Cryptographie

Mercredi 28 Février 2007

Intervenants

- Philippe Perret - MSI Groupe Arkoon
- Serge Richard (CISSP®) - IBM France

Agenda

- Introduction à la cryptographie
- Histoire de la cryptographie
- Concepts et méthodologies
- Applications de la cryptographie
- Attaques sur la cryptographie
- Focus sur les courbes elliptiques

Introduction à la cryptographie

Serge RICHARD - CISSP®

Objectifs

- La **cryptographie** est une des disciplines de la cryptologie s'attachant à protéger des messages (assurant confidentialité et/ou authenticité) en s'aidant souvent de *secrets* ou *clés*. Le mot cryptographie découle des mot grecs "krypto" (je cache) et "graphe" (le document)
- La **cryptologie**, étymologiquement la science du secret, ne peut être vraiment considérée comme une science que depuis peu de temps. Cette science englobe la cryptographie, l'écriture secrète et la cryptanalyse, l'analyse de cette dernière. On peut dire que la cryptologie est un art ancien et une science nouvelle
- **L'objectif fondamental** de la cryptographie est de permettre à deux personnes de communiquer au travers d'un canal peu sûr (téléphone, réseau informatique ou autre) sans qu'un opposant puisse comprendre ce qui est échangé.

Postulats

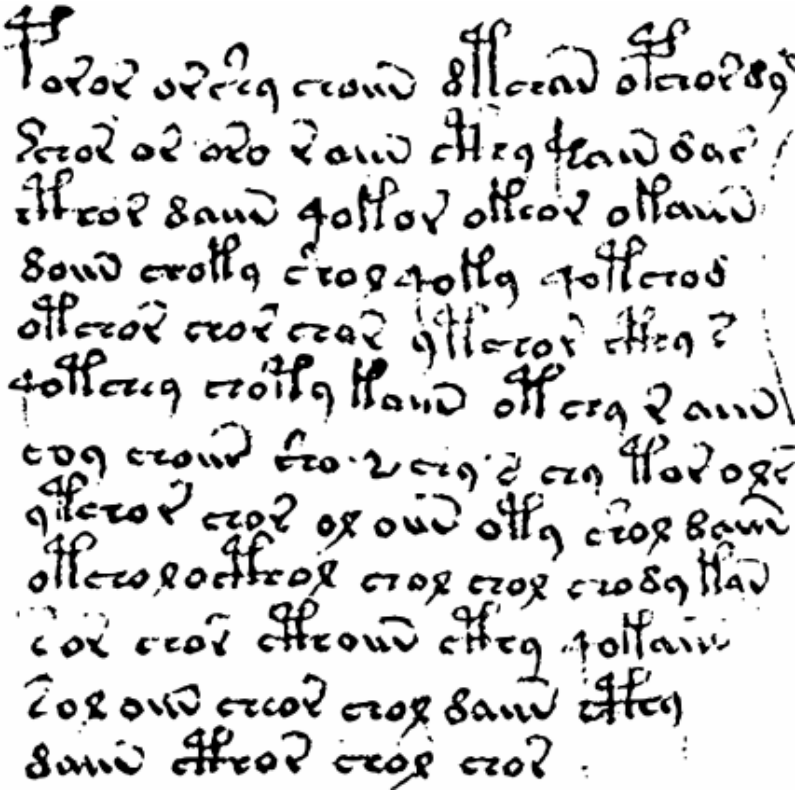
- Les postulats de sécurité associés à la cryptographie sont :
  - L'intégrité des données : Le contrôle d'intégrité d'une donnée consiste à vérifier que cette donnée n'a pas été altérée, frauduleusement ou accidentellement.
  - Le contrôle d'accès : Il s'agit d'authentifier les utilisateurs de façon à limiter l'accès aux données, serveurs et ressources aux seules personnes autorisées (un mot de passe pour un disque dur, par exemple).
  - La confidentialité : Il s'agit de rendre l'information inintelligible à tous les opposants tant lors de sa conservation qu'au cours de son transfert par un canal de communication.
  - L'identification: Le contrôle d'identification consiste à s'assurer que le destinataire est bien celui qui prêtant être (authentification des partenaires) et d'obtenir une garantie que l'expéditeur a bien signé l'acte (authentification de l'origine des informations).
  - La non répudiation: Il s'agit de garantir l'authenticité de l'acte. L'expéditeur ne peut nier le dépôt d'information, le réceptionneur ne peut nier la remise d'information, ni l'un ni l'autre ne peut nier le contenu de cette information.

Glossaire

- Comme toute science, celle-ci possède son propre langage. Étant donnée la relative jeunesse de cette science, et le fait qu'une très grande partie des publications dans ce domaine sont en langue anglaise, le problème de la terminologie francophone se pose, parfois par manque de traduction

- Le **chiffrement** est le procédé grâce auquel on peut rendre la compréhension d'un document impossible à toute personne qui n'a pas la clé de (dé)chiffrement.
- Une **clé** est un paramètre utilisé en entrée d'une opération cryptographique.
- **Déchiffrer** consiste à retrouver le texte original (aussi appelé clair) d'un message chiffré dont on possède la clé de (dé)chiffrement.
- **Décrypter** consiste à retrouver le texte original à partir d'un message chiffré sans posséder la clé de (dé)chiffrement.
- **Texte clair** [Clear text ou Plain text] : Caractères ou bits sous une forme lisible par un humain ou une machine.
- **Texte chiffré** [Cipher text] : Résultat de la manipulation de caractères ou de bits via des substitutions, transpositions, ou les deux.
- La différence entre un **algorithme** et un **protocole** est une question d'interactivité : pour un algorithme, une seule personne est impliquée, celle qui fait les calculs ; pour un protocole, plusieurs entités interviennent, il y a échange d'informations.

Histoire de la cryptographie



L'origine des codes secrets

- De l'antiquité à la renaissance, l'art de la cryptographie met en œuvre, pour cacher la substance d'un texte, une combinaison plus ou moins élaborée de substitutions et de permutations
- Dès l'origine, la cryptographie a été utilisée à des fins diplomatiques puis militaires
  - En Egypte, 2000 ans avant notre ère un scribe avait gravé des hiéroglyphes transformés sur le pierre tombale de Khumhotep II pour rendre inintelligible la description de sa vie.
  - A la même époque, un général Grec, Enée le tacticien, consacre un chapitre de son ouvrage ***Commentaires sur la défense des places fortes*** à la sécurité des communications et donne quelques méthodes pour chiffrer
  - Jules César dans ***la Guerre des Gaules*** décrit un procédé de substitution aujourd'hui bien connu: Il consiste pour chiffrer à décaler d'un nombre de rangs convenu la lettre « claire » dans l'alphabet usuel. Si la clé est 3, a est remplacé par d et b par e …

L'origine des codes secrets

- A Sparte, au IV ème siècle avant notre ère, les communications entre les chefs des armées et les commandants étaient chiffrées à l'aide d'une **Scytale**, un bâton sur lequel on enroule une lanière en spires jointives

L'origine des codes secrets

- En Crète, **un disque de Phaïstos**, datant de 1700 avant notre ère, comportant un texte chiffré sur les deux faces à été retrouvé. Ce texte n'est encore à ce jour décrypté de manière sure.

Les sciences du secret

- Il existe plusieurs manière d'assurer la confidentialité des informations échangées
  - La ***cryptographie*** consistant à crypter le message transmis est sans doute la technologie qui est et a été la plus utilisée.
  - La ***stéganographie*** est une autre technique consistant à dissimuler le message dans un contexte innocent. Impossible donc de trouver un message si on ignore jusqu'à son existence.

- La stéganographie est une discipline très ancienne qui date de l'antiquité mais dont la formalisation est récente
  - Ainsi, en 440 avant notre ère, Hérodote raconte comment, on rasa la tête d'un esclave, puis on y tatoua un message qui devint invisible après que les cheveux aient repoussées
  - Cette méthode était encore utilisée par les espions allemands au début du XX siècle
  - Une ancienne technique chinoise de nature différente : un texte imprimé sur de la soie était enfermé dans une boulette de cire que le messager avalait
  - L'encre sympathique est la plus connue des méthodes de stéganographie
  - La dissimulation d'images ou de texte à l'intérieur d'autres images est devenu un processus facile dont les programmes sont disponibles sur Internet
  - L'ère numérique ouvre de nouvelles possibilités: La stéganographie à clé secrète permet d'extraire un message d'un support numérique, le « stégano-médium »

Un exemple célèbre de dissimulation de message
La lettre de George Sand

Je suis très émue de vous dire que j'ai
bien compris, l'autre jour que vous avez
toujours une envie folle de me faire
danser. Je garde un souvenir de votre
baiser et je voudrais que ce soit
là une preuve que je puisse être aimée
par vous. Je suis prête à vous montrer mon
affection toute désintéressée et sans cal-
cul. Si vous voulez me voir ainsi
dévoiler, sans aucun artifice, mon âme
toute nue, daignez donc me faire une visite.

...

Evolution des technologies cryptographiques
Le Moyen Age: L'obscurographie

- A une époque où les hauts personnages sont pour la plupart illettrés, l'écriture constitue par elle même un moyen de chiffrement réservé aux lettrés
- L'église prohibe l'usage du chiffrement dans lequel est discerne une action démoniaque
- Les dignitaires se réservent le chiffrement pour leur propre usage en utilisant les techniques de l'antiquité
  - Rédaction des voyelles par des points ou des signes convenus
  - Rédaction du texte à l'aide d'un alphabet étranger (Grec ou Hébreu)
  - Lettres ou certains mots remplacés par des signes et des dessins
  - Ecriture du texte de droite à gauche
  - Utilisation de méthodes de stéganographie utilisées par les romains.
- Livrer ses pensées peut être dangereux et conduire, selon l'interprétation de l'église, à la renommée ou au bûcher.
- Les auteurs prennent leurs précautions et chiffrent leur nom pour renier ou revendiquer la paternité de leur écrits.
  - Ainsi Rabelais signe **Alcofribas Nasier**

Evolution des technologies cryptographiques
La renaissance: L'éveil cryptographique

- Avec l'invention de l'imprimerie, vers 1450, l'emploi du chiffre s'impose et se généralise dans les relations diplomatiques et au plus haut niveau du commandement militaire
- La science du chiffre progresse
  - La transposition et la substitution sont reconnus comme étant des principes fondamentaux
  - Ils sont employés isolément ou en combinaison
- L'art du déchiffrement progresse également
  - Analyse des fréquences d'apparition des symboles.
  - La fréquence d'apparition d'une lettre donnée est caractéristique d'une langue.
- Les chercheurs en cryptologie sont renommés
  - ***Alberti***, le célèbre architecte de Florence, ***l'abbé Trithème***, savant lettré consulté par toute l'Europe, le physicien napolitain ***Porta***, le mathématicien Milanais ***Cardan*** …
- En 1586 le mathématicien Français *Blaise de Vignère*, secrétaire de Charles IX, fait la synthèse de tout ces travaux dans le *Traité des secrètes manières d'écrire*

Antoine Rossignol (1600-1682)

- Grand spécialiste des codes et décryptement, il rénove le chiffre Français sous Louis XIV. Il est l'auteur des premiers grands dictionnaires de chiffrement désordonnés tel que le « Grand Chiffre » de Louis XIV qui résistera plus de 200 ans au décryptement

- Le Grand Chiffre, était un code désordonné, c'est à dire que des mots successifs dans l'alphabet ne sont pas chiffrés par des nombres successifs mais par des nombres pris au hasard.
- Cela permet d'éviter qu'un décrypteur ne devine la première lettre du mot à la vue du message chiffré

Evolution des technologies cryptographiques
La renaissance: L'éveil cryptographique

- ***Le procédé de Vigenère*** consiste à changer l'alphabet de substitution à chaque chiffrement d'une lettre, ce qui fait que l'on ne peut tenter de décrypter le message en utilisant la fréquence des lettres.
- Pour cela, on construit un carré constitué de tous les alphabets décalés d'une lettre.
- Le chiffrement part d'un mot clé. Par exemple **TRIAGE**. Pour coder la première lettre C du message en clair **COULER**, on considère la ligne 10 commençant par T, indiquant que le C doit être chiffré par son correspondant sur cette ligne, soit V. La seconde lettre O doit être chiffré en prenant la ligne commençant par R et ainsi de suite.

Clair	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
1	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
2	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
3	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
4	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
5	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
6	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
7	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
8	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
9	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
10	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
11	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
12	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
13	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
14	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
15	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
16	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
17	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
18	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
19	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
20	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
21	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
22	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
23	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
24	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
25	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
26	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

Evolution des technologies cryptographiques
Le déclin: XVIII et début du XIX

- Le chiffre Français s'étiole pour deux raisons :
  - On s'oriente vers des actions d'espionnage et on délaisse peu à peu la cryptologie pure
  - L'activité désinvolte des **« Cabinets noirs »** conduit les ambassadeurs à éviter la poste royale et à systématiser le recours à la valise diplomatique, plus lente mais plus sure

- La science cryptographique Française décline :
  - Les Emigrés contre-révolutionnaires, en 1796, communiquent avec leur partisans restés en France avec un chiffre qui n'est qu'une simple substitution de Jules César
  - Pendant la campagne d'Italie, Bonaparte ne dispose que d'un procédé de Jules César
  - Sous l'Empire, Napoléon dispose d'un Grand Chiffre et d'un Petit Chiffre dont on se sert fort peu et fort mal. L'envoie du même message chiffré puis en clair n'est pas rare.

- Sous la Restauration, Louis Philippe et le second Empire, le déclin se poursuit :
  - Durant la guerre de 1870-1871, le maréchal Bazaine de plaint de ne pas avoir de moyen de chiffrement. Les services de Napoléon III sont incapables de répondre à sa demande

Evolution des technologies cryptographiques
De la fin du XIX siècle à 1914 – Le Réveil

- En 1844, la télégraphie électrique est adoptée en remplacement du télégraphe :
  - Le développement du télégraphe permet l'interception aisée des dépêches diplomatiques
  - Une copie en est remise au Quai d'Orsay et au ministère de la Défense
- L'activité de décryptement renaît :
  - Entre 1887 en 1900, tous les pays d'Europe se dotent de bureaux spécialisés
  - A partir de 1904, la poste envoie systématiquement une copie des télégramme cryptés au Service d'analyse cryptographique de la Sûreté Générale
  - Ce service décrypte le chiffre diplomatique du Japon, pendant la guerre Russo-Japonaise et quantité d'autres (Turquie, Espagne, Monaco, agents financiers Russes, serbes, roumains …) jusqu'en 1913, date à laquelle il lui est interdit d'accéder aux dépêches diplomatiques
- Sur le plan militaire, le chemin de fer et le télégraphe changent les conditions de combat :
  - Le centre de commandement se transforme en centre de transmission
  - Le chiffrement revient à l'ordre du jour, et on l'enseigne dans les écoles militaires
  - L'école Française de cryptologie est la meilleure et compte de nombreux spécialistes

Evolution des technologies cryptographiques
La grande guerre 1914 – 1918 – L'arme cryptographique

- La France crée en 1912 la Section du chiffre de l'armée
- En 1914, les Russes subissent la terrible défaite de Tannenberg en raison d'une absence totale de sécurité des communications.
  - Les premiers chiffrements restent assez simples et sont ainsi facilement décryptés
  - L'établissement du régime Communiste de 1917 est ainsi facilité par le décryptement des communications militaires tsaristes
- Dès le 1er Août 1914, La section du chiffre est capable de décrypter les communications chiffrées Allemandes
  - Le cryptologue le plus doué de l'équipe est le lieutenant **Painvain**.
  - Il est l'auteur d'un véritable exploit en Juin 1918. Les Allemands ont adoptés un nouveau système de chiffrement et espèrent rompre les lignes française et atteindre Paris
  - Cinq axes d'attaque sont possibles. Ou et comment disposer les dernières forces françaises
  - Par un travail acharné, Painvain reconstitue le nouveau code de l'ennemi le 2 Juin
  - Un message chiffré alors décrypté se révèle d'une importance capitale car il permet de déterminer l'axe d'attaque.
  - Foch est averti et fait mettre en place les troupes de réserve. L'attaque allemande a lieue le 9 Juin. Elle est stoppée net et les forces françaises contre-attaquent.
  - La victoire des alliés suivit quelques mois après.

Evolution des technologies cryptographiques
La grande guerre 1914 – 1918 – L'arme cryptographique

Le Radiogramme de la Victoire

DÉCRYPTEMENT DU RADIOGRAMME DE LA VICTOIRE

Pour chiffrer leur message, l'état-major allemand remplaçait chaque lettre du clair par un couple de lettres, la première étant prise dans la colonne et la seconde dans la ligne: ainsi la lettre *m* est remplacée par le couple DA. Le message allemand d'origine, *Munitionierung beschleunigen punkt soweit nicht eingesehen auch bei tag* («Hâter l'approvisionnement en munitions, le faire même de jour tant qu'on n'est pas vu»), était destiné à une grande unité de la région de Remaugis au Nord de Compiègne et, par conséquent, indiquait le lieu de l'attaque allemande. Le message ainsi chiffré avec la clé de substitution était: DAGXFAGFXGG-FAGFXAVXGXFAXXVGXAGDAAGVFFXAGXFAGFXXXAFA-VAGXFADDXGGDADFDXAGFXGFAGFAAGVXGXAGF-FAXXXAGDXAGVXAFADGGXAAGVVGXAGFXGDGXX

Ensuite ce premier cryptogramme était surchiffré avec le tableau de transposition indiqué en bas à gauche.

De sorte que le message était réécrit en prenant les colonnes dans l'ordre de leur numérotation:

FGAXA XAXFF FAFFA AVDFA GAXFX FAAAG DXGGX AGXFD XGAGX GAXGX AGXVF VXXAG XFDAX GDAAF DGGAF FXGGX XDFAX GXAXV AGXGG DFAGD GXVAX VFXGV FFGGA XDGAX ADVGG A

Painvin, après un travail acharné, réussit à reconstituer la clé de substitution et le tableau de transposition, et parvint au décryptement. Le message décrypté fut retransmis au GQG de Foch qui fut convaincu de l'imminence de l'attaque sur Compiègne. Les dernières troupes de réserve furent placées en position et repoussèrent l'attaque. La victoire des Alliés suivit quelques mois après.

CLÉ DE SUBSTITUTION

	A	D	F	G	V	X
A	c	o	8	x	f	4
D	m	k	3	a	z	9
F	n	w	l	o	j	d
G	5	s	i	y	h	u
V	p	l	v	b	6	r
X	e	q	7	t	2	g

TABLEAU DE TRANSPOSITION

6	16	7	5	17	2	14	10	15	9	13	1	21	12	4	8	19	3	11	20	18
D	A	G	X	F	A	G	F	X	G	G	F	A	D	F	A	G	F	X	A	V
X	G	X	F	A	X	X	V	G	X	A	G	D	A	A	G	V	F	F	X	A
G	X	F	A	G	F	X	X	X	A	F	A	V	A	G	X	F	A	D	D	X
G	G	D	A	D	F	D	X	A	G	F	X	G	F	A	G	F	A	A	G	V
X	G	X	A	G	F	F	A	X	X	X	A	G	D	X	A	G	V	X	A	F
A	D	G	G	X	A	A	G	V	V	G	X	A	G	F	X	G	D	G	X	X

George Painvain
(1886 – 1980)

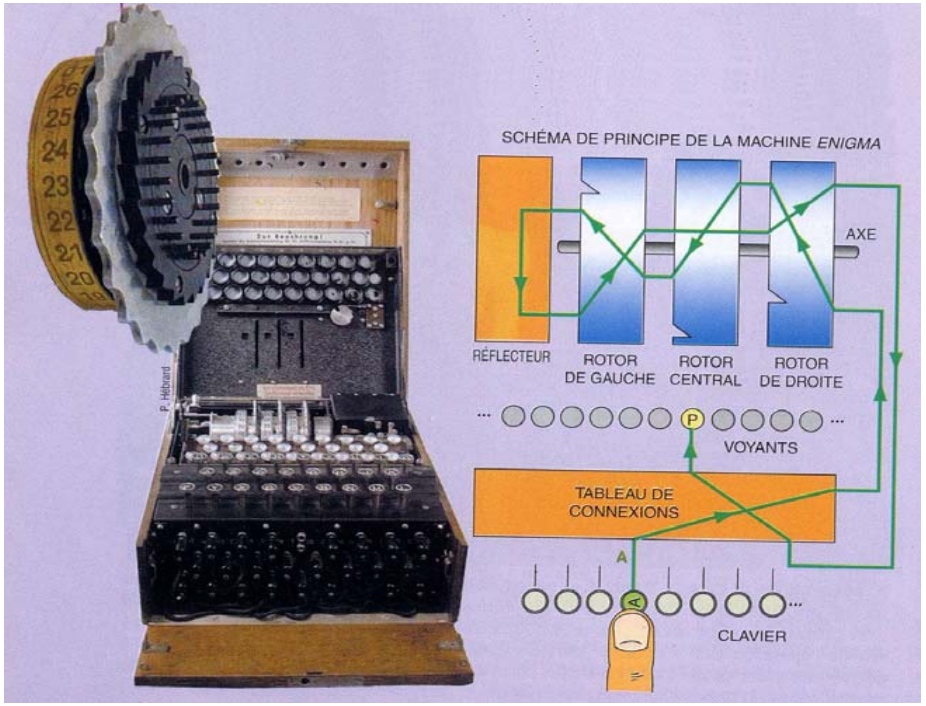
Evolution des technologies cryptographiques
La grande guerre 1914 – 1918 – L'arme cryptographique

- En janvier 1917, le service de décryptement britannique , la Room 40, décrypte une dépêche du ministre allemand des affaires étrangères, Zimmermann :
  - Dans cette dépêche, l'Allemagne annonce son intention de lancer une guerre sous-marine totale
  - Le gouvernement Allemand propose au Mexique une alliance militaire contre les Etats- Unis avec reconquête pour le Mexique, du Texas, Nouveau Mexique et Arizona
- Les Britanniques remettent le clair du télégramme aux autorités Américaines :
  - Livré à la presse et publié le 1er Mars 1917, le télégramme fait basculer l'opinion américaines, encore réticente, à accepter l'entrée en guerre
- Le président Wilson, en se référant au télégramme Zimmermann, obtient l'accord du congés. Les Etats-Unis entrent en guerre :
  - Jamais un décryptement n'a eu une telle conséquence.

De la mécanique à l'ordinateur
La machine Enigma

- L'enseignement que les états majors tirent de la guerre est qu'il faut automatiser les opérations de chiffrement
  - L'armée allemande s'équipe de machines **Enigma** dès 1926
  - L'armée française s'équipe au milieu des années 1930, de matériel suédois: La machine C36 et la machine B211 qui resterons en service environ 20 ans

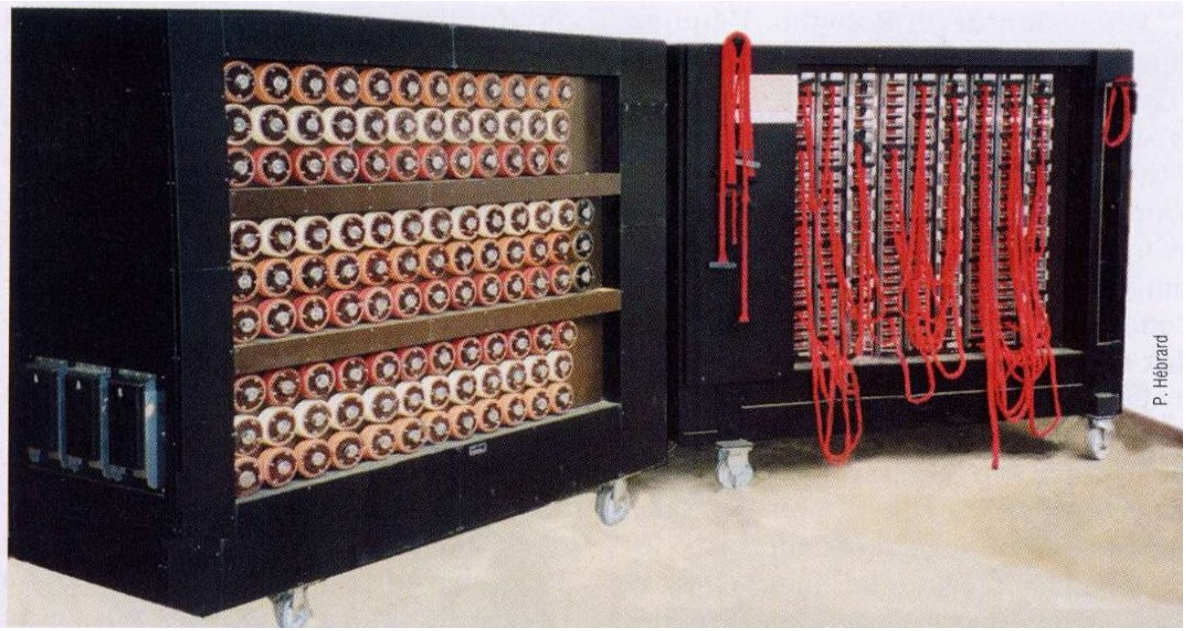
- La machine **Enigma** possède 3 rotors, chaque rotor contenant les 26 lettres de l'alphabet. L'ordre de grandeur de la combinatoire est donc de $(26)^3$, c'est à dire 17576 positions initiales des rotors.
- La combinatoire est encore augmenter par le fait que les rotors sont permutables
- Vers la fin de 1938 les 3 rotors sont choisis parmi 5, ce qui fait passer les possibilités d'arrangement des rotors de 6 à 60.



De la mécanique à l'ordinateur
La machine Enigma

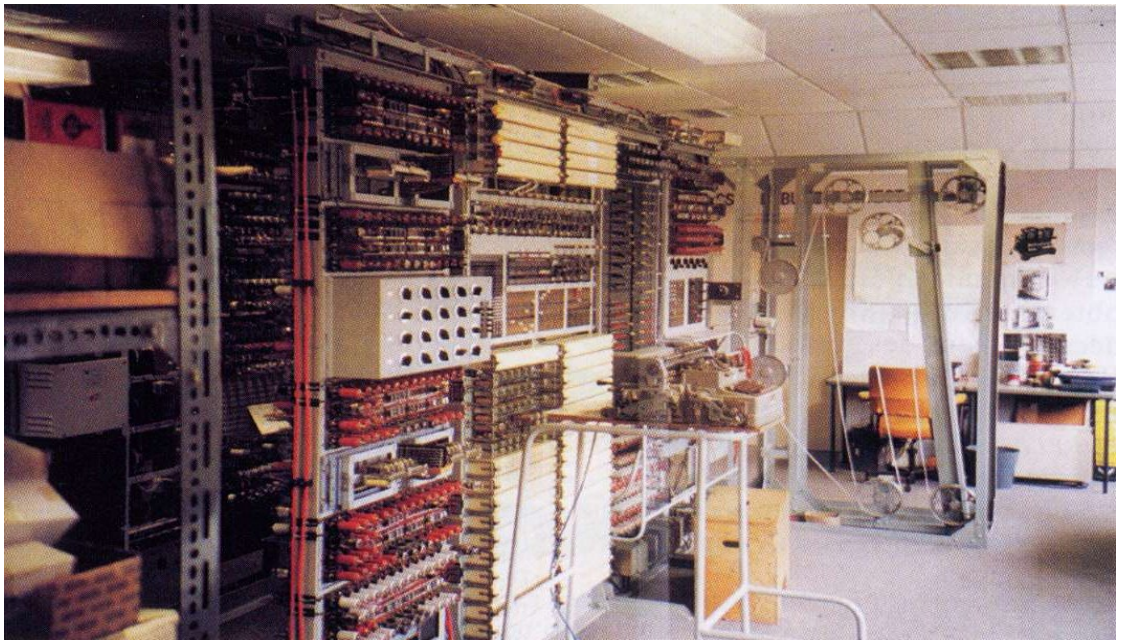
- Après la première guerre Mondiale, le bureau Chiffre de la Pologne s'intéresse de près aux communications Allemandes. Les Polonais connaissent bien Enigma
  - En Décembre 1932, Enigma est entièrement reconstituée et dès 1933 la fabrication des répliques d'Enigma commençait
  - En Septembre 1938, **Rejewski** met au point une machine appelée **Bomba** qui est constituée de six répliques d'Enigma permettant d'accélérer la recherche des clés. La recherche d'une clé prend environ 2 heures.
  - En 1939, les allemands modifient Enigma pour porter la combinatoire à 159 10^{18} mettant les décryptement hors de portée. Devant l'imminence de l'invasion les Polonais décident d'exposer leurs travaux aux Français et aux Anglais.
  - Deux jeunes mathématiciens Anglais, **Welchman** et **Turing**, imaginent une machine universelle, dite **machine de Turing**, qui travaillerai directement sur le contenu du message chiffré de manière à être indépendante des procédures de chiffrement et de transmission
  - Le prototype est prêt en mars 1940 et deux machines plus achevées sont réalisées en Septembre 1940. le décryptement d'un message prend alors environ **2 jours.**
  - A partir de Juin 1943, la mise en service d'une nouvelle version d'Enigma, oblige les Britanniques et les Américains à améliorer les **BOMBES.** Ces décryptements redonnèrent l'avantage aux alliés qui ont remporté la **Bataille de l'Atlantique**, un tournant dans la guerre.

De la mécanique à l'ordinateur
Les BOMBES rapides



- Les Bombes rapides pouvaient réaliser 20 280 essais par seconde, ce qui permettait en moyenne de décrypter en 50 secondes les messages de l'Enigma à 3 rotors et en 20 minutes les messages de l'Enigma M4 (4 rotors).
- Les rotors de la BOMBE tournaient à 1725 tours / minutes

De la mécanique à l'ordinateur Colossus



Geheimschreibers SZ 42

L'initialisation de la machine est réalisé par le positionnement initial des roues dentées (10^{121} possibilités)

- Colossus. Le premier Colossus voit le jour en Décembre 1943 et comprend 1500 tubes à vide. La machine est améliorée en coopération avec les Américains et comprend alors 2500 tubes à vide et l'équivalent de 25 bits de mémoire centrale.
- Il permet la programmation sur la base de ET et de OU. Colossus est ainsi le premier ordinateur avant le célèbre ENIAC

Le rôle de la cryptanalyse dans la seconde guerre mondiale
Les alliés ont gagnés la guerre plus tôt …

La cryptologie a certainement permis de sauver de nombreuses vies humaines. Selon les historiens, la cryptologie a permis d'écourter la guerre d'un an dans le Pacifique et deux ans en Europe

- Grâce aux informations **MAGIC**, les américains ont pu regagner leur supériorité navale sur la flotte japonaise après Pearl Harbor et couper les lignes d'approvisionnement du Japon
- Grâce aux décryptements **d'Enigma**, les Britanniques ont pu repousser les tentatives d'invasion allemande lors de la bataille d'Angleterre
- Grâce aux renseignements **d'ULTRA**, les Britanniques ont pu empêcher l'approvisionnement en carburant des forces de Rommel en coulant, 50 % du tonnage qui leur était destiné
- Grâce encore aux décryptements **d'Enigma**, les Britanniques ont pu desserrer l'étau des sous-marins allemands sur les convois alliés dans l'Atlantique et gagner la Bataille de l'Atlantique
- Enfin, le débarquement et la bataille de Normandie ont été grandement facilités par les informations fournies à Eisenhower concernant les intentions et le potentiel allemand.

De la mécanique à l'ordinateur
La cryptographie moderne

- La cryptographie aujourd'hui se fonde sur les mathématiques, l'électronique et l'informatique.
  - Le savoir faire est désormais sur la place publique
  - Il est facile de concevoir des systèmes de chiffrement très robustes
- On pourrait croire que l'avantage est désormais du coté du cryptologue et que le décrypteur à définitivement perdu la partie
  - Soyons prudent. La sécurité cryptologique ne se démontre pas
  - Le cryptologue n'est pas à l'abri d'une faille dans la mise en œuvre du système de cryptographie ni d'une percée technique inconnue (L'exemple du Colossus)
  - Ainsi des recherches en cours sur la mécanique quantique pourraient révolutionner le monde de l'informatique et les techniques actuelles de décryptage.
  - Le premier embryon d'ordinateur quantique a effectué son premier calcul en factorisant le nombre 15 en Décembre 2001
  - Quelle confiance accorder aux solutions logicielles. Qui peut garantir l'absence de failles volontaires ou involontaires.

Concepts et méthodologies

La cryptographie moderne

- À côté de la fonction de chiffrement, qui permet de préserver le secret des données lors d'une transmission, et qui a été utilisée depuis très longtemps, la cryptologie moderne a développé de nouveaux buts à atteindre et qu'on peut énumérer de manière non exhaustive :
  - **confidentialité**
  - **intégrité des données**
  - **authentification des divers acteurs**
  - **non-répudiation d'un contrat numérique**
  - **signature numérique**
  - **certification**
  - **contrôle d'accès**
  - **gestion des clés**
  - **preuve de connaissance**

Les techniques cryptographiques

- Les techniques cryptographiques de base sont les techniques qui permettent de répondre aux fonctionnalités que nous avons décrites précédemment. On peut citer essentiellement :
  - **Les techniques de chiffrement**
  - **Les techniques de signature**
  - **Les techniques d'authentification**

- Ces techniques font appels à des **primitives cryptographiques** qui elles mêmes sont basées sur des **objets et problèmes mathématiques**.

CLUSIR Rhône Alpes

Les objets et problèmes mathématiques

- La cryptographie à clé secrète fait plutôt usage de :
  - **Fonctions booléennes**
  - **Générateurs de suites pseudo-aléatoires**
  - **Corps finis**
  - **Codes correcteurs d'erreurs**
- La cryptographie à clé publique fait plutôt usage de :
  - **Problème de la factorisation des entiers**
  - **Problème du logarithme discret dans des groupes arithmétiques**
  - **Problèmes liés à la résiduosité quadratique**
  - **Fractions continues, réseaux arithmétiques**
  - **Codes correcteurs d'erreurs**

Algorithmes et Protocoles (1/2)

- Algorithmes de chiffrement faibles (facilement cassables)
  - Les premiers algorithmes utilisés pour le chiffrement d'une information étaient assez rudimentaires dans leur ensemble. Ils consistaient notamment au remplacement de caractères par d'autres. La confidentialité de l'algorithme de chiffrement était donc la pierre angulaire de ce système pour éviter un décryptage rapide. Exemples d'algorithmes de chiffrement faibles :
    - ROT13 (rotation de 13 caractères, sans clé) ;
    - Chiffre de César (décalage de trois lettres dans l'alphabet).
- Algorithmes de cryptographie symétrique (à clé secrète)
  - Les algorithmes de chiffrement symétrique se fondent sur une même clé pour chiffrer et déchiffrer un message. Le problème de cette technique est que la clé, qui doit rester totalement confidentielle, doit être transmise au correspondant de façon sûre. En outre lorsqu'un grand nombre de personnes désirent communiquer ensemble, le nombre de clés augmente de façon importante (une pour chaque couple de communicants). Ceci pose des problèmes de gestions des clés.
    - Chiffre de Vernam
    - DES / 3DES
    - AES
    - RC4 / RC5

Algorithmes et Protocoles (2/2)

- Algorithmes de cryptographie asymétrique (à clé publique et privée)
  - Pour résoudre en partie le problème de la gestion des clés, la cryptographie asymétrique a été mise au point dans les années 1970. Elle se base sur le principe de deux clés :
    - une publique, permettant le chiffrement ;
    - une privée, permettant le déchiffrement.
  - Comme son nom l'indique, la clé publique est mise à la disposition de quiconque désire chiffrer un message. Ce dernier ne pourra être déchiffré qu'avec la clé privé, qui doit être confidentielle.
  - Quelques algorithmes de cryptographie asymétrique très utilisés :
    - RSA ;
    - DSA ;
    - Protocole d'échange de clés Diffie-Hellman ;
- Fonctions de hachage
  - Une fonction de hachage est une fonction qui convertit un grand ensemble en un plus petit ensemble, l'empreinte. Il est impossible de la déchiffrer pour revenir à l'ensemble d'origine, ce n'est donc pas une technique de chiffrement.
  - Quelques fonctions de hachage très utilisées :
    - MD5 ;
    - SHA-1 ;

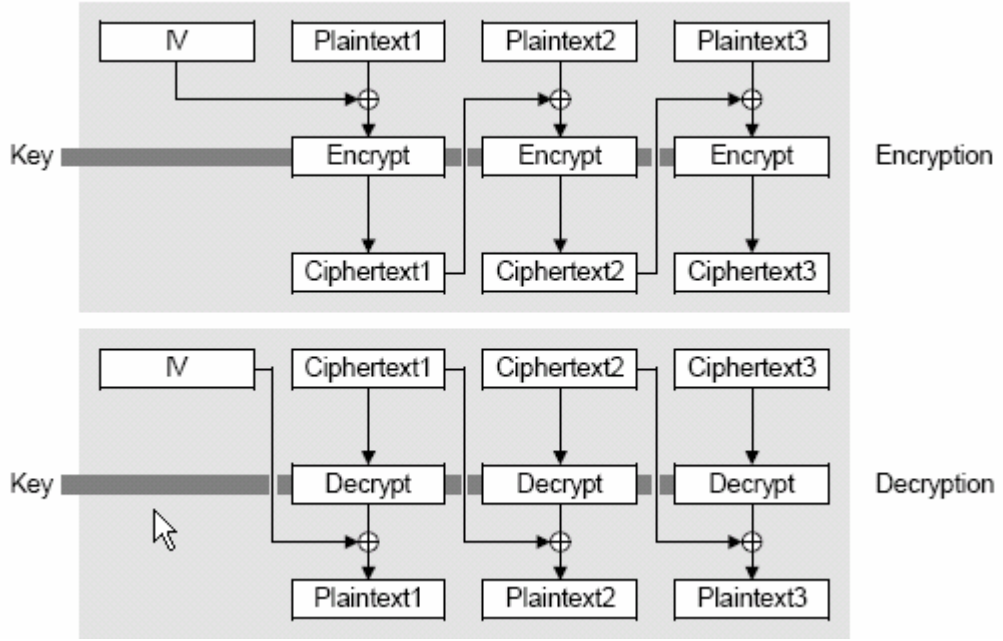
CLUSIR Rhône Alpes

Cryptographie symétrique

- La cryptographie symétrique, également dite à clé secrète est la plus ancienne forme de chiffrement
- L'un des concepts fondamentaux de la cryptographie symétrique est la *clé*, qui est une information devant permettre de chiffrer et de déchiffrer un message et sur laquelle peut reposer toute la sécurité de la communication.
- Jusqu'aux communications numériques, les systèmes utilisaient l'alphabet et combinaient les substitutions — les symboles sont changés mais restent à leur place — et les transpositions — les symboles ne sont pas modifiés mais changent de place. Lorsque la substitution appliquée dépend de la place de la lettre dans le texte, on parle de substitution polyalphabétique.
- Depuis l'avènement du numérique, les paradigmes du chiffrement symétrique ont bien changé. D'une part, la discipline s'est formalisée, même si la conception de système de chiffrement garde inévitablement un aspect artisanal. En effet dans ce domaine, la seule chose que l'on sache prouver est la résistance face à des types d'attaques connues, pour les autres... D'autre part, la forme du texte chiffre ayant changé, les méthodes ont suivi. Les algorithmes modernes chiffrent des suites de bits
- On distingue deux types d'algorithmes, les algorithmes en blocs, qui prennent *n* bits en entrée et en ressortent *n*, et les algorithmes à flots, qui chiffrent bit par bit sur le modèle du chiffre de Vernam

Cryptographie symétrique
Chiffrement par bloc

- Le **chiffrement par bloc** (block cipher) est une des deux grandes catégories de chiffrements modernes en cryptographie symétrique
- Le principe consiste à un découpage des données en blocs de taille généralement fixe (souvent une puissance de deux comprise entre 32 et 512 bits). Les blocs sont ensuite chiffrés les uns après les autres. Il est possible de transformer un chiffrement de bloc en un chiffrement par flot en utilisant un mode d'opération comme ECB (chaque bloc chiffré indépendamment des autres) ou CFB (on chaîne le chiffrement en effectuant un XOR entre les résultats successifs).
- Une liste non-exhaustive :
  - DES, l'ancêtre
  - AES, le remplaçant de DES
  - Blowfish et Twofish, des alternatives à AES



Cryptographie symétrique
Standard de chiffrement avancé (AES)

Fonctionnement

- L'algorithme prend en entrée un bloc de 128 bits (16 octets), la clé fait 128, 192 ou 256 bits. Les 16 octets en entrée sont permutés selon une table définie au préalable. Ces octets sont ensuite placés dans une matrice de 4x4 éléments et ses lignes subissent une rotation vers la droite. L'incrément pour la rotation varie selon le numéro de la ligne. Une transformation linéaire est ensuite appliquée sur la matrice, elle consiste en la multiplication binaire de chaque élément de la matrice avec des polynômes issus d'une matrice auxiliaire, cette multiplication est soumise à des règles spéciales selon GF(28) (groupe de Galois ou corps fini). La transformation linéaire garantit une meilleure diffusion (propagation des bits dans la structure) sur plusieurs tours. Finalement, un XOR entre la matrice et une autre matrice permet d'obtenir une matrice intermédiaire. Ces différentes opérations sont répétées plusieurs fois et définissent un « tour ». Pour une clé de 128, 192 ou 256, AES nécessite respectivement 10, 12 ou 14 tours.

Attaques sur des versions simplifiées

- Des attaques existent sur des versions simplifiées d'AES. En 2000 une attaque sur une version à 7 tours de l'AES 128 bits a été démontrée.
- Une attaque similaire casse un AES de 192 ou 256 bits contenant 8 tours.
- Un AES de 256 bits peut être cassé s'il est réduit à 9 tours avec une contrainte supplémentaire. En effet, cette dernière attaque repose sur le principe des « related-keys » (clés apparentées). Dans une telle attaque, la clé demeure secrète mais l'attaquant peut spécifier des transformations sur la clé et chiffrer des textes à sa guise. Il peut donc légèrement modifier la clé et regarder comment la sortie de l'AES se comporte.

Cryptographie symétrique
Chiffrement de flux

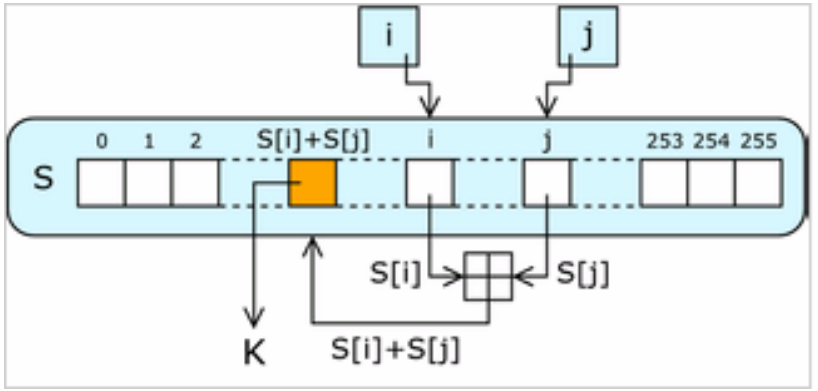
- Le **chiffrement de flux** ou **chiffrement par flot** (stream cipher) est une des deux grandes catégories de chiffrements modernes en cryptographie symétrique. Un chiffrement par flot arrive à traiter les données de longueur quelconque et n'a pas besoin de les découper.
- Une liste non-exhaustive de chiffrements par flot :
  - A5, utilisé dans les téléphones mobiles de type GSM pour chiffrer la communication par radio entre le mobile et l'antenne-relais la plus proche,
  - RC4, le plus répandu, conçu par Ronald Rivest, utilisé notamment par le protocole WEP du WiFi
  - Py, un algorithme récent de Eli Biham
  - E0 utilisé par le protocole Bluetooth
- Un chiffrement par flot se présente souvent sous la forme d'un générateur de nombres pseudo-aléatoires avec lequel on opère un XOR entre un bit à la sortie du générateur et un bit provenant des données. Toutefois, le XOR n'est pas la seule opération possible. L'opération d'addition dans un groupe est également envisageable (par exemple, addition entre deux octets, modulo 256). Un chiffrement par bloc peut être converti en un chiffrement par flot grâce à un mode opératoire qui permet de chaîner plusieurs blocs et traiter des données de taille quelconque.
- **Chiffrement / déchiffrement avec XOR**
  - Soit l'opération booléenne XOR :
  - Chiffrement du message M avec la clé K :
  - Déchiffrement du message C avec la clé K :

Cryptographie symétrique
RC4

- **RC4** est un algorithme de chiffrement à flot conçu en 1987 par Ronald Rivest, l'un des inventeurs du RSA, pour les Laboratoires RSA. Il est supporté par différentes normes, par exemple dans SSL ou encore WEP.

- **Principe**
  - RC4 fonctionne de la façon suivante : la clef RC4 permet d'initialiser un tableau de 256 octets en répétant la clef autant de fois que nécessaire pour remplir le tableau. Par la suite, des opérations très simples sont effectuées : les octets sont déplacés dans le tableau, des additions sont effectuées, etc. Le but est de mélanger autant que possible le tableau. Au final on obtient une suite de bits qui parait tout à fait aléatoire. Par la suite on peut extraire des bits par conséquent pseudo-aléatoires.

- **Crypto systèmes basés sur RC4**
  - WEP
  - WPA



Cryptographie asymétrique

- La **cryptographie asymétrique**, ou *cryptographie à clé publique* est fondée sur l'existence de fonctions à sens unique, c'est-à-dire qu'il est simple d'appliquer cette fonction à un message, mais extrêmement difficile de retrouver ce message à partir du moment où on l'a transformé.
  - F est à sens unique <--> Quelque soit x , y = f(x) est calculable rapidement.
  - X = f-1(y) se calcule en un temps très long
- En réalité, on utilise en cryptographie asymétrique des fonctions à sens unique et à *brèche secrète*. Une telle fonction est difficile à inverser, *à moins de posséder une information particulière*, tenue secrète, nommée *clé privée*.
  - Une fonction est dite trappe ou à brèche secrète si elle est à sens unique sauf pour toute personne connaissant un secret ou une brèche, permettent de calculer un algorithme d'inversion rapide.
  - On appelle exponentiation modulaire de la variable a la fonction ap mod n (p fixe). Si l´existence d'un algorithme permettant de calculer des racines p-ièmes modulo n est démontré, on ne connaît néanmoins pas cet algorithme. Par contre, si on connaît la factorisation de n (la brèche), on peut très facilement inverser l'exponentiation modulaire.
- Une clé est utilisée pour coder le message et une autre pour décoder le message crypté. Dans un système à clé publique , chaque personne dispose de deux clés: une publique et une privée. Les messages chiffrées avec l'une des clés peuvent seulement être déchiffrés par l'autre clé de la paire.

Cryptographie asymétrique
Le protocole de Diffie-Hellman

- La distribution d'une clé secrète est le problème crucial de la cryptographie
  - Ainsi un chiffrement symétrique sûr est fragilisé dans la pratique par le problème de la distribution des clés. La multiplication des contacts nécessaires et la prolifération des réseaux rendent cette problématique de plus en plus coûteuse et hasardeuse

- La solution est apparue en 1976 lorsque W Diffie et M Hellman proposèrent une solution au problème de l'échange des clés secrètes
  - Cette méthode utilise une fonction à sens unique pour tout le monde excepté pour son créateur qui peut l'inverser grâce à la connaissance d'une information particulière
  - Cette fonction se base sur l'arithmétique modulaire. L'idée de base consiste à calculer des valeurs du type $\mathbf{x^a}$ **modulo p**. L'opération inverse est très difficile.
  - Même si l'on connaît les nombres **x**, **p** et $\mathbf{x^a}$ **modulo p** il est impossible en pratique de retrouver le nombre a

- La sécurité de ce protocole est calculatoire
  - Elle se fonde sur l'hypothèse qu'avec une puissance de calcul et un temps limité, un adversaire ne peut inverser la fonction exponentielle modulaire et donc retrouver le secret **a** à partir des éléments échangés.
  - **a** est la clé secrète $\mathbf{x^a}$ **modulo p** est une information publique

Cryptographie asymétrique
L'algorithme RSA

- RSA est le premier système de chiffrement à clé publique
  - Il a été concu en 1977 par **R**ivest, **S**hamir et **A**ldeman du MIT.
  - Rapidement devenu un standard international, la technique RSA a été commercialisée par plus de 400 entreprises et l'on estime que plus de 400 millions de logiciels l'utilisent
- Le système RSA est fondé sur la difficulté de factoriser des grands nombres et la fonction à sens unique utilisée est une fonction puissance
  - Soit p et q deux grands nombres premiers. Il est très difficile de retrouver ces 2 nombres en connaissant leur produit n= p*p
  - Pour le calcul des clés publique et privée, il faut choisir deux grands nombres premiers **p** et **q**. On calcul le produit **n = pq**. On choisi un grand nombre **e** premier avec **(p-1)(q-1).**
  - On calcul ensuite un nombre **d** tel que **ed = 1 mod (p-1)(q-1)**
  - Le couple **(n, e)** est la clé publique, **d** est clé privée
- Le message chiffré s'obtient en calculant
  - **$y = x^e$ modulo n**
- Pour déchiffrer le message il suffit de calculer
  - **$z = y^d$ modulo n** qui vaut **x** puisque $y^d = x^{ed} = x$ modulo n

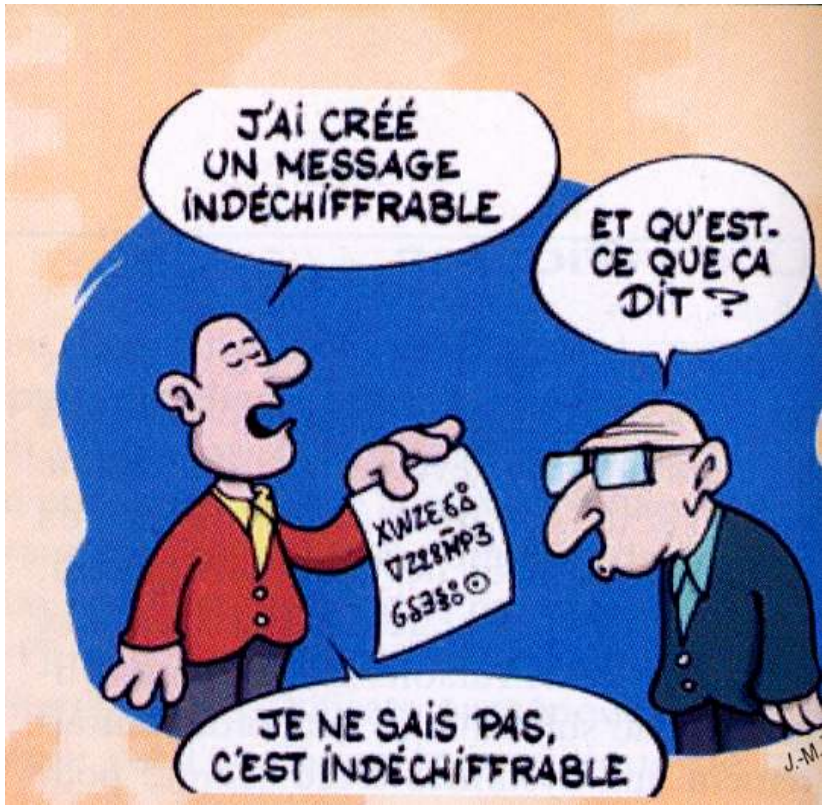
Fonction de hachage

- Une fonction de hash (anglicisme) ou fonction de hachage est une fonction qui associe à un grand ensemble de données un ensemble beaucoup plus petit (de l'ordre de quelques centaines de bits) qui est caractéristique de l'ensemble de départ
- Le résultat de cette fonction est par ailleurs aussi appelé **somme de contrôle**, **empreinte**, **résumé de message**, **condensé** ou encore **empreinte *cryptographique*** lorsque l'on utilise une fonction de hachage *cryptographique*
- Une fonction de hachage cryptographique est utilisée entre autres pour la signature électronique, et rend également possibles des mécanismes d'authentification par mot de passe sans stockage de ce dernier. Elle doit être résistante aux collisions, c'est-à-dire que deux messages distincts doivent avoir très peu de chances de produire la même signature. De par sa nature, tout algorithme de hachage possède des collisions mais on considère le hachage comme cryptographique si les conditions suivantes sont remplies :
  - il est très difficile de trouver le contenu du message à partir de la signature (attaque sur la première pré image)
  - à partir d'un message donné et de sa signature, il est très difficile de générer un autre message qui donne la même signature (attaque sur la seconde pré image)
  - il est très difficile de trouver deux messages aléatoires qui donnent la même signature (résistance aux collisions)
- Liste non exhaustive :
  - SHA-1 / SHA-256 / SHA-512
  - MD5

Fonction de hachage MD5

- MD5 (Message Digest 5) est une fonction de hachage cryptographique qui permet d'obtenir pour chaque message une empreinte numérique (en l'occurrence une séquence de 128 bits ou 32 caractères en notation hexadécimale) avec une probabilité très forte que, pour deux messages différents, leurs empreintes soient différentes.
- MD5 travaille avec un message de taille variable et produit une empreinte de 128 bits. Le message est divisé en blocs de 512 bits, on applique un remplissage de manière à avoir un message dont la longueur est un multiple de 512. Le remplissage se présente comme suit :
  - on ajoute un '1' à la fin du message
  - on ajoute une séquence de '0' (le nombre de zéros dépend de la longueur du remplissage nécessaire)
  - on écrit la taille du message, un entier codé sur 64 bits
  - Ce remplissage est toujours appliqué, même si la longueur du message peut être divisée par 512. Cette méthode de padding est semblable à celle utilisée dans la plupart des algorithmes de Message Digest des familles MD

Applications de la cryptographie



Serge RICHARD - CISSP®

Applications avec une cryptographie symétrique

- Chiffrement de données

Applications avec une cryptographie asymétrique

- Transmission sécurisée pour une cryptographie symétrique
- Mécanismes d'authentification
- Certificats numériques
- Infrastructure à clé publique (IGC)
- Signatures numériques

Applications avec une cryptographie de hachage

- Une fonction de hachage cryptographique est utilisée entre autres pour la signature électronique.
- Une fonction de hachage rend également possibles des mécanismes d'authentification par mot de passe sans stockage de ce dernier.
- Intégrité des données

CLUSIR Rhône Alpes

Cryptographie et la longueur des clés

Algorithm security lifetimes	Symmetric key algorithms (Encryption & MAC)	FFC (e.g., DSA, D-H)	IFC (e.g., RSA)	ECC (e.g., ECDSA)
Through 2010 (min. of 80 bits of strength)	2TDEA[23] 3TDEA AES-128 AES-192 AES-256	Min.: $L = 1024$; $N = 160$	Min.: $k=1024$	Min.: $f=160$
Through 2030 (min. of 112 bits of strength)	3TDEA AES-128 AES-192 AES-256	Min.: $L = 2048$ $N = 224$	Min.: $k=2048$	Min.: $f=224$
Beyond 2030 (min. of 128 bits of strength)	AES-128 AES-192 AES-256	Min.: $L = 3072$ $N = 256$	Min.: $k=3072$	Min.: $f=256$

Attaques sur la cryptographie

Cryptographie et Cryptanalyse

- L'analyse cryptographique ou Cryptanalyse a pour objet de percer l'écran logique derrière lequel sont cachés les informations chiffrées
  - Le chiffrement place l'information dans un coffre fort virtuel dont les personnes non autorisée ignorent la combinaison
  - Ceux qui souhaitent accéder aux informations tentent de forcer le coffre

    soit en recherchant la combinaison,

    soit en essayant de découvrir une faiblesse insoupçonnée du coffre ou de la serrure

    Et ce idéalement sans laisser de trace
- La cryptologie est donc un jeu à deux joueurs
  - Le cryptologue-concepteur conçoit des moyens de chiffrement offrant la meilleur protection possible
  - Le cryptologue-décrypteur utilise tous les moyens imaginables pour percer à jour les messages chiffrés interceptés.
- La question est de savoir si il existe un système de chiffrement théoriquement indécryptable
  - Il en existe un dont le mathématicien Claude Shannon à démontré l'herméticité absolue. C'est le système dit « ***A clé une fois aléatoire*** » utilisé pour les communications au plus haut niveau entre chefs d'états (Téléphone Rouge)

CLUSIR Rhône Alpes

Classification des attaques

- Une attaque est souvent caractérisée par les données qu'elle nécessite :
  - attaque sur texte chiffré seul (*ciphertext-only*) : le cryptanalyste possède des exemplaires chiffrés des messages, il peut faire des hypothèses sur les messages originaux qu'il ne possède pas. La cryptanalyse est plus ardue de par le manque d'informations à disposition.
  - attaque à texte clair connu (*known-plaintext attack*) : le cryptanalyste possède des messages ou des parties de messages en clair ainsi que les versions chiffrées. La cryptanalyse linéaire fait partie de cette catégorie.
  - attaque à texte clair choisi (*chosen-plaintext attack*) : le cryptanalyste possède des messages en clair, il peut générer les versions chiffrées de ces messages avec l'algorithme que l'on peut dès lors considérer comme une boîte noire. La cryptanalyse différentielle est un exemple d'attaque à texte clair choisi.
  - attaque à texte chiffré choisi (*chosen-ciphertext attack*) : le cryptanalyste possède des messages chiffrés et demande la version en clair de certains de ces messages pour mener l'attaque.

Familles d'attaques cryptanalytiques

- Il existe plusieurs familles d'attaques cryptanalytiques, les plus connues étant l'analyse fréquentielle, la cryptanalyse différentielle et la cryptanalyse linéaire.
  - L'analyse fréquentielle : L'analyse fréquentielle examine les répétitions des lettres du message chiffré afin de trouver la clé. Elle est inefficace contre les chiffrements modernes tels que DES, RSA. Elle est principalement utilisée contre les chiffrements mono-alphabétiques qui substituent chaque lettre par une autre et qui présentent un biais statistique.
  - L'indice de coïncidence : L'indice de coïncidence permet de calculer la probabilité de répétitions des lettres du message chiffré. Il est souvent couplé avec l'analyse fréquentielle. Cela permet de savoir le type de chiffrement d'un message (chiffrement mono-alphabétique ou poly-alphabétique) ainsi que la longueur probable de la clé.
  - L'attaque par mot probable : L'attaque par mot probable consiste à supposer l'existence d'un mot probable dans le message chiffré. Il est donc possible d'en déduire la clé du message si le mot choisi est correct. Ce type d'attaque a été menée contre la machine Enigma durant la Seconde Guerre mondiale.
  - L'attaque par dictionnaire : L'attaque par dictionnaire consiste à tester tous les mots d'une liste comme mot clé. Elle est souvent couplée à l'attaque par force brute.
  - L'attaque par force brute : L'attaque par force brute consiste à tester toutes les solutions possibles de mots de passe ou de clés. C'est le seul moyen de récupérer la clé dans les algorithmes les plus modernes et encore inviolés comme AES.
  - Attaque par paradoxe des anniversaires : Le paradoxe des anniversaires est un résultat probabiliste qui est utilisé dans les attaques contre les fonctions de hachage. Ce paradoxe permet de donner une borne supérieure de résistance aux collisions d'une telle fonction. Cette limite est de l'ordre de la racine de la taille de la sortie, ce qui signifie que, pour un algorithme comme MD5 (empreinte sur 128 bits), trouver une collision quelconque avec 50% de chance nécessite 264 hachages d'entrées distinctes.

Les stratégies d'attaque
Les attaques des cryptanalystes

- Aujourd'hui deux techniques standards de cryptanalyse contre les schémas cryptographiques à clé secrète
  - La cryptanalyse linéaire inventée par le japonais Mitsuru Matsui

    L'idée est de trouver des approximations linéaires entre les bits de sortie, les bits d'entrée et les bits de la clé

    Si certaines de ces approximations apparaissent avec une probabilité suffisante, on a alors démontré que la correspondance entre entrée et sortie n'est pas purement aléatoire

    Le nombre de clés a envisager pour déchiffrer le message est restreint
  - La cryptanalyse différentielle découverte par deux cryptologies israéliens: Bihan et Shamir

    Elle consiste à comparer les sorties de l'algorithme quand on lui met en entrée deux messages ayant une différence fixe.

    On étudie comme varient les sorties si les deux messages ne diffèrent que par un seul bit

    Si en déplaçant ce bit à l'intérieur des messages, certains bits des sorties restent inchangés, on a alors trouvé une faille dans l'algorithme et celui-ci est attaquable
- Ces deux méthodes permettent de casser très rapidement la plupart des schémas proposés par des non spécialistes

Peut-on casser les clés

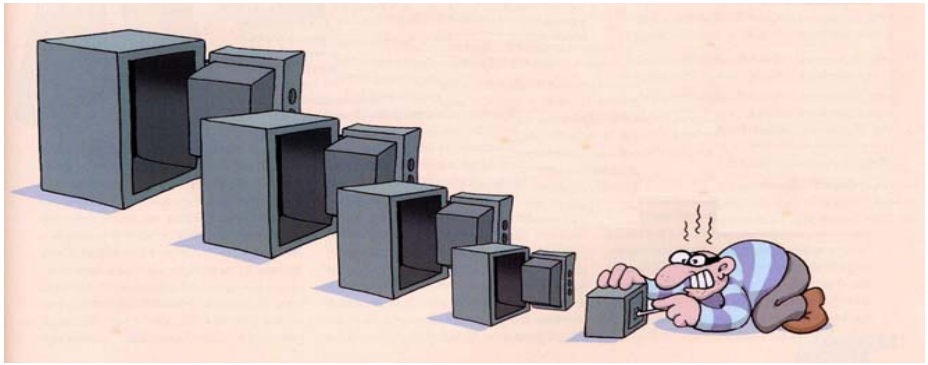
- Les clés cryptographiques sont à la base des systèmes de chiffrement. Leur longueur et la manière dont elles sont crées assurent la sécurité des systèmes cryptographiques bien conçus.

- Un exemple marquant:
  - Durant l'été 1998, Serge Humpich révélait qu'il avait cassé la clé secrète de 320 bits assurant la sécurité des transactions effectuées avec une carte à puce bancaire
  - Début 2000, la publication sur Internet de la clé cassée faisait la une des journaux

- IL existe deux types de clé
  - Les clés utilisées dans les algorithmes de chiffrement symétriques (128 bits en général)
  - Les clés utilisées dans les algorithmes de chiffrements asymétrique (512, 1024, 2048 bits)

Peut-on casser les clés
La clé est la clé

- Le principe de Kerckhoffs
  - La sécurité d'un système de chiffrement n'est pas fondée sur le secret de la procédure mais uniquement sur un paramètre utilisé lors de sa mise en œuvre: **La clé**
- La clé est donc la pierre angulaire d'un système de chiffrement
- La recherche exhaustive d'une clé de chiffrement revient à chercher un grain de sable sur une plage
  - Une plage de quelques Km de long qui contient 10^{16} grains de sable correspond à eu près à l'espace des clés de 56 bits.
  - Toutefois, la recherche exhaustive par des pirates peut être considérablement facilité, si l'on réduit l'espace des clés, par exemple en délimitant la zone de recherche sur la plage



CLUSIR Rhône Alpes

Peut-on casser les clés
Des trappes dans les clés

- Une trappe, est un procédé délibéré qui diminue la sécurité d'un système cryptographique.
  - Une clé avec une trappe est dangereuse, car elle paraît incassable, alors qu'en réalité ses concepteurs savent comment la casser rapidement.
- Exemple
  - L'attaque ADK (Additional Decryption Key) contre le logiciel PGP qui autorisait un attaquant à accoler sa propre clé publique à une autre, lui permettant de déchiffré tous les messages destinés au titulaire de la clé attaquée.
  - Cette faille a été corrigée en 2000, après sa révélation
- Fabriquer une clé d'un système symétrique revient à choisir de manière aléatoire chacun des bits qui la compose
  - Dans la pratique on a recourt à un générateur informatique de bits aléatoires
  - Hors un générateur informatique ne peut engendrer un hasard total.
  - Si le générateur n'est pas aléatoire mais génère certains type de séquence avec une plus forte probabilité, alors la clé générée comporte des faiblesses

Peut-on casser les clés
Des trappes dans les clés des systèmes symétriques

- On peut réduire l'entropie d'un générateur de clé symétriques
  - Avec un générateur produisant beaucoup plus souvent des 1 que des 0. Un attaquant pourra envisager une recherche exhaustive en privilégiant les clés comportant le plus de 1
  - Une autre technique consiste à fixer arbitrairement la valeur d'un certains nombres de bit de la clé.
  - On peut générer des clés en utilisant une combinaison linéaire de clés connues. Il reste alors à trouver les coefficients utilisés.

Peut-on casser les clés
Des trappes dans les clés des systèmes asymétriques

- L'introduction de trappes dans les clés des systèmes asymétriques semble plus difficile puisque ce type de clé possède déjà une structure mathématique
  - La génération de telles clé s'effectue sur la base de 2 grands nombres premiers.
  - Le hasard est ici dans le choix des grands nombres premiers utilisés
  - SI le générateur aléatoire qui engendre ces nombres est biaisé, ce biais facilitera la recherche des nombres premiers ayant servi à l'élaboration de la clé
- Exemple d'attaque du système RSA
  - On peut choisir un petit nombre et un grand nombre premier. Ainsi leur produit est plus facilement factorisable.
  - En 1990, Michael Wiener met en évidence l'existence de paires de clés publiques/privée RSA « faibles ». Une paire de clé RSA est faible lorsque la seule connaissance de la partie publique permet de retrouver la partie privée en un temps raisonnable (polynomial)
  - Si la partie privée d'une clé RSA a un nombre de chiffre 4 fois inférieur à celui de la partie publique de la clé, il existe une méthode rapide de calcul de la partie privée
  - Il existe actuellement des générateurs à trappes utilisant le principe de Wiener produisant des ***clés apparemment anodines*** mais qui sont ***en réalité faibles***

Les stratégies d'attaque du système RSA
Le problème mathématique

- La génération des clés RSA s'appuie sur l'utilisation d'un grand nombre n produit de deux grands nombres premiers p et q : 'n=pq' et 'e' premier avec (p-1)(q-1)
  - **(n, e)** forment la clé publique, et **d** l'inverse de e modulo (p-1)(q-1), la clé privée
  - La première façon d'attaquer l'algorithme RSA est de factoriser n et de retrouver p et q
  - En 1999, un nombre de 512 bits a été factorisé avec une puissance de calcul de 10^4 Mips/an (Soit 10^{10} instructions/s pendant un an)
  - En prenant la loi de Moore comme référence (La puissance double tous les 18 mois) on peut estimer que les clés de 1024 bits pourront être cassées vers l'an 2010 et que les clés de 2048 bits pourront l'être vers 2030
- D'autres attaques sont possibles a condition de faire des hypothèses sur l'exposant secret 'd' inverse de e modulo (p-1)(q-1)
  - Il est facilement possible de retrouver d à partir de n et e par l'attaque de Wiener lorsque d est inférieur à $n^{1/4}$
  - D'autres attaques sont possibles si l'on suppose que certains bits de la clé d sont connus

    Si d a une taille de k bits, la connaissance les k/4 bits de poids faibles (les moins significatifs) est suffisant de reconstituer complètement la clé

Les stratégies d'attaque du système RSA
Les attaques de protocole

- Même si RSA est solide, la façon dont on l'utilise n'est pas neutre. Exemple
  - Si on envoie le même message à 3 personnes différentes, chiffrés avec 3 clés RSA de ces personnes, on peut facilement retrouver les message en clair à partir des 3 messages chiffrés en utilisant la propriété de multiplicativité de la fonction RSA:

    $f(X*y) = f(x) * f(y)$
  - Il est également risqué de chiffrer plusieurs messages liés au moyen de la même clé publique RSA

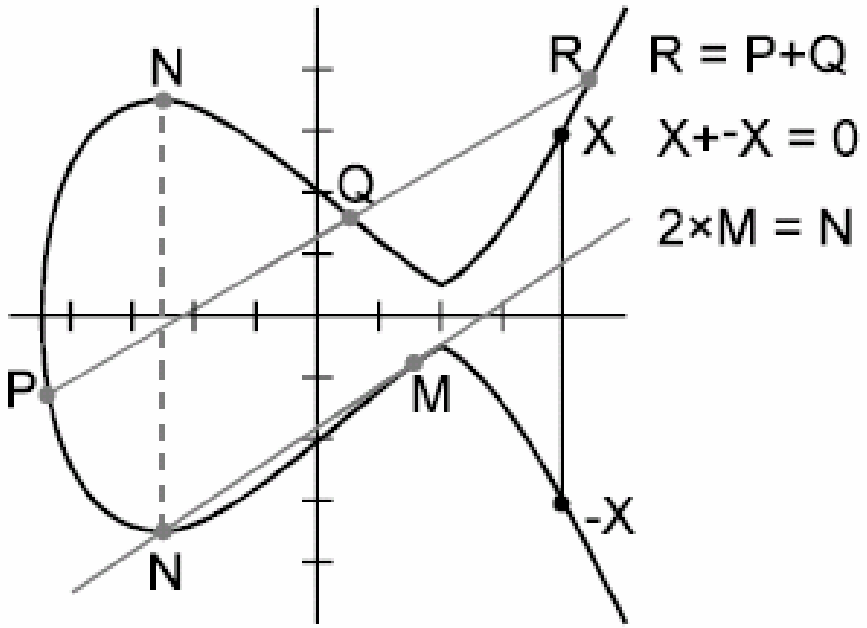
Les stratégies d'attaque du système RSA
Les attaques physiques

- Il s'agit dans ce cas d'attaques se basant sur des propriétés physiques de l'appareil en charge de l'implémentation du protocole RSA
  - Attaques sur le temps de calcul
  - Attaques sur la consommation électrique
  - Attaques par injection de fautes
  - Toutes ces attaques physique concernent essentiellement les cartes à puce pour lesquelles, avec un dispositif adéquat, il est facile d'obtenir des données
- Attaques sur le temps de calcul
  - L'algorithme de calcul de la fonction RSA est toujours le même.
  - En particulier il fait intervenir une boucle pour le calcul de $\mathbf{y^d \bmod n}$ (ou d est la clé secrète). $d=d_1d_2d_3\ldots d_n$. Chaque bit di est égal à 0 ou 1. Or dans la boucle de calcul, on trouve une instruction du type 'si $d_i = 1$ alors faire tel calcul sinon ne pas le faire'
  - En mesurant les temps de calcul pour de nombreuses valeurs initiales de y (message crypté), on peut déduire si le calcul qui est fait lorsque $d_i = 1$ a été réellement effectué et de la retrouver la clé secrète d bit par bit.
  - On peut contourner ce type d'attaque en masquant les différences de temps de calcul

Les stratégies d'attaque du système RSA
Les attaques physiques

- Attaque sur la consommation électrique
  - Le même type d'attaque peut-être effectué avec la consommation électrique
  - Pour chacun des calculs, on mesure la courbe de consommation électrique du composant qui fait le calcul.
  - En analysant la statistique de la consommation électrique à chaque étape du calcul, on déduit de proche en proche la valeur de la clé secrète d.
  - Des méthodes existent pour fausser le consommation électrique et rendre cette information inutilisable
- Attaques par injection de fautes
  - Cette attaque a été conçue en 1996 et présentée comme un nouveau modèle d'attaque physique sur les cartes à puce : »Cryptanalyse en présence d'erreurs de calcul dans les processeurs »
  - Elle se base sur l'utilisation d'une signature RSA erronée puis de la signature correcte
- Les nombreuses attaques présentées montrent que
  - L'utilisation de RSA réclame un soin particulier, que ce soit dans le choix de la taille des paramètres, dans celui du protocole de chiffrement ou de signature, ou même dans la manière dont le calcul est programmé.

Focus sur les courbes elliptiques



Complexité

- Temps de calcul :
  - 1 : Temps constant
  - N : Linéaire
  - N^x: polynomial
  - x^N : exponentiel
- Exemple :
  - Recherche dans une liste : N ➔ linéaire
  - Tri à bulle : N^2 ➔ polynomial
  - Quick sort : N log(N)
  - Calcul AES : 1 (quasi constant quelle que soit la taille de la clé)
  - Attaque en force brute sur l'AES : x^N ➔ exponentiel
  - Calcul RSA : N^2 ➔ polynomial
  - Attaque en force brute sur le RSA : x^N ➔ exponentiel

CLUSIR Rhône Alpes

Pour la cryptographie…

- Le saint Graal :
  - Constant pour l'utilisation
  - Exponentiel pour l'attaquant
- Jamais vrai en théorie car :
  - Les utilisations ne sont jamais constantes
  - Des attaques intelligentes font que ce n'est pas purement exponentiel
- En algorithmes symétriques, le Saint-Graal n'est jamais très loin
- En algorithmes asymétriques, le Saint-Graal est loin.

Petit théorème de Fermat

$$a^m \equiv a \Leftrightarrow a^{m-1} \equiv 1$$

- Si :
  - m est premier
  - a n'est pas multiple de m
- Exemple :
  - 20^{13} mod 13 = 13
  - Car 20^{13}= 8192000000000000
  - Et 8192000000000000 mod 13 = 7 (=20-13)

Problème de la factorisation

$$m = np$$

- Il n'existe pas de méthode rapide (i.e. polynomiale) pour factoriser le produit de deux nombres premiers.
- ➔ Impossible de retrouver n et p connaissant m

Algorithme RSA

$$m = pq$$

$$e.d \equiv 1 \bmod (p-1)(q-1) \Rightarrow d = e^{-1} \bmod ((p-1)(q-1))$$

$$c = x^e \bmod m$$

$$x = c^d \bmod m$$

- Avec :
  - p et q sont deux nombres premiers
  - m est le modulo
  - e est l'exposant public (généralement 2^x+1)
  - d est l'exposant privé
  - x est la donnée en clair
  - c est la donnée chiffrée

Problème des logarithmes discrets

$$a^x = b \Rightarrow x = \frac{\log b}{\log a}$$

- Il n'existe pas de méthode rapide (i.e. polynomiale) pour calculer des logarithmes sur des entiers
- Il est impossible de retrouver x connaissant a et b
- NB : si a=1, l'implication est fausse

Algorithme Diffie-Hellman

$$X = g^{x} \bmod n \qquad Y = g^{y} \bmod n$$

$$k = Y^{x} \bmod n \qquad k' = X^{y} \bmod n$$

$$k = k' = g^{xy} \bmod n$$

- Avec :
  - g et n sont des données publiques
  - x et y sont les données privées
  - k est la clé échangée
- Permet l'échange de clés

Courbes elliptiques

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_5$$

- Equation d'une courbe elliptique sous la forme de Weierstrass
- Ne pas confondre avec des ellipses.
- a et b permettent de définir la courbe elliptique

Courbes elliptiques classiques

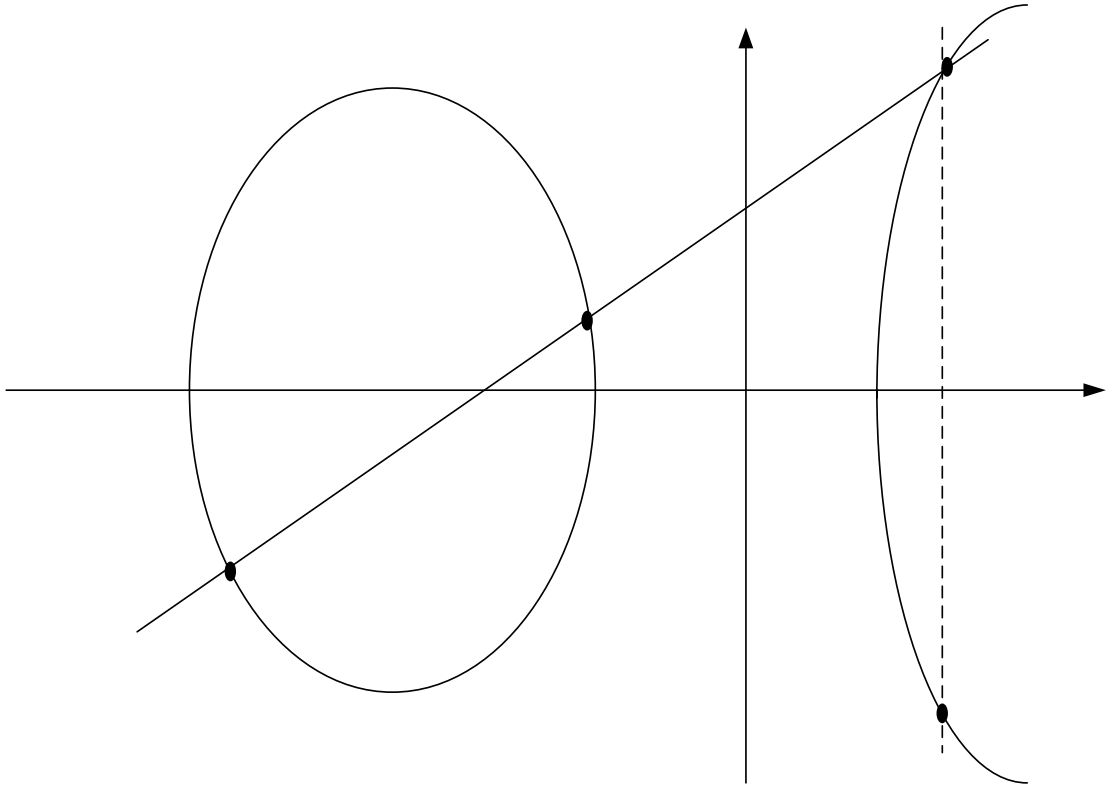
$$y^2 = x^3 + ax + b$$

$$4a^3 + 27b^2 \neq 0$$

- Utilisation de nombres réels dans un plan

Addition de points

$$L = J + K$$



Addition de points

$$x_l = s^2 - x_j - x_k$$

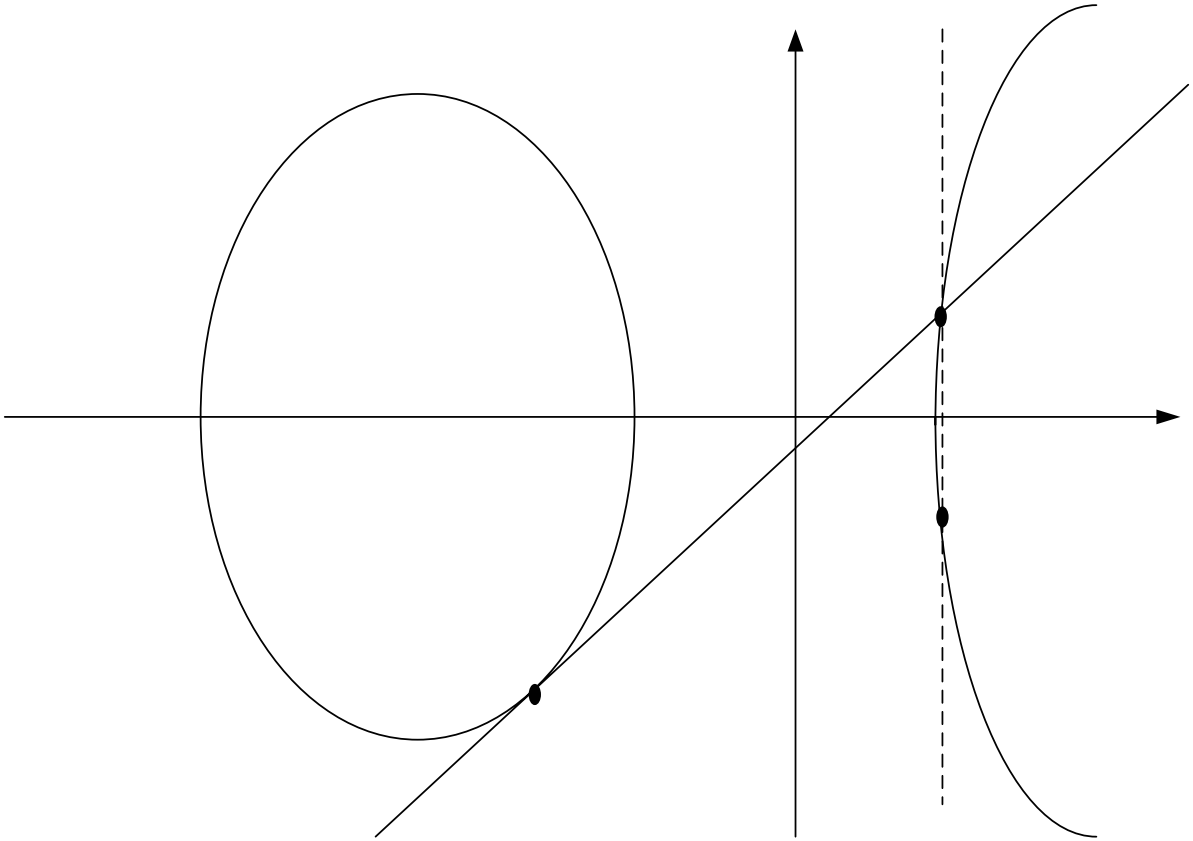
$$y_l = s(x_j - x_l) - y_j$$

$$s = \frac{y_j - y_k}{x_j - x_k}$$

- Cas particuliers :
  - K=-J ➔ L=0 (point à l'infini)
  - K=J ➔ L=2J=2K (doublement du point)
- L'opération est commutative (J+K=K+J)

Doublement d'un point

$$L = 2J$$



Doublement d'un point

$$x_l = s^2 - 2x_j$$

$$y_l = s(x_j - x_l) - y_j$$

$$s = \frac{3x_j^2 + a}{2y_j}$$

- Cas particulier:
  - $y_J = 0$ ➔ $2J = 0$ (point à l'infini)

Multiplication d'un point

$$P(x_p, y_p), Q(x_q, y_q)$$

$$Q = kP$$

- k est un entier.
- La multiplication est une suite d'addition et de doublements
- Exemple :
  - 23 = 10111 en binaire
  - Q = 23P ⇔ Q = 16P+4P+2P+P ➔ Q=2(2(2(2P)+P)+P+P

Mise en œuvre

- Les principes ont été édictés en utilisant des nombres réels :
  - Arrondis de calcul
  - Nombres avec des décimales nombreuses (voire infinies)
- Les courbes elliptiques peuvent s'appliquer à d'autres types de « nombres » (corps de Gallois)
- En pratique :
  - Modulo un nombre premier
  - Polynômes binaires
  - Bases normales

Calculs modulaires

$$y^2 \bmod p = (x^3 + ax + b) \bmod p$$

$$(4a^3 + 27b^2) \bmod p \neq 0$$

- Tous les calculs se font modulo un nombre premier (p)
- L'aspect géométrique précédent est caduque mais les équations restent valables
- x et y forment un nuage de points

Polynômes binaires

$$y^2 + xy = x^3 + ax + b \qquad b \neq 0$$

$$p = \sum_{i=0}^{n-1} c_i x^i \qquad c_i = 0 \text{ ou } 1$$

- Les valeurs sont en fait les coefficients de polynômes binaires (toujours 0 ou 1)
- L'implémentation est simple (shift et XOR)
- Les calculs se font modulo un polynôme irréductible (qui n'est pas le produit de deux polynômes)

Bases normales

$$y^2 + xy = x^3 + ax + b \quad avec \quad b \neq 0$$

$$e = \sum_{i=0}^{m-1} e_i \beta^{2^i} \quad avec \quad \beta = \sum_{i=0}^{n} a_i x^i$$

- Très mathématique
- Implémentation performante (xor, and, shift)
- Calcul modulo une valeur « première »

Utilisation en cryptographie

- Les courbes elliptiques sont une nouvelle méthode d'utilisation d'algorithmes existants :
  - DH ➔ ECDH
  - RSA ➔ ECRSA
  - DSA ➔ ECDSA
  - ...

Logarithmes discrets

$$y^2 = x^3 + ax + b$$

- a et b définissent la courbe elliptique
- Un point générateur $G(x_g,y_g)$ est choisi sur la courbe
- La clé publique est un point de la courbe $P(x_p,y_p)$
- La clé privée k est un nombre aléatoire
- La clé publique est obtenue en multipliant le point G par la clé privée : P = kG
- Il est impossible de retrouver k connaissant P et G (problème de logarithmes discrets)

$$X = xG \qquad Y = yG$$

$$K = xY \qquad K' = yX$$

$$K = K' = xyG$$

- Le point K ne peut être déduite de l'interception de X et Y
- La valeur de la clé est classiquement x_k

$$m = pq$$

$$e.d \equiv 1 \bmod((p+1)(q+1)) \Rightarrow d = e^{-1} \bmod((p+1)(q+1))$$

$$c = e.x$$

$$x = d.c$$

- p et q sont deux nombres premiers.
- x est un point sur la courbe qui correspond à l'information protégée.
- e est une information publique.
- d est une information privée.

Comparaison des tailles de clés

Algorithme symétrique	RSA ou DH	ECRSA ou ECDH
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	521

Source : NIST

NSA Suite B

- La suite B correspond aux algorithmes standards pour un usage général :
  - Chiffrement symétrique : AES 128 et 256
  - Empreinte: SHA-256 et 384
  - Echange de clés :

    ECMQV (Menezes-Qu-Vanstone) basé sur DH

    ECDH (Diffie-Hellman)
  - Signature : ECDSA
- La Suite A correspond aux algorithmes non publiés pour systèmes très sensibles.

CLUSIR Rhône Alpes

Méthode et solution informatique

- Société de service et éditeur de logiciels spécialisé dans la sécurité logique et les réseaux
- Produits : Gamme Security BOX®
- Actionnaire : ARKOON (100%)

- Adresse : 3 place Renaudel
  69003 LYON
  Tél : 04 78 14 04 10 Fax : 04 78 14 04 11
  Web : http://www.securitybox.net

- Philippe PERRET
  Directeur technique
  philippe.perret@msi-sa.fr

Références

- Portail de la cryptologie :
  - http://fr.wikipedia.org/wiki/Wikip%C3%A9dia:Portail_Cryptologie