

Présentation

- Pascal PETIT
- 01 60 87 39 03 (peu joignable)
- petit@shayol.org (trop joignable)
- <http://www.ibisc.fr/~petit>
- Crypto: bibi
- Compression: N. Thibault

Chiffrement

- Auteur : P. Petit (pascal.petit@shayol.org)
- La bibliographie cite des sources/ressources utiles de deux catégories:
 - Des sources dont je me suis inspiré pour certains points (notamment support de cours de C. Laforest qui a assuré cet enseignement jusqu'en 2007-2008)
 - Des sources pour des approfondissements
- Les schémas/photos qui ne sont pas de moi ont en général été récupérés sur wikipedia

Définitions

- Texte en clair : un texte sous sa forme originale, compréhensible tel quel
- Chiffrement : transformer un texte en clair en un texte incompréhensible
- La transformation inverse quand on possède tous les éléments pour le faire s'appelle le déchiffrement (ne pas confondre avec décryptage)
- Décrypter un texte: faire de même sans avoir les éléments (clef, ...). Le correspondant légitime déchiffre le texte, l'attaquant le décrypte.

Définitions

- cryptographie : domaine scientifique et technique dont le but est de garder les messages secrets. Pratiquée par les cryptographes
- cryptanalyse : domaine scientifique et technique dont le but est de retrouver les messages en clair sans avoir tous les éléments pour le faire. Pratiquée par les cryptanalystes
- cryptologie : regroupe cryptographie et cryptanalyse. Pratiquée par les cryptologues.
- Stéganographie: domaine scientifique et technique dont le but est de faire passer inaperçu un message dans un autre objet

Stéganographie : exemple (G. Sand à A. De Musset)

Je suis tres emue de vous dire que j'ai bien compris l'autre soir que vous aviez toujours une envie folle de me faire danser. Je garde le souvenir de votre baiser et je voudrais bien que ce soit la une preuve que je puisse etre aimée par vous. Je suis prete a montrer mon affection toute desinteressee et sans calcul, et si vous voulez me voir aussi vous devoiler sans artifice mon ame toute nue, venez me faire une visite. Nous causerons en amis, franchement. Je vous prouverai que je suis la femme

sincere, capable de vous offrir l'affection la plus profonde comme la plus étroite en amitie, en un mot la meilleure preuve que vous puissiez rever, puisque votre ame est libre. Pensez que la solitude ou j'habite est bien longue, bien dure et souvent difficile. Ainsi, en y songeant j'ai l'ame grosse. Accourez donc vite et venez me la faire oublier par l'amour ou je veux me mettre.

Définitions

- Soit M un message en clair à faire transiter de façon sûre entre Alfred et Bachir
- Soit E le processus de chiffrement
- Soit D le processus de déchiffrement
- Alfred calcule et transmet $C=E(M)$
- Bachir reçoit C et doit connaître D pour retrouver $M=D(C)$
- On doit avoir $M=D(E(M))$

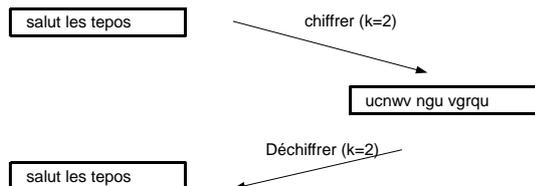
Historique

- L'artisanat
 - Chiffrement de César
 - Permutation et attaque statistique
- La technique
 - ENIGMA
- Masque jetable
- L'ère scientifique (actuelle)
- Principes actuels

Chiffrement de César

$k=2$

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
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



Chiffrement de César

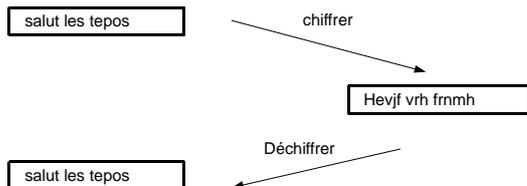
- Décaler chaque lettre de K caractères dans l'alphabet
- Exemple1: $k=2$ « salut les tepos » devient « ucnvw ngu vgrqu »
- Le déchiffrement se fait en décalant les lettres dans l'autre sens
- Exemple2: rot13: l'opération de codage et de décodage sont les mêmes (but: qu'un texte ne soit lu que par les gens qui souhaitent le lire. Utilisé couramment sur les forums USENET)

Chiffrement de César

- Une fois le mécanisme est connu, la sécurité repose sur la connaissance de k
- 25 valeurs possibles pour k . Il suffit de les essayer toutes jusqu'à trouver un texte qui a un sens
- Attaque en force brute: on essaie tout ou partie des clefs
- Ici :
 - l'espace des clefs est trop petit (25 valeurs possibles)
 - Les textes résultats sont reconnaissables

Permutation alphabétique

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
e	t	c	g	r	u	i	o	q	a	x	v	w	s	m	n	b	d	h	f	j	k	l	y	z	p



Permutation alphabétique

- On utilise une permutation quelconque de l'alphabet
- Avec un alphabet de n caractères, $n!$ permutations possibles
- L'espace des clefs devient très grand ($26! \sim 2^{88}$). L'attaque par force brute devient trop longue

Permutation alphabétique

- Problème: chaque lettre est toujours remplacée par la même lettre. Si on a réussi à la décoder une fois, on saura la décoder partout
- 3 attaques complémentaires possibles :
 - Parfois, de notre connaissance de la structure du message, on peut en déchiffrer certaines parties
 - On peut déchiffrer les lettres correspondantes partout dans le message
 - Attaque statistique: connaissant la langue dans laquelle le message a été écrit, on peut s'appuyer sur des statistiques d'occurrences des caractères dans cette langue

Permutation alphabétique: exemple

- Sur la page WeB de ressources du cours, on vous propose un fichier chiffré à l'aide d'une permutation alphabétique
- Voir <http://www.ibisc.fr/~petit>
- Déchiffrez le (à faire pour la prochaine séance)

Chiffrement de vigenère: substitution polyalphabétique

- Au XVIe siècle, Alberti eu l'idée de combiner plusieurs alphabets chiffrés mais sans aboutir à un système complet viable
- Son idée avait l'avantage de casser les attaques statistique puisqu'une même lettre peut être codée de plusieurs façon différente
- Jean Tritheme, un abbé allemand, Giovanni Porta, un savant italien continuèrent son travail
- Blaise de Vigenère, un diplomate français, s'appuya sur leur travail pour proposer un système de chiffrement révolutionnaire qui portera son nom.

Chiffrement de vigenère: substitution polyalphabétique

- Principe: chaque lettre du message est chiffré à l'aide d'un chiffrement de César avec un décalage différent;
- Pour simplifier la transmission des tables, on indique la version chiffrée de A (et on en déduit le décalage et donc les versions chiffrées des autres lettres);
- La clef est un texte indiquant la suite des versions chiffrées de la lettre A
- Un fois arrivé au bout de la clef, on repart au début

Vigenère: exemple

- Clef: tepos
- Texte à chiffrer: « ilfaitfaim »
- La lettre « i » est chiffrée avec la transformation de César transformant « a » en « t », « l » avec celle transformant « a » en « e »

ilfaitfaim (texte à chiffrer)

tepostepos (clef répétée autant que nécessaire)

B P U O A M J P W E (version chiffrée du texte)

La table de la page suivante simplifie le travail de chiffrement.

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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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

Vigénère: solidité

- Espace des clefs : n^p (avec n : nombre de caractères possibles et p : taille de la clef)
- 26^8 (avec un alphabet non accentué en minuscules et une clef de 8 lettres) = $\#2 \cdot 10^{11} = \#2^{31}$
- Des lettres identiques sont chiffrées différemment: attaque statistique impossible
- râl

Attaques sur Vigénère

- Pb: comment trouver la taille de la clef ?
- Exemple tiré de [SINGH-1999] :
 - Voir en TD

Transposition

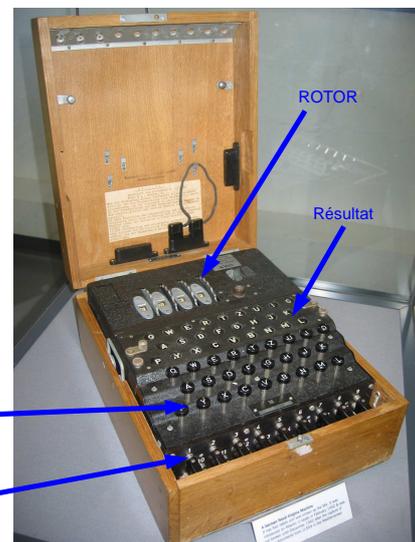
- Transposition: changer l'ordre des lettres d'un texte
- Exemple:
 - on range le texte du message dans un tableau rectangulaire ligne par ligne
 - Le message chiffré s'obtient en lisant le tableau colonne par colonne

ENIGMA

- Utilisé par les allemands durant la seconde guerre mondiale
- déchiffré par les anglais sur de longues périodes

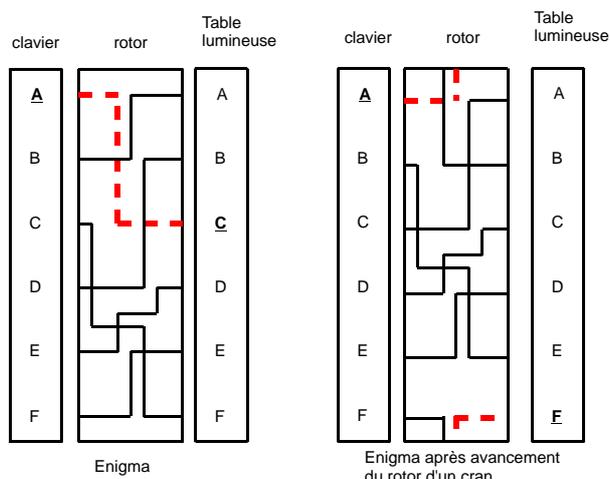
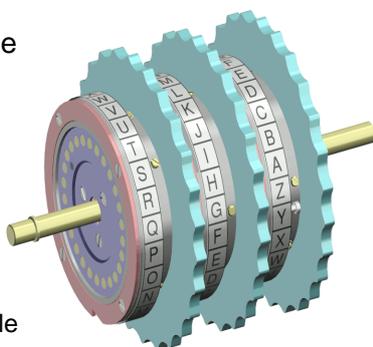
Entrée

Permutations de 6 paires de lettres



ENIGMA

- Chaque rotor réalise une substitution alphabétique
- À chaque codage d'un caractère,
 - le premier rotor tourne
 - Quand le premier rotor a fait un tour, le second rotor tourne
 - ...



Enigma

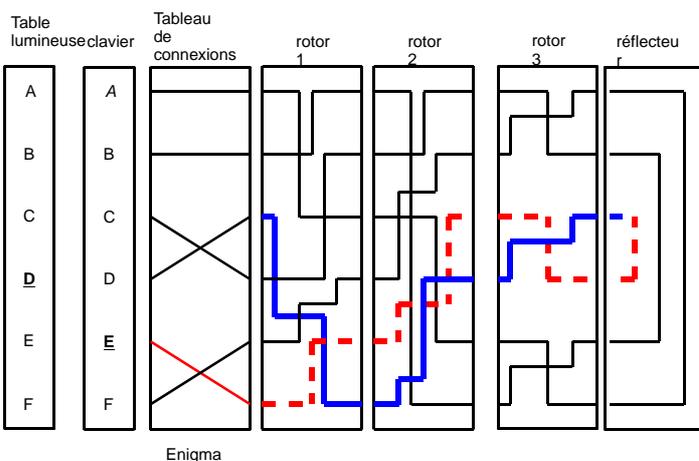
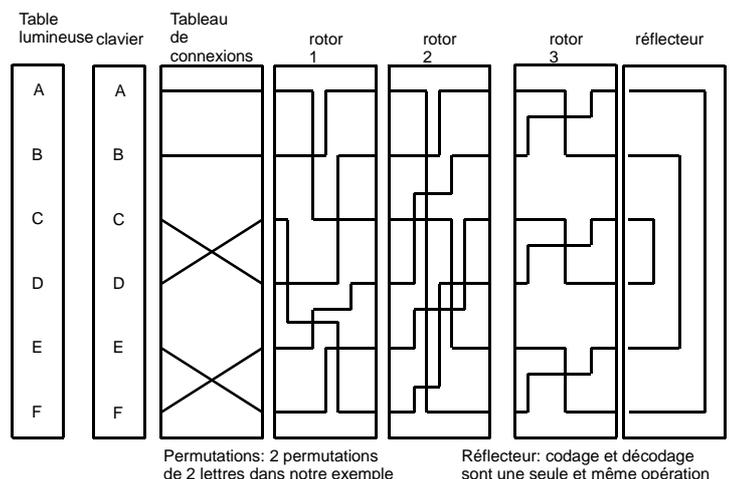
- Conséquence :
 - Les substitutions changent donc à chaque caractère codé
 - Il faut que **tous** les rotors aient fait un tour complet pour qu'on retrouve la même transformation
 - Avec un rotor alphabétique, il faudrait 26 mouvements pour revenir à la transformations initiale
 - Avec deux rotors, 26^2
 - Avec n rotor 26^n
 - Les attaques sur vigenere ont montré la faiblesse que constituait de la répétition des transformations
 - Là, on les limite à défaut de les supprimer

ENIGMA: transpositions

- Pour compliquer :
 - ajout d'un étage de transposition permettant d'échanger deux lettres: ENIGMA avait 6 mécanismes permettant l'échange de 2 lettres au choix
 - Ajoute 100 391 791 500 possibilités = $C(26,2) * 11 * 9 * 7 * 5 * 3 * 1$
 - $C(26,2)$: choisir 12 lettres parmi 26 sans tenir compte de l'ordre
 - Ensuite, on choisit la lettre qu'on associe à la première: 11 possibilités.
 - Il reste 10 lettres disponible. On fait de même pour la première de ces 10 lettres: reste 9 possibilités
 - ...

ENIGMA: nature et nombre des clefs

- Clef:
 - Le choix de la position des rotors. 3 rotors différents que l'on peut placer à la place de son choix : 6 possibilités
 - La position initiale des rotors => $26^3 = 17576$ clefs
- des attaques manuelles sont encore possible
- Plus tard: jusqu'à 8 rotors + choix des rotors
- Un mécanisme de permutations de 6 fois 2 lettres multiplie le nombre de possibilités par 100 391 791 500
- => espace de clef très grand = $\#10^{16} = \#2^{53}$



Mise en oeuvre d'Enigma

- Une clef différente par jour (unique pour toutes les Enigma) :
 - Réglage des connexions: A/L, B/T, E/U, P/F, O/Y
 - Emplacement des brouilleurs : 2, 1, 3
 - Orientation des brouilleurs: Q-C-W (lettre visible)
 - Cette clef sert à chiffrer et transmettre la clef qui servira à chiffrer réellement le message :
 - Pour chaque message, l'émetteur choisit une orientation des brouilleurs et la transmet chiffrée avec la clef du jour. Les autres réglages restent identiques

Bibliographie

- [SINGH-1999]: « Histoire des codes secrets » de Simon Sigh, Livre de poche, 1999 : un ouvrage de vulgarisation qui lit facilement et qui contient aussi pas mal d'informations techniques sur les chiffrements historiques et notamment Enigma

Masque jetable

- Principe du tel. Rouge entre URSS et USA
- Soit M un message binaire= $b_1b_2b_3...b_l$ (avec l le nombre de bits du message)
- Soit $K=k_1k_2k_3...k_l$ une suite de bits impossibles à prédire (on utilise une suite tirée aléatoirement)
- Pour obtenir le message chiffré, on fait un ou exclusif entre chaque bit du message et celui de la clef
 - $c_i = b_i \text{ XOR } k_i$

Masque jetable

- Table du XOR: $0 \text{ XOR } 0 = 0$, $1 \text{ XOR } 0 = 0 \text{ XOR } 1 = 1$ et $1 \text{ XOR } 1 = 0$
- Avantages du masque jetable:
 - Simple à mettre en oeuvre, rapide
 - Sûr si la clef est imprévisible
- Défauts :
 - Transport de la clef: les deux extrémités doivent l'avoir mais pas l'espion. Le transfert sûr de la clef est aussi difficile que celui du message.
 - La génération de la clef qui ne peut être réutilisée d'un message à un autre

Masque jetable

- Connaissant le message et sa version chiffrée, on peut en déduire facilement la clef K
- $C = M \text{ XOR } K$
- $K = M \text{ XOR } C$
- Conséquence: il faut une nouvelle clef pour chaque message
- Méthode du masque jetable ou « One Time Pad »

Principes de Kerckhoffs

- Auguste Kerckhoffs (Hollande, 1883)
 - Seule une donnée de petite taille (clef) doit suffire à assurer la sécurité
 - La sécurité d'un mécanisme ne doit pas reposer sur son caractère secret
- Il est beaucoup plus facile de garder secret un clef connue d'une personne qu'un procédé mis au point par plusieurs personnes.

L'ère scientifique:

- 1976: Diffie et Hellman découvrent la cryptographie à clef publique en mettant au point un algorithme d'échange de clefs ne supposant aucun échange de secret préalable
- 1977: DES (standard américain de chiffrement symétrique)
- 1978: Rivest, Shamir et Alderman (re)découvrent RSA (système de chiffrement à clef publique)

algorithme de chiffrement symétrique (à clefs privées)

- Chiffrement symétrique:
 - la même clef sert au chiffrement et au déchiffrement
 - C'est le principe du coffre fort:
 - Akira et Barack connaissent tous deux la combinaison du coffre fort :
 - Akira dépose un message dans le coffre fort en utilisant la combinaison : elle chiffre le message avec la clef partagée
 - Barack récupère le message en ouvrant le coffre avec la même combinaison: il déchiffre le message avec la clef partagée
 - Si une autre personne réussit à avoir la combinaison, il peut lui aussi ouvrir le coffre et lire ou déposer des messages: elle peut chiffrer de nouveaux messages ou déchiffrer les messages transmis

39

Chiffrement symétrique

- les algo classiques sont rapides
- Pb:
 - comme faire en sorte que Bob et Alice connaissent la clef ?
 - Problème loin d'être négligeable qui se coûtait des sommes importantes aux services secrets du monde entier pour diffuser et renouveler les clefs secrètes envoyées à leur agents :
 - Renouveler suffisamment souvent les clefs
 - Avoir une clefs spécifique pour chaque contexte/agent pour éviter les conséquences de la récupération d'une clef par l'ennemi

algorithme de chiffrement

- chiffrement asymétrique:
 - Chaque participant x
 - a une clef publique P_x qu'il peut diffuser à tous
 - A une clef secrète Q_x qu'il doit être seul à connaître
 - Le chiffrement se fait avec la clef publique
 - Le déchiffrement se fait avec la clef privée
 - Principe de la boîte aux lettres :
 - Alice peut déposer des messages dans la boîte aux lettres: elle chiffre un message avec la clef publique
 - Bob est le seul à avoir la clef de la boîte aux lettres et donc le seul à pouvoir lire les messages qui y ont été déposés: il est seul à pouvoir déchiffrer des messages avec la clef privée.
 - Exemple: si Alice veut envoyer un message à Bob
 - Elle chiffre le message avec la clef publique de Bob
 - Bob reçoit le message chiffré et le déchiffre avec sa clef privée
 - les algo classiques sont lents

41

algorithmes classiques

- symétriques:
 - DES (1976): standard américain (1977), clef de 56 bits sur des blocs de 64 bits. dépassé de nos jours.
 - triple DES (1978): variante, triple application de DES, clefs entre 128 et 192 bits sur des blocs de 64 bits.
 - RC2, RC4, RC5 (1994) et RC6:
 - IDEA (1992): clef 128 bits sur des blocs de 64 bits
 - blowfish: clef 32 à 448 bits sur des blocs de 64 bits. Algo très analysé, considéré comme solide. utilisation libre.
 - AES (1998): clefs 128, 192 ou 256 bits sur blocs de 128 bits. standard américain. utilisation libre.

42

algorithmes classiques

- asymétriques:
 - RSA s'appuyant sur la factorisation de nombres premiers
 - Diffie-Hellman et El Gamal s'appuyant sur le calcul des logarithmiques discrets
 - des algorithmes nouveaux s'appuyant sur les courbes elliptiques

43

Système hybrides

- On génère une clef de session K_s
- On utilise un chiffrement à clef publique pour la transmettre à son correspondant
- On chiffre le reste de la communication avec un algorithme symétrique (donc rapide) utilisant la clef K_s

L'espion

- L'espion est un personnage classique de la cryptographie. Le but initial de la cryptographie était de protéger des communications de ses actions :
 - Il peut vouloir écouter et déchiffrer un message
 - Il peut vouloir déchiffrer tous les messages échangés entre Ahmed et Bernard
 - Il peut vouloir modifier les messages entre Arthur et Bérénice (on parle alors d'écoute active)

L'espion (2)

- Il peut se faire passer pour Anas auprès de Bérénice: on parle d'usurpation d'identité
- Il peut se faire passer pour Alex auprès de Bertrand et pour Bertrand auprès d'Alex : attaque « Man In the Middle »
- Bertrand peut refuser de reconnaître être l'auteur d'un message (reconnaissance de dette, ...) qu'il a pourtant envoyé à Aïcha.

Services s'appuyant sur de la cryptographie

- Confidentialité
- Intégrité
- Authentification:
- Non répudiation

Confidentialité

- protection des données contre une divulgation non autorisée
- 2 moyens techniques complémentaires
 - protéger l'accès aux données (implique authentification et contrôle d'accès). Ex.: authentification windows + ACL NTFS
 - les chiffrer
- intégrité, confidentialité : des contraintes opposées
 - intégrité : multiplier les sauvegardes notamment hors site
 - confidentialité: limiter les lieux de stockage pour faciliter le contrôle d'accès

48

Intégrité

- certifier que les données n'ont pas été altérées de façon intentionnelle ou accidentelle
- la modification peut avoir lieu
 - lors du transfert des données (corruption, écoute active)
 - lors du stockage des données
 - lors de leur traitement (bogues des logiciels applicatifs, des OS).
- Implications:
 - légales, plantage des applications et perte d'activité
 - perte d'image

49

Identification et authentification

- **identification**: définir l'identité de l'utilisateur
- **authentification**: permet de vérifier l'identité fournie (authentification simple vs authentification forte)
 - via un élément que l'utilisateur connaît (mot de passe, ...)
 - via un élément que l'utilisateur possède (carte à puce, certificat, ...)
 - via biométrie

50

authentification

- élément clef pour assurer :
 - la confidentialité et l'intégrité des données via un contrôle d'accès: seules les personnes identifiées, authentifiées et habilités à le faire peuvent accéder/modifier les données
 - la non-répudiation et l'imputabilité (preuve d'une transaction, ...)
- Authentification unique (SSO: Single Sign On)
 - l'utilisateur s'authentifie une fois
 - il a accès à toutes les ressources du réseau
 - cf partie technique (keberos, ...)

51

non répudiation

- **non répudiation** : ne pouvoir nier qu'un événement a eu lieu
- **imputabilité**: on sait qui a réalisé une action
- **traçabilité**: mémoriser des événements imputables
- **auditabilité**: pouvoir réaliser une analyse ultérieure d'un événement. Ex.: en cas d'intrusion.
- moyens: utilisation de journaux
 - de taille limitée
 - éventuellement hors site (intrusion)

52

Signature électronique

- Définition: la *signature électronique* a pour objectif de permettre à une personne d'attacher son identité à un message.
- Problèmes:
 - Le message doit être protégé contre les modifications sinon que certifie-t-on en le signant ?
 - La signature ne doit pas pouvoir être utilisée pour signer un autre message

Signature électronique: exemple à ne pas suivre

- Supposons que signer se résume à ajouter son nom à la fin d'un fichier
 - Tout le monde peut imiter une telle signature (pb de non répudiation)
 - Le document signé peut-être modifié (ajoutons un zéro sur la somme citée dans un chèque et changeons le bénéficiaire)
 - Ajouter de l'information à la fin d'un fichier peut le corrompre

Signature:

- Elle se décompose en deux parties:
 - Un **procédé de signature**: permet d'obtenir les données signées.
 - Ne doit pouvoir être appliqué que par le signataire.
 - Utilise en général un secret détenu par le signataire
 - Un **procédé de vérification**: à partir d'un texte signé et de l'identité du signataire, le procédé de vérification doit confirmer que le texte signé a bien été signé par le signataire désigné
 - doit pouvoir se faire sans secret détenu par le signataire.
- Signature et confidentialité sont deux services distincts qui sont parfois intégrés dans un même système.

Chiffrement symétriques

- clef de chiffrement = clef de déchiffrement
- Chiffrements par bloc:
 - DES (1977), blocs de 64 bits, clefs de 56 bits
 - IDEA (Lai Massey 1991), blocs de 64 bits, clefs de 128 bits
 - Rijndael (Rinmen, Daemen, 1997): blocs de 128 ou 256 bits, clefs de 128, 192 ou 256 bits
 - AES, blocs de 128 bits, clefs de 128, 256 bits
- Chiffrement en continu d'un flux
 - RC4: chiffrement octets par octets
 - Pseudo-Vernam: XOR entre le flux et la sortie d'un générateur aléatoire

Principes de conception

- Problème :
 - On connaît de nombreux systèmes faibles (cesar, substitution, vigenere, ...)
 - comment construire des systèmes sûrs et plus efficaces que le masque jetable

Principes de conception

- Claude Shannon, 1949, « Communication Theory of Secrecy Systems »
 - Confusion: la relation entre le texte clair et le message chiffré doit être impossible à établir. Ca doit notamment être le cas pour les propriétés statistiques de l'un et de l'autre
 - Diffusion: un bit de clef ou de texte clair doit influencer de nombreux bits du texte chiffré.