



Pierre DUSART (Université de Limoges)

LA CRYPTOGRAPHIE

Aborder la cryptologie de façon historique



Communications en Alice et Bob

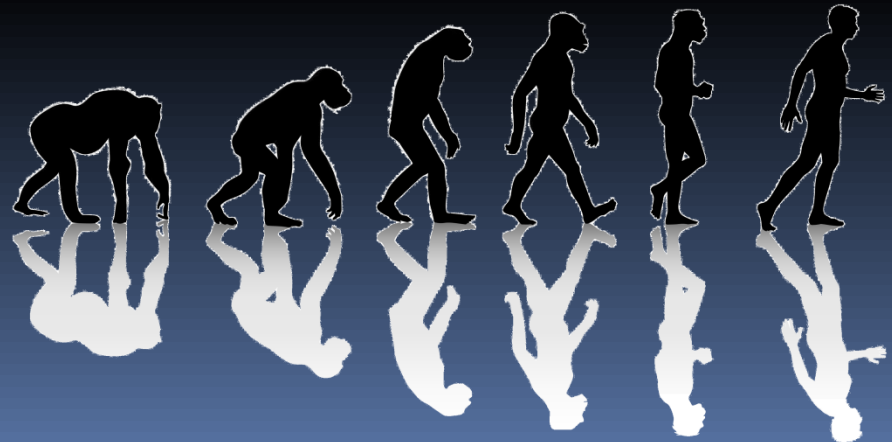


- Dans le langage courant, on parle de codes secrets mais il vaut mieux parler de chiffrement (service du chiffre) pour ne pas confondre avec les codes correcteurs d'erreurs.
- Ce sont les militaires qui créent, s'approprient et développent le concept!

Au travers des âges

- Trois grandes étapes :
 - Chiffrements alphabétiques manuels (1500)
 - Chiffrements alphabétiques mécaniques (1930)
 - Chiffrements numériques (1990)

- Futur : chiffrement quantique (???)



Connaissances en Classe de Seconde

- Depuis le début de l'année, avec eux j'ai seulement parlé:
 - du chiffrement de César,
 - du chiffrement affine.
 - du reste de la division modulo 26.
- certains ont puisé l'info sur internet du décodage affine mais nous n'avons pas abordé la théorie (nous utilisons le tableur pour déterminer les inverses dans $\mathbb{Z}/26\mathbb{Z}$)

Chiffrements alphabétiques

- Substitution
 - César (OUI + 10 -> ??)
 - Chiffrement affine
 - Vigenère



- Permutation
 - Scytale (-600 av JC)
 - Carrés 5*5 (I=J)
 - Transpositions



E	R	S	C	H	O
T	T	H	E	G	O
F	D	O	M	Y	L
A	N	I	H	E	B
E	M	T	E	E	M

E	R	S	C	H	O
T	T	H	E	G	O
F	D	O	M	Y	L
A	N	I	H	E	B
E	M	T	E	E	M

Vigenère

	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
A	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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



ZERO (Message)
 + ZERO (Clef)
 = YIIC (Chiffré)

Anagramme choisie

LA CRYPTOGRAPHIE C'EST FACILE

L	A	C	R	Y
P	T	O	G	R
A	P	H	I	E
C	E	S	T	F
A	C	I	L	E

HSTIGOTPECILEFERYRCALPACA

Carré de Polybe

	1	2	3	4	5
1	C	R	Y	P	T
2	O	G	A	H	I,J
3	E	B	D	F	K
4	L	M	N	Q	S
5	U	V	W	X	Z

J'ECOUTE EN CLASSE

25 31 11 21 51 15 31 31 43 11 41 23 45 45 31

A vous de déchiffrer

33 31 15 31 42 14 45 31 43 15 31 42 14 45

Chiffrements alphabétiques mécaniques

- Le but : ne plus faire les opérations à la main
 - Fastidieux
 - Risque de se tromper
- Enigma



Réglages initiaux = Clef

- On règle la machine :
 - On choisit 3 lettres : Chaque rotor peut être mis sur une lettre
 - On choisit les lettres échangées dans le tableau de connections
 - On choisit l'ordre des rotors.
- Cette position initiale conditionne le comportement de la machine : c'est la clef secrète!

Chiffrements numériques

Codage de caractères (ce n'est pas de la crypto)

On transforme les signes (lettres) par des nombres (ensemble de 0 et 1)
selon la table ASCII :

'A' = (01000001)

Et ainsi de suite

Chiffrement XOR (Ou-exclusif)



Exemple :

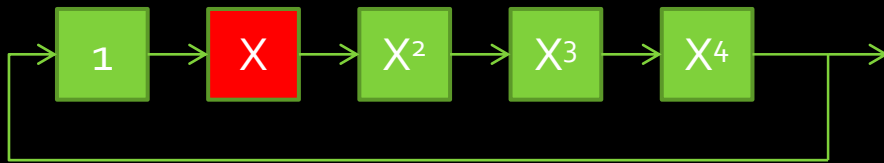
MESSAGE = 01001101.01000101.01010011.01010011.01000001.01000111.01000101

SECRETS = 01010011.01000101.01000011.01010010.01000101.01010100.01010011

Résultat = 00011110.00000000.00010000.00000001.00000100.00010011.00010110

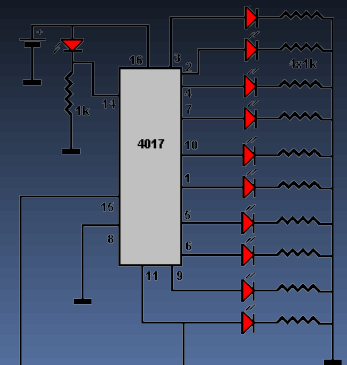
Chiffrements numériques

Construction de clefs aléatoires : Chenillard aléatoire



A chaque itération, la case allumée se déplace vers la droite.
Cela correspond à une multiplication par X.
Pour revenir au départ, on pose $X^5 = 1$.

On peut compliquer en rajoutant des connexions de type XOR.
Cela devient un chenillard qui clignote n'importe comment ou presque...



Chiffrements numériques

- Il existe des chiffrements particuliers :
 - Il y a deux clefs différentes (au lieu d'une seule) :
 - Une clé pour chiffrer (publique : on peut la donner à tout le monde)
 - Une clé pour déchiffrer (privée : on la garde secrète)
- Exemple : RSA (vu en terminale)
 - Basé sur la difficulté de décomposition en nombres premiers
 - Il faut calculer des inverses dans $\mathbb{Z}/n\mathbb{Z}$ et des puissances
 - La clé publique est un entier n et un autre nombre
 - La clé privée est liée à la connaissance de la décomposition de n en nombres premiers.

Crypto dans la vie de tous les jours : où la trouve-t-on?

- Les cartes à puces
- Les distributeurs de billets
- Les téléphones mobiles

- Le commerce électronique
- Les réseaux informatiques, le wifi, ...
- Les données sécurisées : Disque dur protégé, ...

- Les numéros de série : certains mais pas tous!

Distributeur Billets



Validation
Transaction



Message
+ chiffré

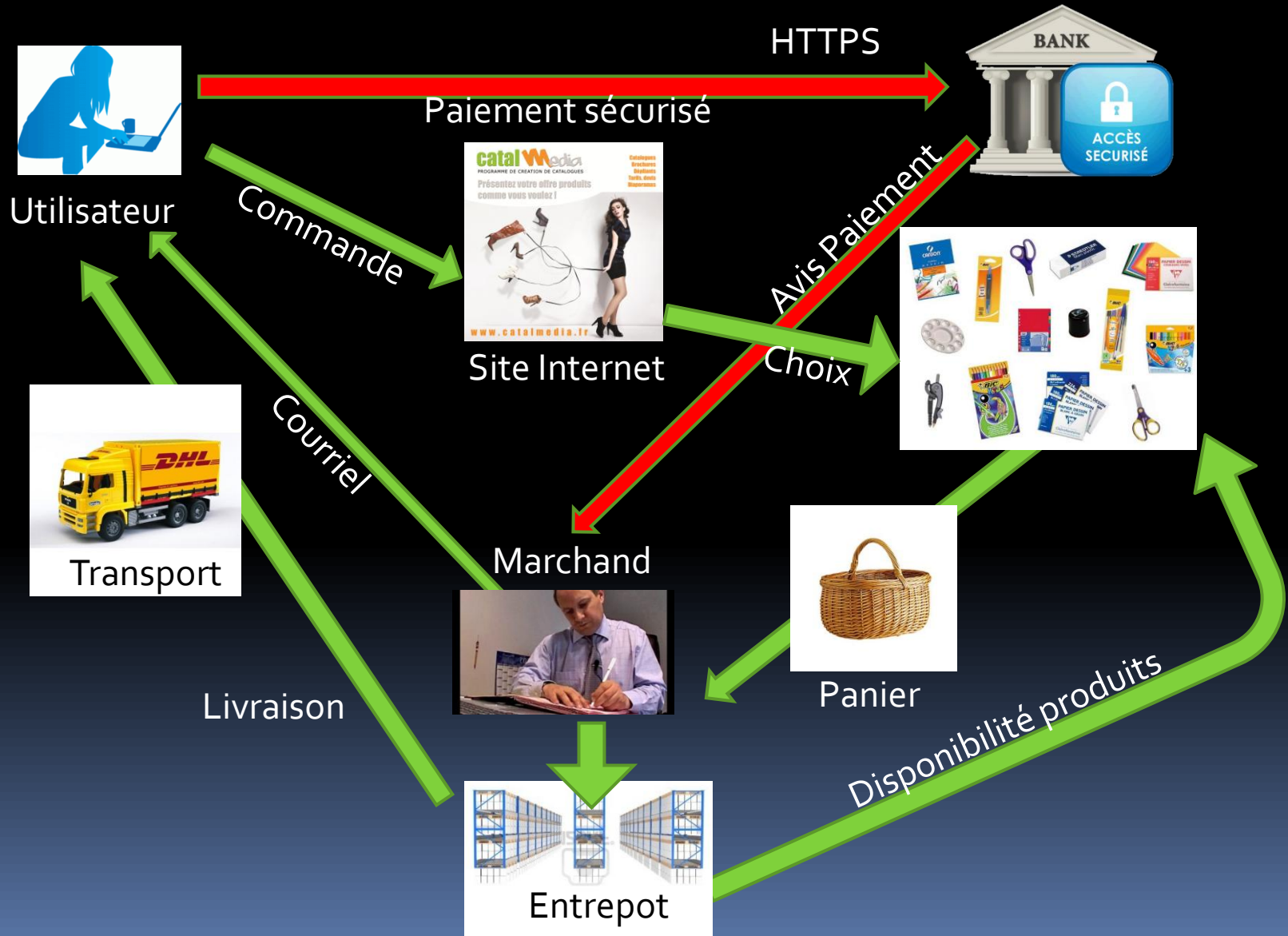
Preuve scellée
Facturette



PIN



Commerce électronique






Utilisation de « certificats »

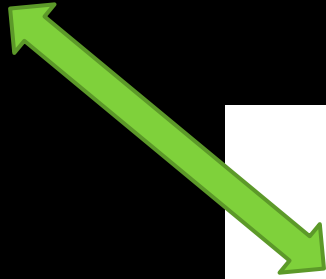
- Ce sont des éléments de sécurité qui contiennent un ensemble de clés préinstallées. Les grandes enseignes de commerce (Ebay, Paypal, Amazon, ...) sont ainsi connues de votre navigateur WEB.
- Cela permet de reconnaître si le site distant est bien celui voulu (Authentification).
- Une liaison sécurisée (Apparition d'un Cadenas) est établie (chiffrement des données transmises)



Authentification

- On cherche à prouver que l'on connaît le secret (la clef) sans la dévoiler
 - Pour cela, on chiffre un message aléatoire
 - Si le chiffré fourni correspond à celui calculé avec la clef secrète c'est que l'interlocuteur connaît aussi le secret.
- 

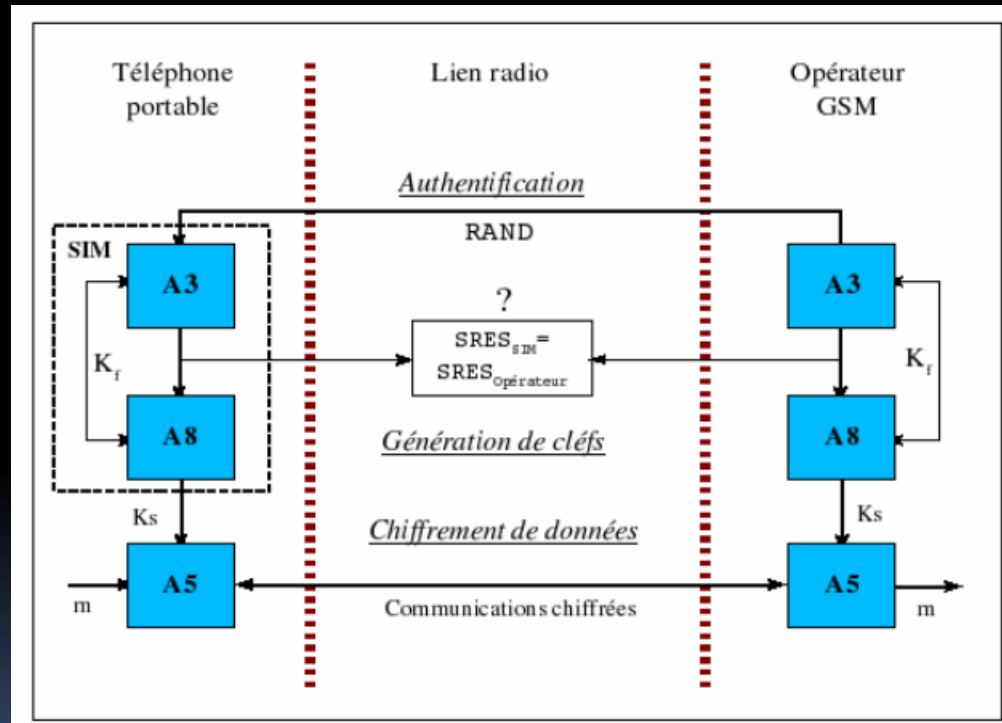
Téléphone mobile



Cryptographie et GSM

- Le téléphone doit « reconnaître » son propriétaire : pour l'instant, on lui demande de rentrer un mot de passe (le PIN)
- Le réseau téléphonique doit reconnaître si le client est bien membre de son réseau (Orange, SFR, Bouygues, Free, ...)
- Les communications sont chiffrées jusqu'à l'antenne relais.

Algorithmes téléphonie GSM




Trois phases

Une session de communication par GSM passe par trois phases : l'authentification, la génération de clés de session et le chiffrement de données échangées.

- Au niveau de l'accès au réseau, l'authentification est basée sur la SIM et est réalisée de la manière suivante.
 - Chaque SIM contient une clé secrète K_f , le « réseau » retrouvant K_f à l'aide d'une clé mère K_m et des données d'identification de la SIM (ex.: numéro de série, etc.)
 - Le « réseau » envoie un challenge RAND (un nombre aléatoire de 128 bits). A la réception de RAND, la SIM calcule la réponse SRES sur 32 bits obtenue en appliquant un algorithme cryptographique appelé A3 (implémenté dans la SIM) au challenge RAND, avec la clé secrète K_f .
 - Le réseau vérifie que la réponse SRES envoyée par la SIM correspond bien au challenge précédemment envoyé; l'authentification de la SIM est valide si tel est le cas, sinon l'authentification a échoué.
- La sécurité des communications est obtenue en chiffrant les échanges entre le téléphone portable et le réseau.
 - Ce chiffrement nécessite la génération d'une clé de session K_s de 64 bits. Cette clé obtenue par la deuxième phase (génération de clés) en appliquant un algorithme appelé A8 (implémenté dans la SIM) au challenge précédant RAND, avec une clé K_f .
 - Une fois la clé de session générée par la SIM, elle est fournie au téléphone portable qui va chiffrer les communications (troisième phase) à l'aide de l'algorithme cryptographique A5.



Nombres aléatoires omniprésents


- Besoin de nombres aléatoires pour
 - Clefs secrètes
 - Engagements aléatoires
 - Le chiffré ne doit pas avoir de propriétés statistiques et doit ressembler à une suite aléatoire
- 

Théories mathématiques à la base de la cryptographie

- On cherche une méthode pas compliquée pour chiffrer et compliquée pour déchiffrer
- Compliquée pour déchiffrer si on n'a pas la connaissance d'un petit secret (clef ou autre)
- On suppose que la méthode est connue ou peut le devenir : la sécurité ne doit pas être basée sur le secret de la méthode (Principe de Kerckhoffs)
- On essaie de « prouver » la sécurité : on se raccroche donc à des problèmes connus pour être difficiles (donc souvent en mathématiques....)



Métier

- Connaître les spécificités de chaque chiffrement (avantages/inconvénients)
 - Inventer de nouveaux chiffrements
 - Les tester, démontrer leur robustesse
 - Les mettre en œuvre
 - Valider leur mise en œuvre et leur intégration dans des systèmes plus complexes
- 

Métiers et des débouchés qui suivent ce type d'étude


- Les cryptanalystes sont très souvent au travail pour des gouvernements, des firmes d'antivirus/produits de sécurité, ou compagnies informatisées.
- **Métiers** : Ingénieur cryptologue, ingénieur d'études et développement de logiciels sécurisés, ingénieur R&D en sécurité et cryptologie, consultant sécurité, chef de projet sécurité...
- **Secteurs d'activité** : industrie des cartes à puce, des télécommunications, des équipements réseaux, éditeurs de solutions de protection de documents multimédia, sociétés de conseil en hautes technologies, éditeurs de logiciels, établissements publics (Ministère de la Défense),...

Labo de cryptographie à la fac


- Frontière entre les mathématiques, l'électronique et l'informatique
- Niveau Master (Bac +4) : c'est loin...
- Site Internet : www.cryptis.fr

www.cryptis.fr

DEVENEZ
EXPERT
EN SÉCURITÉ DE
L'INFORMATION
CRYPTIS



Sécurité de l'information à Limoges

- Cryptographie
 - Code correcteurs d'erreurs : codage de canal
 - Copyright
 - Watermarking : marquage de support numérique avec une « encre » invisible.
 - Sécurité Informatique et réseaux
 - Cartes à puce et systèmes embarqués
- 



Séance de travaux pratiques

- César et Vigenère avec Excel
 - Utilisation des fonctions :
 - CHAR, ORD, MOD
 - Logiciel spécialisé Cryptool
- 