : initialisations

- Soit 2 grands nombres premiers p et q
- Soit n = p * q
- La factorisation, décomposition en nombres premiers est difficile
- Soit e, un entier n'ayant aucun (peu) diviseur commun avec (p-1)*(q-1)
- La clé publique est composée du couple {e , n}
- La clé privée {d , n} telle que

$$e * d = 1 \bmod (p-1)(q-1)$$

L'algorithme RSA : opérations

- Découpage du message en blocs représentés chacun par un entier plus petit que n
  - ex. ordre alphabétique ou code ASCII
- Chiffrement du caractère M

$$C = M^e \bmod n$$

- Déchiffrement du caractère C

$$M = C^d \bmod n$$

L'algorithme RSA : exemple

- Soit p=3 et q=11 deux nombres premiers
- n = 33 = 3 * 11
- e = 7 entier n'ayant aucun diviseur commun avec (3-1)*(11-1)=20 (2 * 2 * 5)
- d = 3 car 7 * d = 1 mod 20
- Message 'OLIVE' -> 151209…
- $M_1 = 15$ $C_1 = 15^7 \bmod 33 = 27$
- $C_1 = 27$ $M_1 = 27^3 \bmod 33 = ?$
- $M_2 = 12$ $C_2 = 12^7 \bmod 33 = ?$
- $C_2 = ?$ $M_2 = ?^3 \bmod 33 = ?$

L'algorithme RSA

- La sécurité de RSA repose sur la difficulté de factoriser des très grands nombres (n'ayant que 2 diviseurs premiers grands eux aussi)

  http://www.mystery-twister.com/

PKCS Public Key Cryptographic Standards

- Formats normalisés par le RSA http://www.rsa.com
- **PKCS#1** The RSA encryption standard. This standard defines mechanisms for encrypting and signing data using the RSA public key system.
- **PKCS #7** The cryptographic message syntax standard. This defines a generic syntax for messages which have cryptography applied to it.
- **PKCS # 8** The private-key information syntax standard.
- **PKCS # 12** The personal information exchange syntax standard. This describes a portable format for storage and transportation of user private keys, certificates etc.

UNIVERSITÉ DE STRASBOURG S5b

Loi française et cryptographie

- Dépendant de la taille des clés
- Les droits s'appliquent à la génération, l'importation, l'utilisation
- Pour chaque action dans le contexte d'une utilisation privée ou professionnelle, le statut peut être :
  - Utilisation libre
  - Nécessite une déclaration
  - Nécessite une autorisation
  - Interdit

Loi française et cryptographie (références)

- DCSSI Direction Centrale de Sécurité des Systèmes d'Information)

  http://www.ssi.gouv.fr
- Depuis 1998 les clés de chiffrement ne sont plus limitées à 40 bits mais à 128 bits.

  http://www.ssi.gouv.fr/fr/reglementation/regl_crypto.html
- Les décrets de l'Autorité de Régulation des Télécommunications

  http://www.art-telecom.fr/
- Droit et Nouvelles Technologies

  http://www.droit-technologie.org/default.asp

UNIVERSITÉ DE STRASBOURG S5b

Vous en voulez encore ?

http://www.apprendre-en-ligne.net/crypto/menu/index.html

http://www.bibmath.net/crypto/index.php3

http://www2.cnrs.fr/presse/communique/947.htm

http://csrc.nist.gov/

http://www.journaldunet.com/solutions/0406/040610_crypto_quantique.shtml