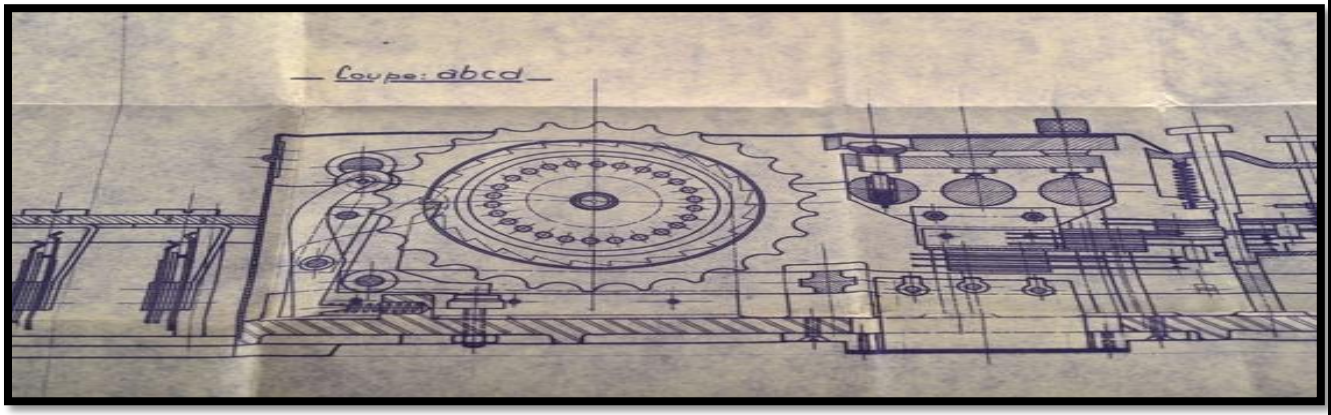
M4204 - CRYPTOGRAPHIE

TD05 – CHIFFREMENT SYMETRIQUE



Après avoir vu les techniques de bases de la cryptographie et utiliser des méthodes de chiffrement de type « papier-crayon », nous allons maintenant aborder la cryptographie moderne et essayer de comprendre comment sont mis en œuvre les différents algorithmes de chiffrement à notre disposition.

© Patrice Gommery – 2019

TD05 – CHIFFREMENT SYMETRIQUE

1 – SYMETRIQUE ou ASYMETRIQUE

Dans un premier temps, il est important de comprendre à quel type de chiffrement nous avons à faire. Si comme l'a démontré Kerchoffs dans son traité de cryptographie militaire en 1883, la sécurité ne repose que sur le secret de la clé, il faut avant tout distinguer deux types de clés (et donc de chiffrement) :

LE CHIFFREMENT ASYMETRIQUE qui utilise deux clés : Une clé privée et une clé publique.

LE CHIFFREMENT SYMETRIQUE ou chiffrement à clé secrète qui utilise une seule clé. **Cette même clé servant à la fois à chiffrer et à déchiffrer**. C'est ce type de chiffrement que nous avons utilisé jusqu'ici et dont nous allons découvrir les versions « modernes ».

2 – ENIGMA

Impossible de ne pas parler d'Enigma dans un cours de Cryptographie.

Cette machine électromécanique qui ressemble à une machine à écrire est à la croisée des méthodes anciennes et modernes de la cryptographie. Utilisée par les allemands pendant la seconde guerre mondiale, elle est constituée d'une partie mécanique utilisant des rotors et d'une partie construite autour de composants électriques permettant d'afficher le résultat du chiffrement.

Ce système tend à s'approcher du « Chiffrement Parfait » décrit par Vernam en 1926 en permettant, de par sa complexité, l'utilisation de plusieurs milliards de milliards de combinaisons possibles pour générer une clé.

KERCKHOFFS

« La sécurité d'un système de cryptage ne doit pas dépendre de la préservation du secret de l'algorithme. La sécurité ne repose que sur le secret de la clé »

Traité de cryptographie militaire - 1883

© *Patrice Gommery - 2019*

CHIFFRE DE VERNAM

En 1917 Gilbert VERNAM, ingénieur d'AT&T pose les bases d'un système de chiffrement parfait utilisant un masque jetable.

La clé du système de chiffrement doit posséder les caractéristiques suivantes :

- La clé est aussi longue que le texte a chiffré
- Les caractères de la clé doivent être choisi de façon totalement aléatoire
- La clé ne doit être utilisée qu'une seule fois

En 1949, Claude Shannon démontre qu'effectivement un tel système est théoriquement inviolable, mais malheureusement dans la réalité il est très difficilement exploitable vu la complexité de mise en œuvre.

L'explication en Vidéo :

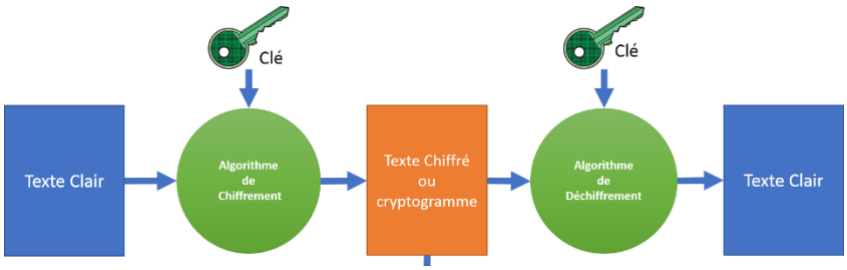
Exo7Math - Cryptographie - Partie 3

3 – LES ALGORITHMES A CHIFFREMENT SYMETRIQUE

De nos jours l'Informatique à bien entendu supplantée toutes les méthodes de chiffrement anciennes, mais sans pour autant les remplacer complétement, puisque toutes ces techniques de substitution ou de transposition sont simplement appliquées au numérique avec la puissance des ordinateurs d'aujourd'hui.

On ne parle donc plus vraiment de mécanismes de chiffrement, mais d'algorithmes qui sont implémentés par divers programmes comme par exemple OpenSSL ou PGP que vous avez utilisé pendant les travaux pratiques.

Tous les algorithmes que nous verrons dans ce cours sont des algorithmes à clé secrète et mettent donc en œuvre un chiffrement symétrique des données avec une seule clé pour chiffrer et déchiffrer.



Nous conservons donc notre schéma classique avec une même clé qui sert à la fois à chiffrer et à déchiffrer le message. Les algorithmes de chiffrement et de déchiffrement utilisent la même clé et fonctionnent donc de façon réversible.

Ces algorithmes sont connus de tout le monde et c'est donc juste le secret de la clé qui va garantir la sécurité des données.

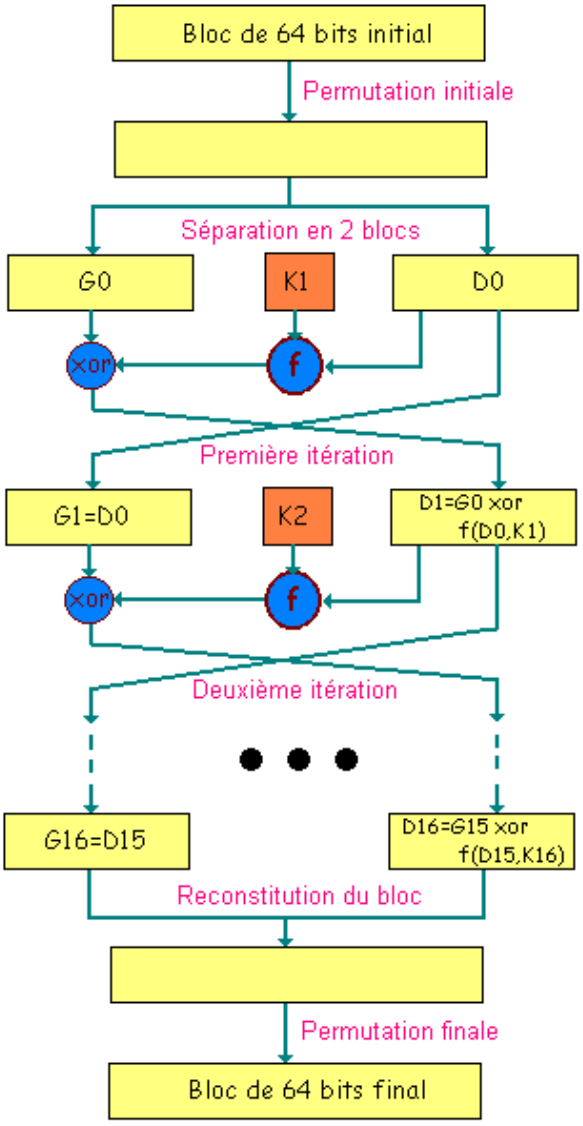
4 – DES & TRIPLE DES

Le plus ancien de ces algorithmes est sans doute DES (Data Encryption Standard). Sa version standard est apparue en 1977 et est depuis devenu complètement obsolète, surtout à cause du peu de clés utilisables et surtout facilement calculables rapidement avec les ordinateurs actuels.

:

© Patrice Gommery - 2019

DES comme la majorité des algorithmes modernes est un système de chiffrement par Bloc. Il manipule des blocs de 64 Bits et fonctionne en quatre étapes :



- Diversification de la clé initiale en 16 sous-clés
- Permutation initiale du Bloc à chiffrer.
- 16 itérations utilisant chacune des sous-clés
- Permutation finale pour reconstituer un bloc chiffré.

Les itérations sont des suites de substitutions et de permutations mettant en œuvre des fonctions logiques simples comme par exemple le XOR ou OU-EXCLUSIF.

Petite Explication en vidéo : Exo7Math - Cryptographie - Partie 3
(à 13 :38 mn dans le film)

ALAN TURING

Mathématicien et cryptologue britannique, il est un des plus célèbres pionniers de l'informatique actuelle.

La machine qu'il conçoit pour « casser » les messages chiffrés avec Enigma par les allemands pendant la seconde guerre mondiale est pour certains le premier ordinateur de l'Histoire.

Le film « Imitation Game » relate sa vie et sa contribution à la cryptanalyse d'Enigma.

Un lien pour comprendre Enigma :

E-Penser : Ordinateur et Pomme Empoisonnée

© *Patrice Gommery - 2019*

CHALLENGE RSA

La compétition de clé secrète RSA était un concours lancé par le laboratoire RSA
(à ne pas confondre avec l'algorithme de chiffrement asymétrique du même nom)

Crée en 1997 son but était d'estimer la sécurité des algorithmes de chiffrement symétrique tels que DES

En Juin 1997, le premier DES a permis de retrouver une clé de 56Bits en 140 Jours.

En 1999, il n'a fallu que 22 heures et 15 Mn pour que conjointement une machine dédiée (Deep Crack) et Distribued.net (un projet de calcul distribué sur le Net) réussisent la même opération.

A l'origine DES utilise des clés de 64 Bits (56 Bits+8 Bits de parité) ce qui donne environ 72 milliards de milliards de possibilité.

Dès 1997, il n'avait à l'époque fallu que trois semaines à quelques centaines d'ordinateur pour casser DES et générer toutes les clés possibles. Aujourd'hui avec la puissance de calcul des ordinateurs actuels, il ne faudrait que quelques secondes.

Pour combler cette faiblesse est apparu à la fin des années 90, un autre algorithme le TRIPLE-DES qui comme son nom l'indique applique 3 fois le chiffrement DES original.

L'enchainement et le calcul des clés fournit alors une clé finale de 112 Bits. Bien que reconnu et normalisé par le NIST (Institut National des normes et de la technologie) américain, cet algorithme est peu utilisé à cause de sa lenteur. Il fut rapidement remplacé par A.E.S au début des années 2000.

5 – IDEA

International Data Encryption Algorithm fut proposé dès 1992 pour le remplacement de DES. Il est notamment utilisé par le logiciel PGP (Pretty Good Privacy).

Il utilise des clés de 128 Bits et seulement 3 opérations :

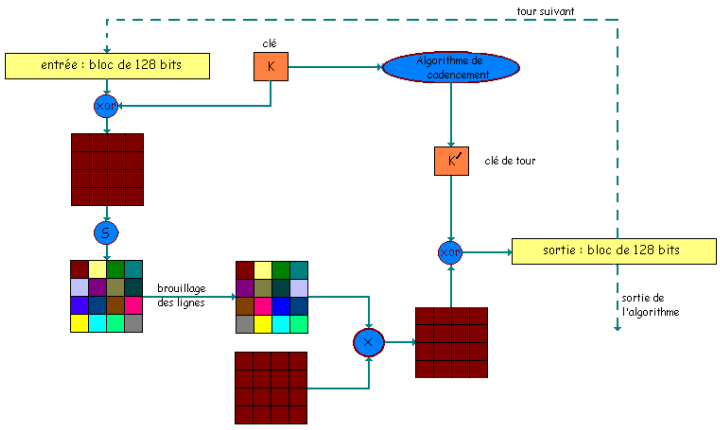
- Le XOR
- L'Addition Modulo 2^{16}
- La Multiplication Modulo 2^{16}

Donc là aussi des opérations relativement simples et rapide à exécuter pour un processeur moderne.

6 – AES

Advanced Encryption Standard (Norme de Chiffrement avancé) est aussi connu sous le nom de **Rijndael**. Il est le lauréat d'un concours organisé en 2000 par le **NIST** et devint le nouveau standard de chiffrement symétrique en remplacement de DES. Il est encore aujourd'hui un des algorithmes de chiffrement symétrique le plus utilisé.

© Patrice Gommery - 2019



Il chiffre par blocs de 128 Bits qui subissent chacun une séquence de 5 transformations répétées 10, 12 ou 14 fois (tours) selon la longueur de la clé :

- Addition (XOR)
- Transformation non linéaire (Matrice 4x4)
- Décalage de lignes
- Brouillage de colonnes
  (Multiplication de la matrice par une autre)
- Addition de la clé de tour (Clé de contexte)

Les clés peuvent faire 128, 192 ou 256 Bits. Pour l'instant, il n'existe pas d'attaque connue en un temps raisonnable sur cet algorithme, mais pour combien de temps encore ?

7 – FORCES ET FAIBLESSES DU CHIFFREMENT SYMETRIQUE.

Vous l'aurez compris, la principale faiblesse des algorithmes de chiffrement symétrique est la clé secrète. En effet, hormis sa longueur qui peut être plus ou moins grande, il subsiste dans tous les cas un problème crucial :

Comment transmettre la clé ?

© Patrice Gommery - 2019

LA CRYPTOGRAPHIE MODERNE

« N'accordez jamais une confiance aveugle à un système de cryptographie »

Gilles Dubertret

Initiation à la cryptographie.

Cours et Exercices corrigés

Aout 2018
ISBN : 978-2-311-40615-3

XOR

Le XOR est une fonction logique très utilisée par les algorithmes de chiffrement symétrique.

Elle est rapide et surtout réversible. En effet si l'opération A XOR B donne C, C XOR A donnera forcément B et B XOR C donnera forcément A.

A	B	C
0	0	1
0	1	0
1	0	0
1	1	1

En effet, si nous prenons comme exemple un échange de message entre Alice et Bob. Nous voyons bien sur le schéma qu'ils utilisent la même clé secrète pour chiffrer et déchiffrer, mais comment BOB a-t-il obtenu la clé d'Alice ?

Autre point faible. Que se passe-t-il si Alice veut envoyer des messages à plusieurs correspondants ?
Doit-elle utiliser une clé pour chacun de ses correspondants ou doivent-ils se mettre d'accord sur l'utilisation d'une clé commune ? Dans ce dernier cas, tout le monde utilisant la même clé, comment savoir qui a chiffré le message ?

C'est un autre point faible du chiffrement symétrique. Celui-ci **n'assure que la confidentialité des données**, **pas l'authentification** de l'émetteur du message.

Alors, malgré ses faiblesses, pourquoi utiliser le chiffrement symétrique ? Tout simplement parce qu'il est **facile à mettre en œuvre et rapide à exécuter.**

7 –EXERCICES : ALGORITHME SYMETRIQUE

Pour l'exemple, nous allons simuler un algorithme symétrique avec 2 opérations simples : un XOR et un décalage.

Notre clé aura une valeur entre 1 et 20
Nous utiliserons la table ASCII pour convertir nos lettres en numérique. Exemple A = 65, B=66 etc. ..
Pour les opérations XOR, une simple calculette en mode programmeur ou scientifique suffit.

Notre algorithme de chiffrement est le suivant :

1. Traduction du mot en valeurs numériques (table ASCII)
2. Coupure du mot en deux parties – Permutation des deux parties
3. Réalisation d'un XOR sur chaque caractère de la partie de droite avec une la clé
4. Décalage des caractères de deux positions sur la droite
5. Second découpage du mot et nouvelle permutation
6. Nouvel XOR sur la partie de droite.
7. Traduction des nouvelles valeurs numériques en lettres.

© Patrice Gommery - 2019

Étape 1 :

Décrivez l'algorithme de déchiffrement

Étape 2 :

Déchiffrez le mot **ONRPME]T** qui est chiffré avec la valeur 17.

Étape 3 :

Codez un mot de 8 lettres (en MAJUSCULES) avec une valeur comprise entre 10 et 15.

Étape 4 :

Échangez votre résultat (sans la clé) avec votre voisin

Étape 5 :

Essayez de décrypter le mot chiffré par votre voisin

Algorithme de chiffrement :

1. **Traduction du mot en valeurs numériques (table ASCII)**
2. **Coupure du mot en deux parties – Permutation des deux parties**
3. **Réalisation d'un XOR sur chaque caractère de la partie de droite avec une la clé**
4. **Décalage des caractères de deux positions sur la droite**
5. **Second découpage du mot et nouvelle permutation**
6. **Nouvel XOR sur la partie de droite.**
7. **Traduction des nouvelles valeurs numériques en lettres.**

TABLE ASCII

Dec	Carácter
64	@
65	A
66	B
67	C
68	D
69	E
70	F
71	G
72	H
73	I
74	J
75	K
76	L
77	M
78	N
79	O
80	P
81	Q
82	R
83	S
84	T
85	U
86	V
87	W
88	X
89	Y
90	Z
91	[
92	\
93	]
94	^
95	

© *Patrice Gommery - 2019*