

Sécurité des systèmes d'information

Initiation à la cryptographie

SR – 2015-2016 –



Problématique

- Protection d'un SI
 - Information numérique
 - Communications sur des canaux publics
 - Machines reliées par un réseau
 - Multi-utilisateurs
- Protection des informations



Pourquoi la cryptographie

- Alice veut envoyer un message à Bob
- Ils ne souhaitent pas que Charlie (un tiers) puisse :
 - Lire le contenu du message : Confidentialité
 - Modifier le message : Intégrité
 - Envoyer de faux messages, usurper l'identité : Authentification
 - Réinjecter d'anciens messages : Anti-rejeu
- Alice ne doit pas pouvoir nier avoir envoyé le message : non-répudiation

Types d'attaques

- **Attaques passives**
 - Analyse de trafic (méta-données)
 - Interception de messages
- **Attaques actives**
 - Modification
 - Insertion
 - Suppression
 - Rejeu
 - Déni de service

Vocabulaire

- Cryptographie
 - Κρυπτός : secret, γράφειν : écrire
 - Art et science de conserver les messages secret
- Cryptanalyse
 - Art et science de déchiffrement des messages chiffrés sans en connaître la clé
- Cryptologie
 - Regroupe Cryptographie et Cryptanalyse

Vocabulaire

- Chiffrer/chiffrement
 - Transformation d'un message clair en un message incompréhensible par quelqu'un ne disposant pas de la clé de déchiffrement
- Déchiffrer
 - Transformation d'un message chiffré en un message compréhensible à l'aide de la clé de déchiffrement
- Décrypter
 - Retrouver le message en clair à partir d'un message chiffré SANS connaître la clé de déchiffrement
- **Crypter**

Trois approches classiques

- Codage
- Stéganographie
- Chiffrement

----- texte chiffré -----
783ce4bc5828a52e4292e11b632775204c94b5fb6bfc4b578d85727b1947b0f1
67aae28ec2a62542f7900a91f05de9c916e0d2b87dc75099f0935aa40c3dc884
82190daf9e7251e106af8a3b9ae11afe9d25de46d5a15a2311f337c526092b54
1a06b1e2281c6a6a90c2a1f77948b9d52fc2d860a2b904ee7b25af272dc8911c
c6f1aa5a1bcbd06f766583ecf623e9b1b2a1fe6dd14fbfab6b068a95f3372e07
f79b90b903e691e69016e17c78bc9ac7eacb3e1838b5833c643d1357dcc13936
5ce61b7f00f4f2d74f0d8cb6407c4c6c0cb95dc6efd2fa498bdfb22a2388ea91
dcde26ac868689b2463fda779a6b10650719b0396532c0c21538d9db9b1c93fb
e8b4414bb7cf6074be7a8dfea92b448f07133d2c4085bec4a6661dea058622c7
6570553a460156c20a0d5b586ad01e9ebb8fc0f0d34266764675fa64dc12e6d8
5bf0d518ef86420c1ece833053347e1b3317d1d14cebf5a7cc0ccd247eb40ea7
e52e7e30421416ef2d4fd4938b252a1ee1d3f29b27ac34b3cb43ba8cbb03b139
f52ee656923456924857a53e8faf8b8db867eeb57c52241fe43841d0745afcce
e2eece5599ce79883516ba34468edccea72bd3d9afe6de49744d2b1bd85e368ce
d5232724063e11bada0d19e3e84952cbc001880948e49e800377dc635c173755
b199b250db61af75d5bbac7d55e7571adb099b0028cac3af2a7f93489d76a8e9d
825fd52eafbd9b766899c21875e1c13684fd531513a2584c39d48b5fc88eb590
8c2711ace2030608e164a926c9589f4e80e79e4764a9234ae0e136f801c3fe83
d6622f4cc6886c9c28ddef1888d575a227d0a4c47ac8a88b98cf02518fa1345
948822da700ddb781c5a419e44020a1f67601185b4adabe0cce4c14ce13ec884
81bc1420728158b706082d05d42b0a202814bf55ed7b62c1316166d46422540



RadioLondres

@_RadioLondres_

Ici #RadioLondres "les sanglots longs
des violons de l'automne blessent
mon coeur d'une langueur monotone"
je répète .. 06juin44 #DDay



Codage

- Découpage d'un message en unité syntaxique
 - Syllabes, mots, phrases...
- Substitution de chaque unité par une autre selon une table de transformation : clé ou livre de code
 - La table peut aller d'une simple feuille à plusieurs livres
 - Le niveau de sécurité augmente avec la taille du livre de code (limite les répétitions)
 - Cryptanalyse demande beaucoup de matériau chiffré pour détecter les répétitions

Codage - exemples

- Exemple
 - 10-13 à NYC
 - Policier à besoin d'aide immédiate
 - 144D3
 - Remplace le 3^{ème} mot de la D^{ème} ligne de la page 144 d'un livre (édition spécifique convenu à l'avance)
 - « Les sanglots longs des violons de l'automne... »
 - Signale de l'imminence du débarquement allié aux résistants français à la radio

Codage – non sécuritaire

- Certains code ne sont pas utilisés dans un but sécuritaire mais pour compresser les messages courants
 - Communication radio :
 - QSA : My signal strengh is..
- Code convenu à l'avance, usage limité à la création



Codage : limites et cryptanalyse

- Epeler les mots absents du dictionnaire de codage
 - Se comportent souvent comme un chiffre classique par substitution
- Lenteur de codage/décodage manuel
- Code établit au préalable
- Cryptanalyse essentiellement linguistique
- Un élément du livre de code ne peut pas être décodé tant qu'il n'a pas été utilisé
 - Parfois possible de décoder tout les message sans avoir la table de codage intégrale

Stéganographie

- Consiste à disperser un message au sein d'un message anodin :
 - Encre invisible
 - Microfilm
 - Image
 - Mots d'un texte
- La clé est la fonction de dispersion
 - Ex: 1^{er} mot de chaque ligne

Stéganographie - exemple

Disadvantages and advantages of networks

Since the first concoction of a nexus of computational processing power in the late 1960s, never has the practicality of networks been bought into question due to the advancements of on-going assemblages excogitating advantageous intimations for the ever changing cycle of headway to the modern day network. Providing valuable resources to organisations, innumerable technicians give their time to creating and perfecting a cornucopia of networks.

The advantages of networks are prominent and numerous, and very well documented. So you might be asking yourself why there is debate over aspects of networks, from home networks up to large corporate networks. This is due to the widespread fear that networks are essentially neversafe, due to the interlacing of computers providing an ideal environment for viruses which are going to exploit a security loophole to contaminate multiple computers, which ultimately prevails to high costs for companies. Once one computer in a network is infected, the virus can competently let itself in to other computers on the network; it only takes one computer linked to yours to infect you. This has led to concerns over the security of organisations having a system which can be taken down with just one file.

Stéganographie - intérêts

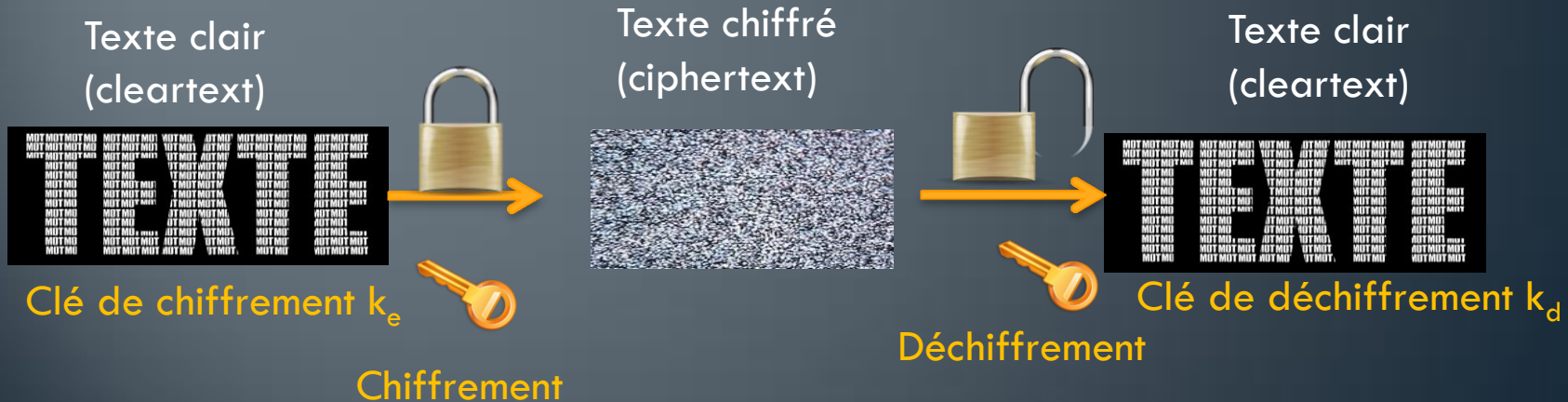
- Communiquer lorsque c'est interdit/impossible
 - Censure/surveillance
 - Loi interdisant le chiffrement
 - Discrétion
- Publier ouvertement des informations à l'insu de tous pour pouvoir en prouver l'antériorité le cas échéant
- Inconvénient : énorme « overhead »

Stéganographie - applications

- Canaux cachés
 - Etablir un canal de communication caché au dessus de protocoles anodins : contourner le blocage d'un pare-feu en encapsulant les données dans un protocole légitime (http, https, dns...)
- Filigrane
 - Identifier l'auteur dans un document numérique
 - noms en blanc sur fond blanc dans un pied de page
 - Identifier la source d'une fuite en marquant de façon discrète chaque exemplaire.

Chiffrement

- Transformer un message clair en le découpant en unités d'information de taille fixe (bit, caractère, bloc) sans se préoccuper des unités syntaxiques du message
- La clé est un paramètre de la fonction de transformation



Chiffrement et déchiffrement

- Chiffrement :
 - fonction bijective
 - Assure la confidentialité
 - Nécessite une clé
- $C = E_{K_e}(M)$: Chiffrement de M avec la clé K_e
- $M = D_{K_d}(C)$: Déchiffrement de C avec la clé K_d
- $(D_{K_d} \circ E_{K_e}) = Id$
- Le chiffrement et le déchiffrement d'un message n'augmentent pas la quantité de données (hors protocole)

Chiffrement – qualité d'un bon chiffre


- Trouver la fonction inverse D_{K_d} de E_{K_e} doit être un problème difficile
- La clé doit être temporaire : tout chiffre est cassé un jour ou l'autre. Il doit résister durant la période de validité de l'information qu'il protège.
- La difficulté du déchiffrement ne doit pas dépendre du secret des algorithmes mais du secret des clés (principe d'Auguste Kerckhoffs 1883)
 - Un algorithme reste rarement secrets (ex:RC4)

Chiffrement – qualité d'un bon chiffre


- Un chiffre doit être stable
- Les opérations de chiffrements et déchiffrements doivent être rapide, simple et sans erreurs
- La clé doit être imprévisible : choisie aléatoirement dans un espace de clé très grand
- Les doivent être changées fréquemment et facilement
- Les messages en clair doivent comporter le moins de redondance possible
 - Compression ou ajout de bruit

Espace de clé


I'll just comment out these lines...




```
//MD_update(&m, buf, j);
```



```
//do_not_crash();
```



```
//prevent_911();
```



IN THE RUSH TO CLEAN UP THE DEBIAN-OPENSSL FIASCO, A NUMBER OF OTHER MAJOR SECURITY HOLES HAVE BEEN UNCOVERED:

AFFECTED SYSTEM	SECURITY PROBLEM
FEDORA CORE	VULNERABLE TO CERTAIN DECODER RINGS
XANDROS (EEE PC)	GIVES ROOT ACCESS IF ASKED IN STERN VOICE
GENTOO	VULNERABLE TO FLATTERY
OLPC OS	VULNERABLE TO JEFF GOLDBLUM'S POWERBOOK
SLACKWARE	GIVES ROOT ACCESS IF USER SAYS ELVISH WORD FOR "FRIEND"
UBUNTU	URNS OUT DISTRO IS ACTUALLY JUST WINDOWS VISTA WITH A FEW CUSTOM THEMES

A. Kerckhoffs – Desiderata de la cryptographie militaire

Il faut bien distinguer entre un système d'écriture chiffrée, imaginé pour un échange momentané de lettres entre quelques personnes isolées, et une méthode de cryptographie destinée à régler pour un temps illimité la correspondance des différents chefs d'armée entre eux. Ceux-ci, en effet, ne peuvent, à leur gré et à un moment donné, modifier leurs conventions ; de plus, ils ne doivent jamais garder sur eux aucun objet ou écrit qui soit de nature à éclairer l'ennemi sur le sens des dépêches secrètes qui pourraient tomber entre ses mains.

Un grand nombre de combinaisons ingénieuses peuvent répondre au but qu'on veut atteindre dans le premier cas ; dans le second, il faut un système remplissant certaines conditions exceptionnelles, conditions que je résumerai sous les six chefs suivants :

A. Kerckhoffs – Desiderata de la cryptographie militaire

1. Le système doit être matériellement, sinon mathématiquement, indéchiffrable ;
2. Il faut qu'il n'exige pas le secret, et qu'il puisse sans inconvénient tomber entre les mains de l'ennemi ;
3. La clef doit pouvoir en être communiquée et retenue sans le secours de notes écrites, et être changée ou modifiée au gré des correspondants ;
4. Il faut qu'il soit applicable à la correspondance télégraphique ;
5. Il faut qu'il soit portatif, et que son maniement ou son fonctionnement n'exige pas le concours de plusieurs personnes ;
6. Enfin, il est nécessaire, vu les circonstances qui en commandent l'application, que le système soit d'un usage facile, ne demandant ni tension d'esprit, ni la connaissance d'une longue série de règles à observer.

Cryptanalyse

- Attaque à texte chiffré connus (C) (*ciphertext only*)
 - L'attaquant ne dispose que de messages chiffrés
- Attaque avec texte clair connu (M,C) (*known plaintext*)
 - L'attaquant dispose des textes clairs et de leur version chiffré
- Attaque à texte clair choisi ($M \rightarrow C$) (*chosen plaintext*)
 - L'attaquant peut faire chiffrer ce qu'il veut et obtenir le résultat
- Attaque à texte chiffré choisi : ($C \rightarrow M$) (*chosen ciphertext*)
 - L'attaquant peut faire déchiffrer ce qu'il veut et obtenir le résultat

Cryptanalyse

- Interception (Man In The Middle)
- Horloge (timing)
- Obtention de la clé par d'autre moyens..

Cryptanalyse : exemple

Le chiffre de César paramétrique

- Décalage circulaire des lettres de n positions dans l'alphabet
- Exemple : $n=4$

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
Chiffré	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

- ASYRIA = EWCVME
- Nombre de clé faible : 26 (bruteforce possible)
- Analyse fréquentielle simple

Exemple de texte chiffré avec le code César

- Y'uvire f'vafgnyyr qbhprzrag qnaf yn ahvg Yn arvtr rfg ervar n fba gbhe Ha eblnhzr qr fbyvghqr Zn cynpr rfg yn cbhe gbhwbfhef Yr irag dhv uheyr ra zbv ar crafr cyhf n qrzvna Vy rfg ovra gebc sbeg W'nv yhggr, ra inva Pnpur grf cbhibvef, a'ra cneyr cnf Snvf nggragvba, yr frperg fheivien Cnf q'rgngf q'nzr, cnf qr gbhezragf Qr fragvzragf Yvorerr, Qryvierr Wr ar zragvenv cyhf wznvf Yvorerr, Qryvierr P'rfq qrpvqr, wr z'ra invf W'nv ynvffr zba rasnapr ra rgr Creqhr qnaf y'uvire Yr sebvq rfg cbhe zbv, Yr cevk qr yn yvoregr. Dhnaq ba ceraq qr yn unhgrhe Gbhg frzoyr vafvtavsvnag Yn gevfgrrffr, y'natbvffr rg yn crhe Z'bag dhvggrrf qrchvf ybatgrzcf Wr irhk ibve pr dhr wr crhk snver Qr prggr zntvr cyrvar qr zlfgrerf Yr ovra, yr zny wr qvf gnag cvf Gnag cvf. Yvorerr, Qryvierr Yrf rgbvyrf zr graqrag yrf oenf Yvorerr, Qryvierr Aba, wr ar cyrher cnf Zr ibvyn ! Bhv, wr fhvf yn ! Creqhr qnaf y'uvire Zba cbhibve ivrag qh pvry rg rainuvy y'rfcnpr Zba nzt f'rkcevzr ra qrffvanag rg fphycgnag qnaf yn tynpr Rg zrf crafrrf fbag qrf syrhef qr pevfgny tryrrf. Aba wr ar erivraqenv cnf Yr cnffr rfg cnffr ! Yvorerr, Qryvierr Qrfbezvfv cyhf evra ar z'neergr Yvorerr, Qryvierr Cyhf qr cevaprffr cnesnvgr Wr fhvf yn ! Pbzzr wr y'nv erir ! Creqhr qnaf y'uvire Yr sebvq rfg cbhe zbv yr cevk qr yn yvoregr

Cryptanalyse

R	205	20,34%
F	84	8,33%
V	83	8,23%
N	70	6,94%
Y	69	6,85%
A	69	6,85%
G	66	6,55%
E	64	6,35%
Q	43	4,27%
H	42	4,17%
C	40	3,97%
B	40	3,97%
Z	31	3,08%
I	24	2,38%
P	17	1,69%
W	14	1,39%
O	12	1,19%
S	9	0,89%

On identifie
clairement le E
 $E \rightarrow R = +13$

La clé est +13

E	17,115
S	7,948
A	7,636
I	7,529
T	7,244
N	7,095
R	6,553
U	6,311
L	5,456
O	5,378
D	3,669
C	3,26
P	3,021
M	2,968
V	1,628
Q	1,362
F	1,066
B	0,901

Fréquence d'apparition
des lettres dans le cypher

Fréquence d'apparition des lettres en français

Chiffre de Vigenère

- Substitution polyalphabétique
 - Version généralisée du chiffrement de César
 - Clé de plusieurs caractères
 - Au lieu d'utiliser le même décalage pour chaque lettre, on utilise un décalage dépendant de chaque caractère de la clé
 - Sécurité dépend de la longueur de la clé
 - Présenté au XVI^{ème} siècle, pas cassé avant le XIX^{ème} siècle
 - Trouver la longueur de la clé par recherche de motifs (recherche du PGCD des écarts entre les motifs)
 - Retour à un cas de substitution monoalphabétique (ex: César)

Cryptanalyse – Chiffre de Vigenère

KQOWEFVJPUJUUNUKGLMEKJINMWUXFQMKJBGWRLFNFGHUDWUUMBSVLPS
NCMUEKQCTESWREEKOYSSIWCTUAXYOTAPXPLWPNTCGOJBGFQHTDWXIZA
YGFFNSXCSEYNCTSSPNTUJNYTGGWZGRWUUNEJUUQEAPYMEKQHUIDUXFP
GUYTSMTEFFSHNUOCZGMRUWEYTRGKMEEDCTVRECFBDJQCUSWVBPNLGOYL
SKMTEFVJJTWWMFMWPNMEMTMHRSPXFSSKFFSTNUOCZGMDOEOYEKCPJR
GPMURSKHFRSEIUEVGOYCWXIZAYGOSAANYDOEOYJLWUNHAMEBFELXYVL
WNOJNSIOFRWUCCESWKVIDGMUCGOCRUGNMAAFFVNSIUDEKQHCEUCPFC
MPVSUDGAVEMNYMAMVLFMAOYFNTQCUAFVFJNXKLNEIWCWODCCULWRIFT
WGMUSWOVMATNYBUHTCOCWFYTNMGYTQMKBBNLGFBTWOJFTWGNTTEJKNEE
DCLDHWTYYIDGMVRDGMPLSWGJLAGOEKJOFEKUYTAANYTDWIYBNLNYP
WEBFNLFYNAJEBFR

Cryptanalyse – Chiffre de Vigenère

KQOWEFVJPUJUUNUKGLMEKJINMWUXFQMKJBGWRLFNFGHUD**WUU**MBSVLPS
NCMUEKQCTESWR**EEK**OYSSIWCTUAXYOTAPXPLWPNTCGOJBGFQHTD**WXIZA**
YGFFNSXCSEYNCTSSPNTUJNYTGGWZGR**WUU**NEJUUQEAPYMEKQHUIDUXFP
GUYTSM TFFSH**NUOCZGM**RUWEYTRGKMEEDCTVRECFBDJQCUSWVBP NLGOYL
SKMTEFVJJTWWMFMWPNMEMTMHRSPXFSSKFFST**NUOCZGM****DOEOY****EEK**CPJR
GPMURSKHFRSEIUEVGOYC**WXIZAYG**OSAANY**DOEOY**JLWUNHAMEBFELXYVL
WNOJNSIOFRWUCCESWKVID**GMU**CGOCR UWGNMAAFFVNSIUDEKQHCEUCPFC
MPVSUDGAVEMNYMAMVLFMAOYFNTQCUAFVFJNXKLNEIWCWODCCULWRIFT
W**GMU**SWOVMATNYBUHTCOCWFYTNMGYTQMKBBNLGFBTWOJFTWGNT EJKNEE
DCLDHWTYYIDGMVRDGMPLSWGJLAGOEKJOF EKUYTAANYTDWIYBNLNYNP
WEBFNLFYNAJEBFR

Cryptanalyse – Chiffre de Vigenère

Longueurs de clef possibles (diviseurs de la distance)					
Séquence répétée	Distance entre les répétitions	2	3	5	19
WUU	95			x	x
EEK	200	x		x	
WXIZAYG	190	x		x	x
NUOCZGM	80	x		x	
DOEOY	45		x	x	
GMU	90	x	x	x	

Clé de 5 caractères, on peut donc appliquer l'analyse fréquentielle sur les 5 groupes pour trouver la clé

Aujourd'hui

- 1950
 - Arrivé des ordinateurs
 - Explosion des capacités de calcul
- Nouveaux canaux de communication
 - Internet
 - Besoin d'échanger en temps réel
 - Volumétrie des échanges explose
 - Démocratisation du chiffrement pour le grand public

Cryptographie symétrique

- Secret partagé entre les deux parties
 - Opérations symétriques
 - La même clé est utilisé pour chiffrer et déchiffrer
- Problématique
 - Nécessité de disposer d'un canal de confiance pour échanger ce secret
 - Authentification préalable ?

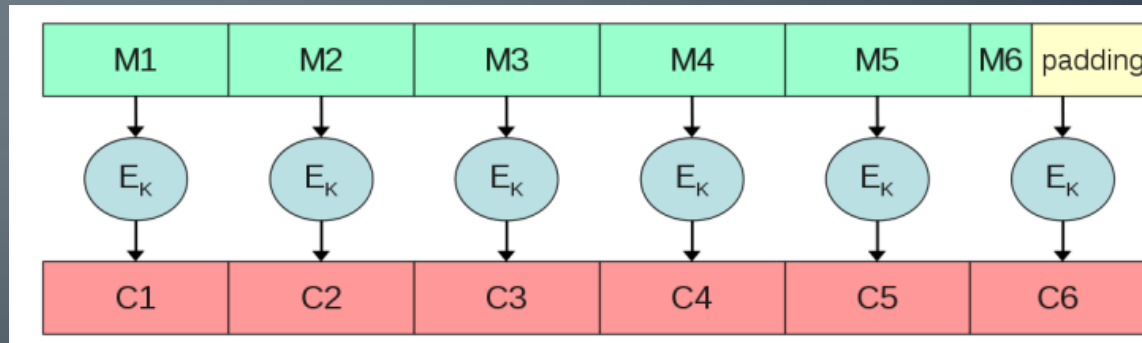


Familles

- Deux familles de chiffrement symétrique
 - Chiffrement par flot
 - Peu utilisé aujourd'hui (ex : RC4)
 - Chiffrement par bloc

Chiffrement par bloc

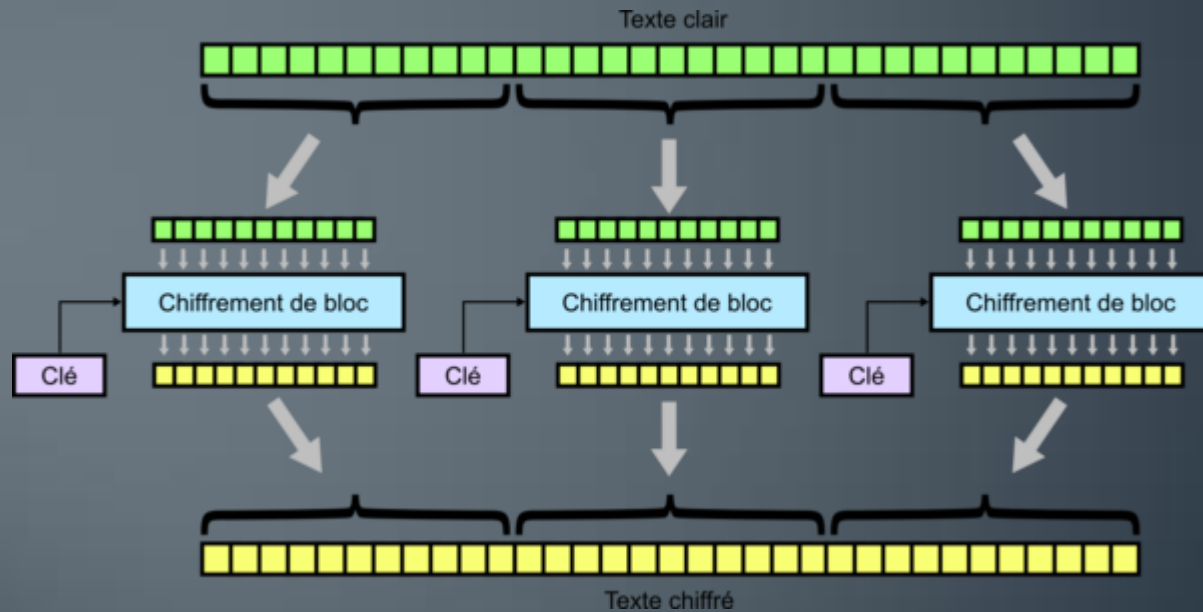
- Principe
 - Opération sur un flot généralement fini
 - Chiffrement/déchiffrement sur des blocs de taille fixe (ex. 64, 128, 256bits)
 - Il faut parfois rajouter du padding pour compléter un bloc



Chiffrement par bloc

- Opération de chiffrement sur les blocs variés en fonction
 - Des performances
 - De la sécurité
 - De la propagation des erreurs au cours du chiffrement
- Plusieurs algorithmes
 - DES
 - 3DES
 - AES
 - TwoFish
- Plusieurs modes
 - ECB
 - CBC
 - CTR

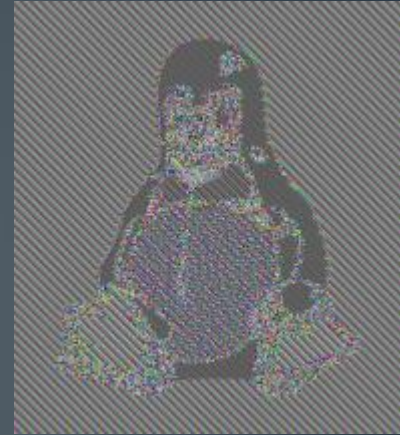
Chiffrement par bloc - ECB



Chiffrement par bloc - ECB



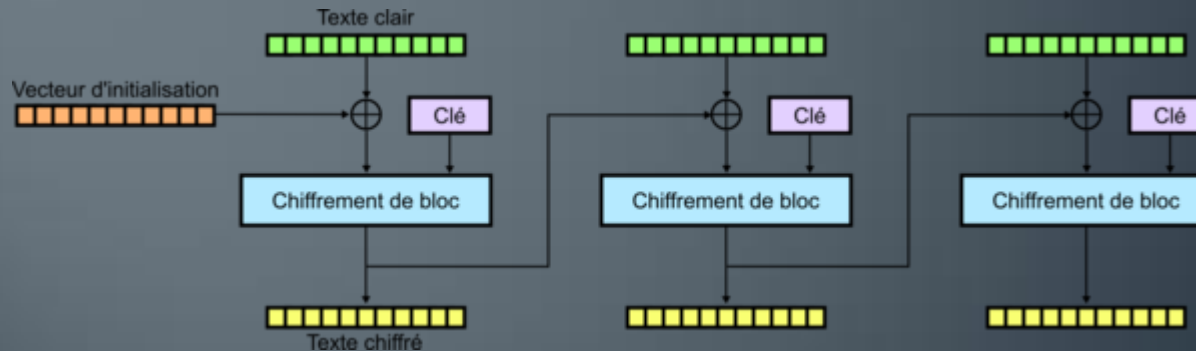
**Do Not
Use**



- Un attaquant peut réinjecter des blocs chiffré
 - $C_0C_1C_2C_3 \rightarrow C_0C_3C_1C_2C_3$ (modification d'un RIB sur un virement...)

Chiffrement par bloc - CBC

- CBC – Cipher Block Chaining
 - Chainage des blocs, deux blocs identiques seront chiffrés différemment
 - Ajout d'un vecteur d'initialisation (IV) → Session
 - IV doit servir qu'une fois et être non prédictible

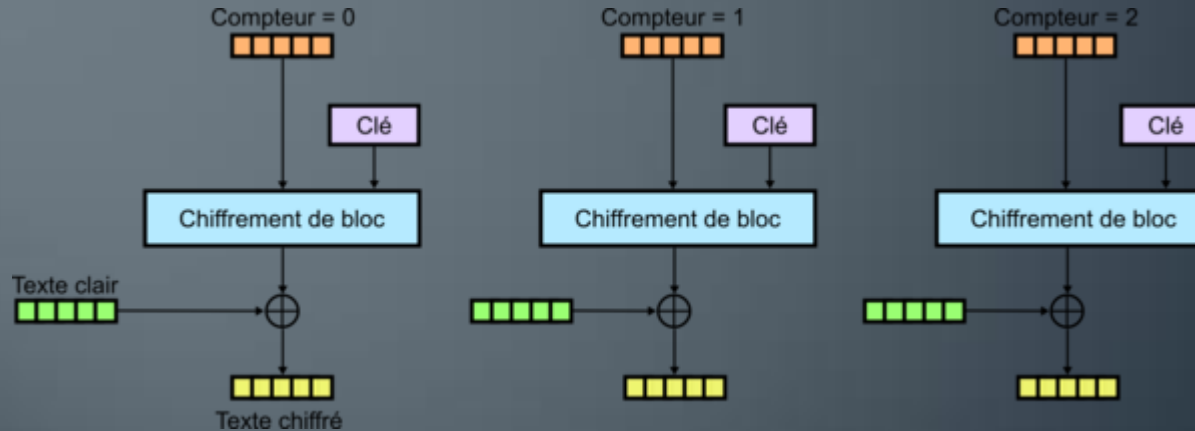


Chiffrement par bloc - CBC



Chiffrement par bloc - CTR

- Permet l'accès aléatoire et le chiffrement par flot
- Parallélisable, bien pour les multiprocesseurs
- À utiliser avec un IV !



DES(s)

- DES

- Clé de 56 bits, blocs de 64 bits
- EFF deep Crack (1998) : 3 jours, 250 000\$
- EFF 'Deep Crack' et distributed.net (1999) : 22h15
- COPACABANA (2006) : 6,4 jours, 10 000\$
- RIEVYERA S3 – 5000 (2008) : <1 journée, 128 FPGA

- 3DES

- Variante du DES
- Utilise 2 ou 3 clés DES (112 à 168 bits)
- Chiffrement [k1], Déchiffrement [k2], Chiffrement [k3 ou k1]
- En pratique, sécurité réduite à 112 bits max
- Trois fois plus lent que DES
- Compatible avec DES si $K1=K2$

AES – Advanced Encryption Standard 1998

- Clés de 128, 192, 256 bits
- Blocs de 128 bits
- Très rapide
 - Logiciellement : substitution ou opération simple
 - Matériellement : Intel fournit des instructions 'aes' dans ses processeurs
- Algorithme intensément analysé, premier algorithme approuvé par la NSA pour le TOP SECRET (2003)

Les deux parties doivent connaître la clé
Les communications à N parties nécessitent $\frac{n*(n-1)}{2}$ clés

Cryptographie asymétrique

- Cryptographie à clé publique
 - Chiffrement et déchiffrement utilisent chacun une clé différente
- Deux clés en jeu
 - Une clé de chiffrement, publique, communiqué aux partenaires
 - Une clé de déchiffrement, privée, elle doit rester secrète
- Plus besoin d'avoir un canal sécurisé pour l'échange de secret
 - Authentification nécessaire cependant
- Principe de la signature numérique impliquant la non-répudiation

Cryptographie asymétrique

- Basé sur des problèmes mathématique sans solution efficace connue
 - Facile à calculer dans un sens
 - Difficile à inverser sans connaître une information particulière : clé privée
- Exemples:
 - Logarithme discret (Diffie-Hellman, DSA, ElGamal)
 - Factorisation de grands entiers (RSA)
 - Logarithme discret sur les courbes elliptiques (ECDSA, ECDH)

Cryptographie asymétrique

Utilisation

- Chiffrement
 - Alice chiffre le message m avec la clé publique de Bob
 - Seul bob dispose de la clé privée associée permettant de déchiffrer le message
- Signature numérique
 - On chiffre un hash du message avec sa clé privée
 - N'importe qui peut vérifier la signature en 'déchiffrant ' avec notre clé publique
 - Seul le détenteur de la clé privée peut générer cette signature

Cryptographie asymétrique

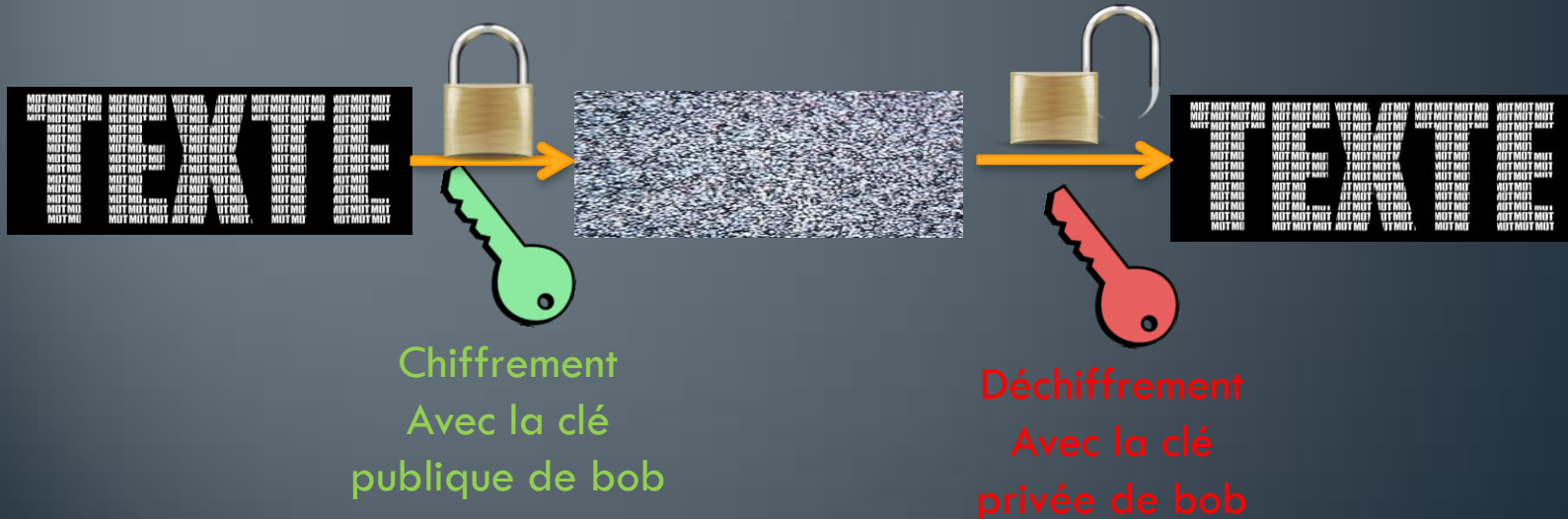
Historique

- 1976 : Diffie-Hellman
- 1978 : RSA (Rivest, Shamir et Adleman)
- 1983 : RSA est breveté
- 2000 : RSA entre dans le domaine public
- 1984 : ElGamal
- 1991 : DAS/DSS
- 2004 : ECC (courbes elliptiques)

Cryptographie asymétrique

Utilisation : chiffrement

- Alice souhaite envoyer un message à bob
 - Bob a envoyé sa clé publique à Alice
 - Bob utilise sa clé privée pour déchiffrer



Cryptographie asymétrique

Utilisation : signature

- Authentification, intégrité, non-répudiation



Authentication != signature

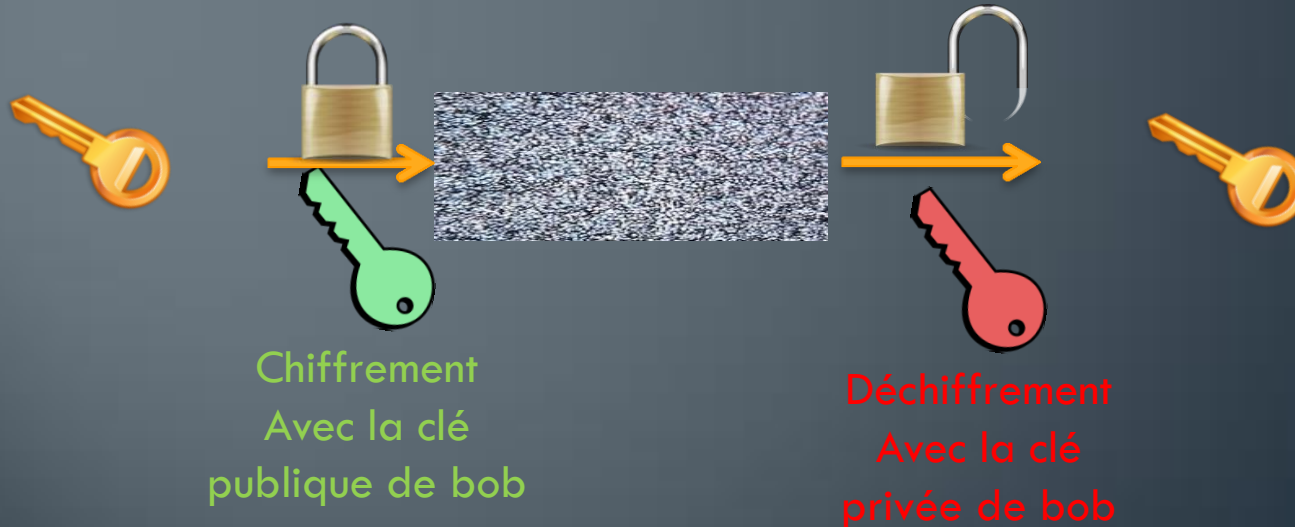
L'authentification permet de répondre à la question :

- Qui a émis le message ?

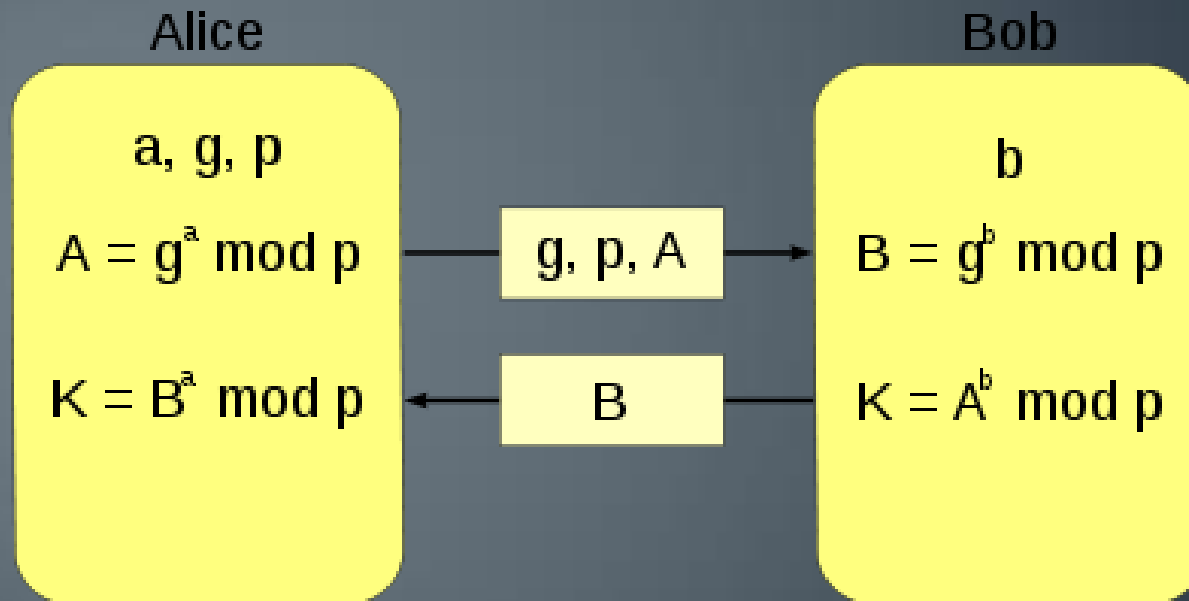
Pour savoir si on peut parler de signature, il faut savoir qui pose la question

- MAC : l'autre est possesseur de la clé secrète, donc deux personnes peuvent émettre
- Signature : un possesseur de la clé publique, donc tout le monde peut vérifier, mais une seule personne peut émettre
 - Principe de non-répudiation !

Utilisation – transport de la clé

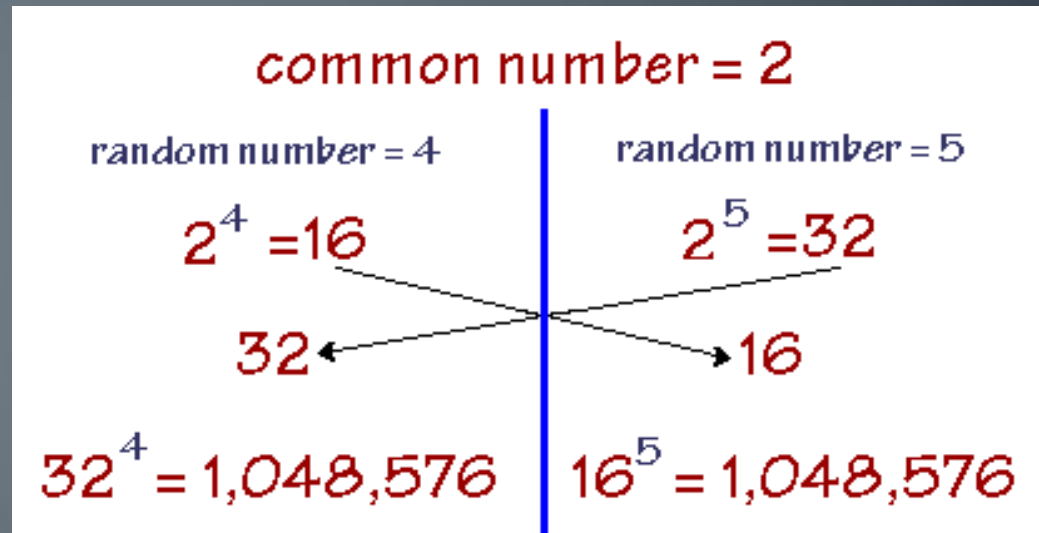


Diffie Hellman



$$K = A^b \text{ mod } p = (g^a \text{ mod } p)^b \text{ mod } p = g^{ab} \text{ mod } p = (g^b \text{ mod } p)^a \text{ mod } p = B^a \text{ mod } p$$

Exemple

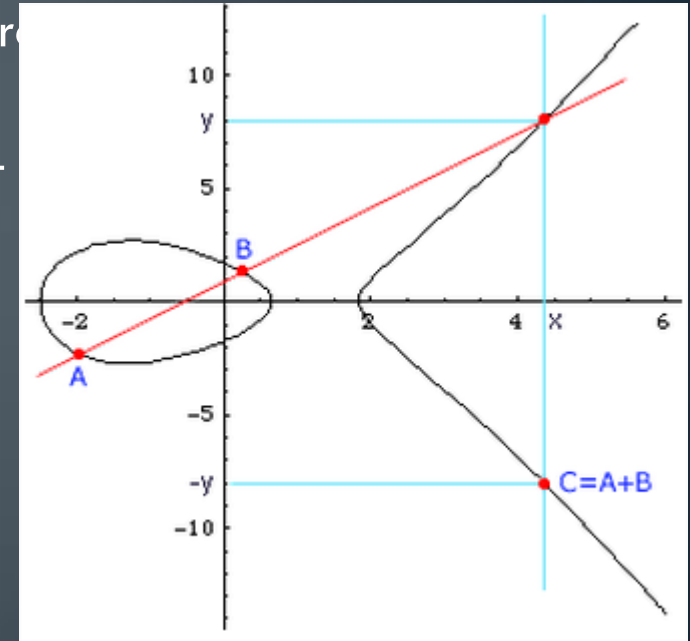


Diffie-Hellman

- Échange de secrets sans canal préalable
 - Vulnérable à une attaque man-in-the-middle
 - Nécessite d'être réalisé sur un canal authentifié
- Permet la Perfect Forward Secrecy
 - Renouvellement fréquent des secrets
 - En cas de compromission d'une conversation, une conversation antérieure ne pourra être déchiffrée

Courbes elliptiques

- Objets mathématiques sur lequel on peut définir un ensemble (de points) munis d'une addition
 - Clés employées plus courtes (moins de ressources de sécurité)
 - Repose sur le problème du logarithme discret dans le groupe correspondant
 - Aucun algorithme connu plus efficace que les méthodes génériques de calcul de logarithme discret



Bilan

Avantages

- Pas besoin de canal de confiance, la clé est publique
- Permet de faire
 - de la signature numérique avec non-répudiation
 - de l'échange de clé

Inconvénients

- Opérations extrêmement lentes
 - On ne peut chiffrer que des informations petites
- Comment déterminer si l'on possède la bonne clé publique ?
 - Problème de l'authentification du canal