

Introduction à la cryptographie

**Pierre-Alain Fouque
Université Rennes 1 et
Institut Universitaire de France (IUF)**

Pierre-Alain.Fouque@ens.fr

Introduction

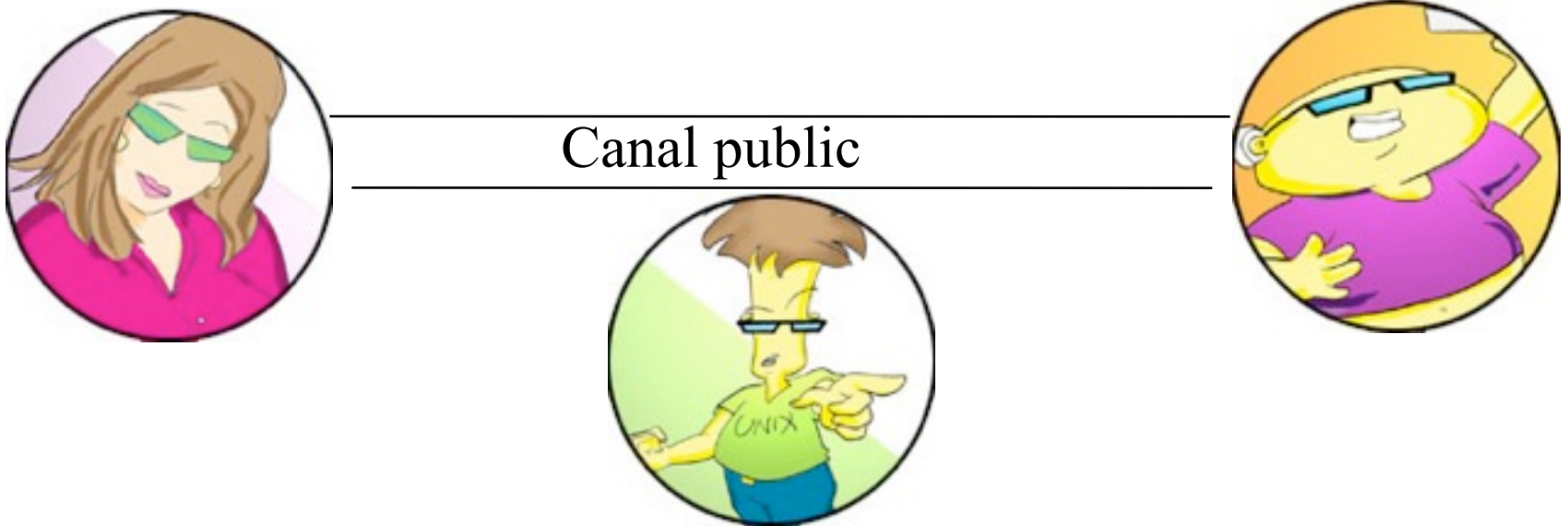
- Introduction à la cryptographie

Objectifs de la cryptographie

But : Assurer la sécurité des communications transmises sur un canal public en présence d'adversaires

Adversaire passif : Écoute les communications

Adversaire actif : capable d'écrire, modifier et effacer des informations passant sur le canal de communication



- Introduction à la cryptographie

Services de sécurité

- Confidentialité : Garantir que le contenu d'une communication ou d'un fichier n'est pas accessible aux tiers (GSM, Internet)
 - ✓ Mécanismes cryptographiques : Chiffrement
- Intégrité : Garantir que le contenu d'une communication ou d'un fichier n'a pas été modifié
 - ✓ Mécanismes cryptographiques : signature, MAC
- Authentification : Garantir l'identité d'une entité (*identification*) ou l'origine d'une communication ou d'un fichier (*authentification de données*)
 - ✓ Mécanismes cryptographiques : signature, MAC
 - Non-répudiation (**signature**) : le signataire ne peut pas renier sa signature

Repères historiques

- **Age artisanal:** (→ 1900)
 - César : chaque lettre est remplacée par celle située trois positions plus loin dans l'alphabet
 - Systèmes de substitutions et de permutations basiques
- **Age technique:** (1900 → 1970)
 - Substitutions et permutations utilisant des machines mécaniques ou électro-mécaniques: Hagelin, Enigma (2ème guerre mondiale)

Repères historiques (2)

- Age paradoxal (depuis 30 ans):

Nouveaux mécanismes répondant à des questions *a priori* hors d'atteinte

- Comment assurer un service de confidentialité sans avoir établi une convention secrète commune sur un canal qui peut être écouté par un attaquant ?
- Comment assurer un service d'authenticité – basé sur la possession d'un secret – sans révéler la moindre information sur le secret ?

Cryptographie et Cryptanalyse

La cryptologie se partage en deux sous-disciplines:

- la *cryptographie* propose des méthodes pour assurer les services précédents
- la *cryptanalyse* recherche des failles dans les mécanismes proposés

Cryptologie: Science aujourd'hui à mi-chemin entre les *mathématiques* et *l'informatique*

Généralités

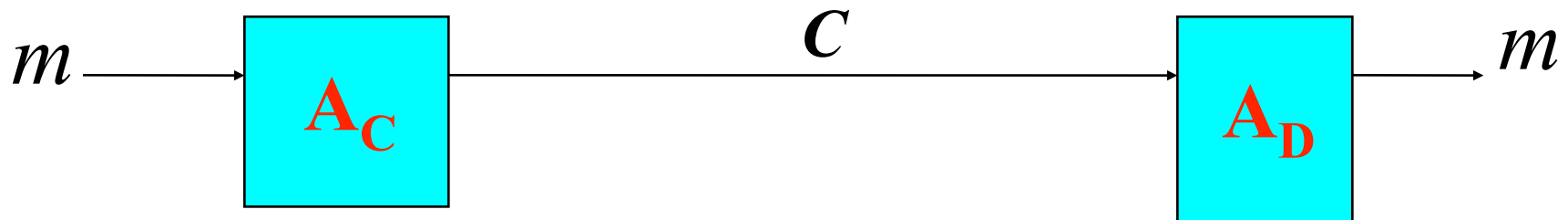
Cryptographie à clé secrète
vs.
Cryptographie à clé publique

- Introduction à la cryptographie

Principe du chiffrement

Algorithme de chiffrement, A_C

Algorithme de déchiffrement, A_D



Sécurité (confidentialité): impossible de retrouver le clair m à partir du chiffré c seul

Principes de Kerckhoffs

Notion de clé

En 1883, Kerckhoffs énonce plusieurs principes dont:

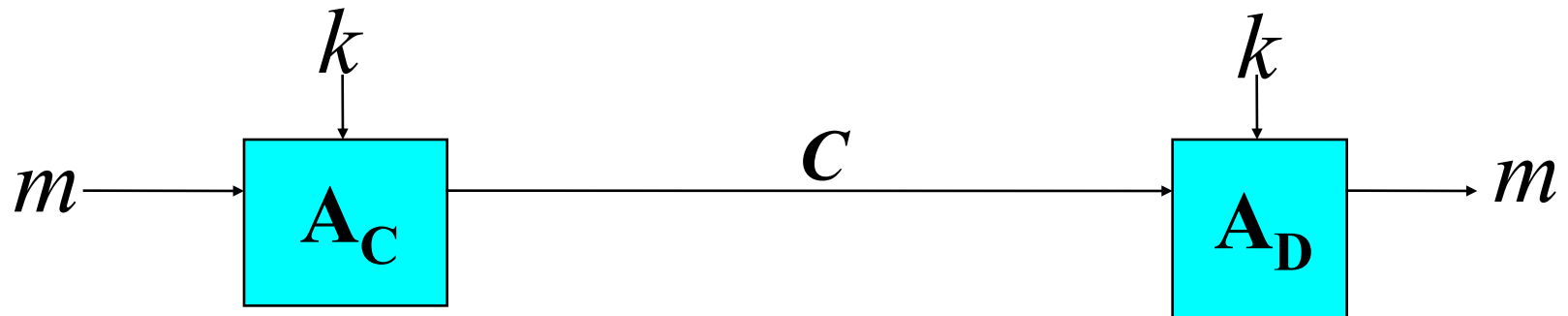
« la sécurité d'un système ne doit pas être fondée sur son caractère secret »

« seule une donnée de petite taille (clé) doit assurer la sécurité »

Chiffrement symétrique

Algorithme de chiffrement, A_C

Algorithme de déchiffrement, A_D



Sécurité: impossible de retrouver m à partir de c
sans k

Exemples de primitives: DES, AES

Problème de la cryptographie à clé secrète

Ne pas utiliser la même clé trop longtemps

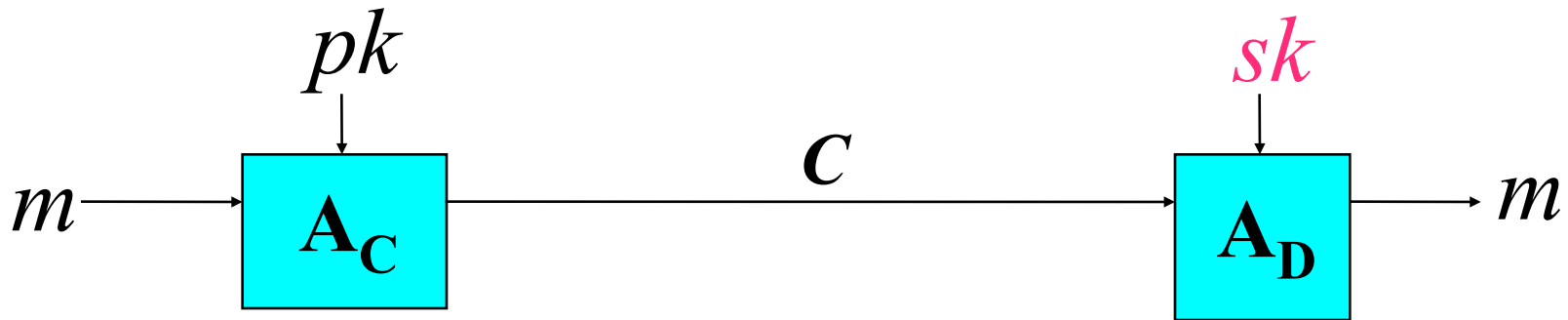
⇒ Problème de l'échange de clé

Transmission d'une nouvelle clé oblige les deux parties à se rencontrer

Chiffrement asymétrique (Diffie-Hellman / 1976)

Algorithme de chiffrement, A_C

Algorithme de déchiffrement, A_D



Sécurité: impossible de retrouver m à partir de c
sans sk connaissant pk

Exemples de primitives: RSA, ElGamal

Temps de calcul

- Combien d'opérations peut effectuer un ou plusieurs ordinateurs en un temps fini ?
- Un ordinateur cadencé à 1Ghz peut effectuer en 1 seconde 2^{30} opérations élémentaires
- $2^{90} = 10^{27} = 4 \cdot 10^{11}$ années à 1Ghz = nombre d'opérations qu'aurait pu effectuer un ordinateur depuis le début de l'univers
- On estime que l'on peut effectuer 2^{64} opérations, mais que 2^{80} et *a fortiori* 2^{128} opérations ne sont pas atteignables en temps raisonnable (moins de 100 ans)

Niveau de sécurité

- 2^{80} opérations représente aujourd'hui un *niveau fort de sécurité*
- Suivant les applications, on préférera 2^{128}
- Une clé est une suite aléatoire de bits (0 ou 1)
- *Clé symétrique*: la taille des clés est aujourd'hui de **128 bits**
- *Clé asymétrique*: la taille des clés est aujourd'hui de **1536 bits** (modules RSA)
- Problème pratique: Plus la taille des clés augmente, plus les algorithmes sont lents surtout en cryptographie asymétrique

Systemes cryptographiques

- Introduction à la cryptographie

Primitives de la cryptographie

(Briques de base pour concevoir des systèmes cryptographiques)

- Introduction à la cryptographie

One-Time Pad et chiffrement par flot

Chiffrement: $c = k + m$ avec $+$ le ou-exclusif

Déchiffrement: $m = c + k$

Sécurité Parfaite: même si l'adversaire a une puissance de calcul infinie, il ne pourra obtenir aucune information sur le message clair

Inconvénients:

- 1) Clé aussi longue que le message
- 2) Changer de clé pour chaque message

En pratique, Chiffrement par flot pour générer k à partir d'une petite clé.

Systemes de chiffrement

- Cryptographie à **clé secrète (conventionnelle)**
 - Système de chiffrement par flot (**stream cipher**)
 - Système de chiffrement par bloc (**block cipher**)
- Cryptographie à **clé publique**
 - Système de chiffrement par bloc
- Construction de **schémas de chiffrement** pour garantir la **confidentialité**

Data Encryption Standard (DES)

Algorithme de chiffrement symétrique par bloc

- Clé de 56 bits (2^{56} clés différentes)
- Bloc de taille 64 bits
- En 1977, 2^{56} représente un nombre de chiffrement très grand
- Aujourd'hui, longueur de clé trop petite car on peut effectuer 2^{56} chiffrement DES en 2 jours
- 3DES pour éviter une partie de ces problèmes...

Advanced Encryption Standard (AES)

Algorithme de chiffrement symétrique par bloc

- Clé de 128, 192 ou 256 bits (2^{128} , 2^{192} , 2^{256} clés différentes)
- Bloc de taille 128 bits
- En 2000, 2^{128} représente un nombre de chiffrement gigantesque et hors d'atteinte

Rivest, Shamir et Adleman (RSA)

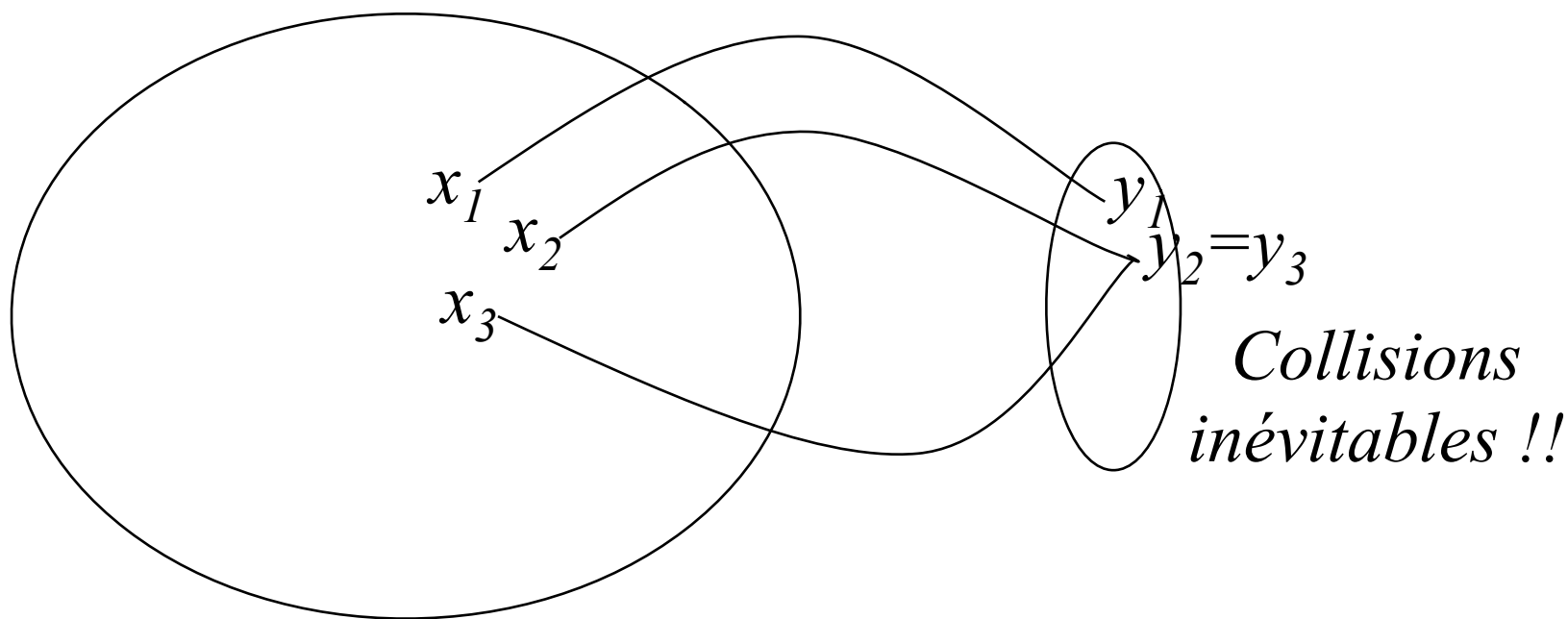
Algorithme de chiffrement asymétrique par bloc

- Clé de 1024 bits (niveau de sécurité en 2^{80})
- Bloc de taille 890 bits
- Si $N=pq$, il existe e et d tels que pour tout $x < N$,
$$x^{ed} = x \bmod N$$
- A partir de $c < N$, calculer x t.q. $c = x^e \bmod N$, est un problème apparemment difficile sans la connaissance de d (la trappe dans RSA)

Fonctions de hachage

Définition : Produisent une empreinte du message (haché du message) de petite taille à partir d'un message m arbitrairement grand

Exemples : SHA-1 (160 bits) ou MD5 (128 bits)



Sécurité des fonctions de hachage

Résistance aux collisions :

Il est difficile de trouver x et x' tq $H(x) = H(x')$

Résistance à un deuxième antécédent :

Connaissant $H(x)$ et x trouver $x' \neq x$ et $H(x) = H(x')$

Paradoxe des anniversaires : Si D est la taille de l'ensemble d'arrivée, on trouve des collisions avec $pr > 1/2$ en essayant $\sqrt{D}$ valeurs aléatoires

Niveau de sécurité : 2^{80} pour SHA-1

Mécanismes cryptographiques

- Introduction à la cryptographie

Garantir la confidentialité
=
Système de chiffrement

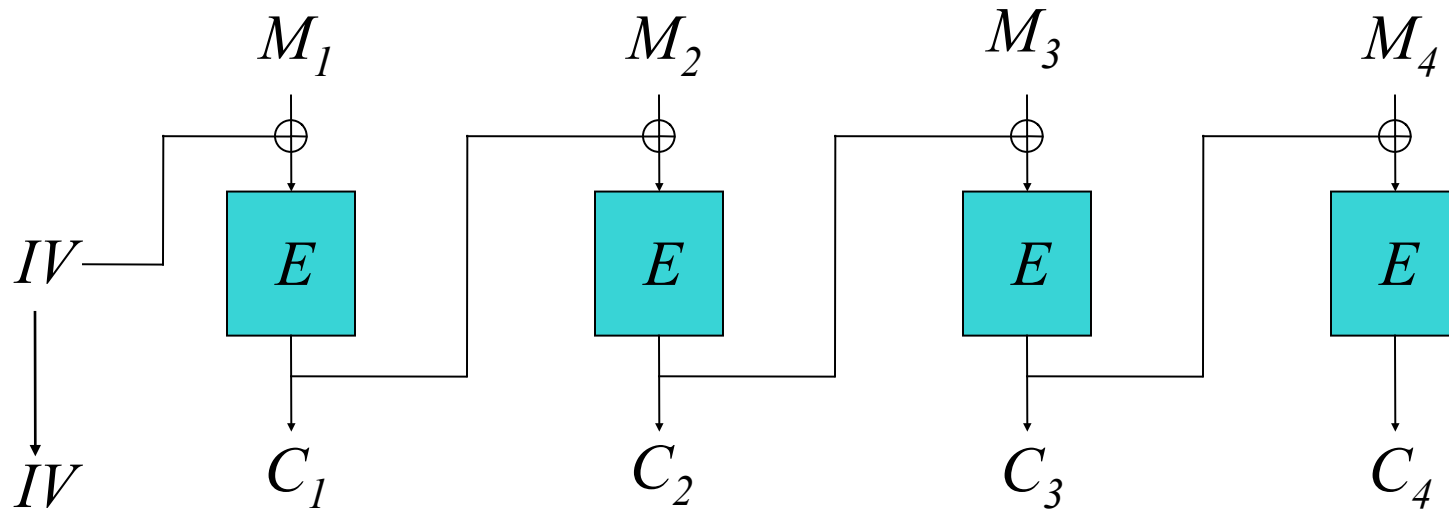
- Introduction à la cryptographie

Modes opératoires

**Comment chiffrer de longs messages avec un
algorithme de chiffrement par bloc ?**

- Introduction à la cryptographie

Cipher Block Chaining (CBC)



- $C_i = E_k (M_i \oplus C_{i-1})$
- $M_i = D_k (C_i) \oplus C_{i-1}$
- $C = (IV, C_1, C_2, C_3, \dots, C_i)$
- Désavantage : Non parallélisable
- Avantage : Auto-synchronisant

Schéma d'encapsulation (padding) pour RSA

**Comment chiffrer efficacement et de manière
sûre avec RSA ?**

Paddings de RSA

- RSA est *déterministe* : le chiffrement d'un même message produit le même chiffré

Utilisation d'*aléa* pour masquer l'information chiffrée

- Si les messages chiffrés sont *trop petits*, il est facile d'inverser la fonction RSA
 - Utilisation de *bits de bourrage* (padding) pour toujours chiffrer des messages suffisamment longs
- Certains paddings ont été cassés (PKCS#1 dans SSL)
- Le nouveau padding PKCS#1 v2 est prouvé sûr

Schéma hybride

**Comment chiffrer efficacement de longs messages
sans avoir de clé en commun ?**

- Introduction à la cryptographie

Avantage / inconvénient des systèmes symétriques et asymétriques

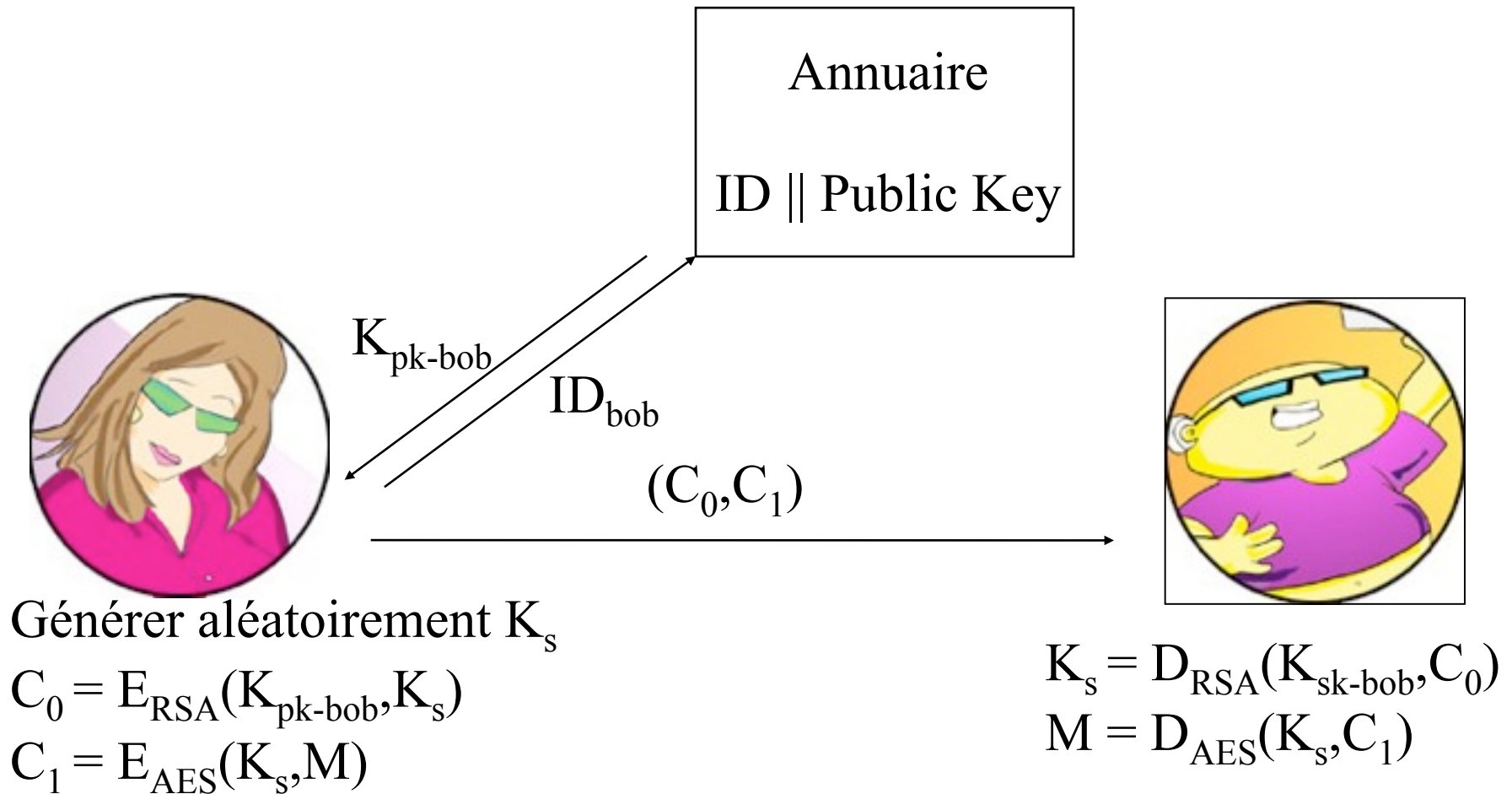
Clé asymétrique:

- **Avantages:**
 - Gestion des clés (seule la clé secrète doit le rester), (n clés)
 - Non-répudiation
- **Inconvénients:**
 - Lenteur (100 fois plus lent, dépend de la taille de du module)
 - Charge machine importante

Clé symétrique:

- **Avantages:**
 - Rapidité (soft qq 10Mo/s, hard qq 100Mo/s)
 - Clés très courtes
 - Peu gourmand en ressources machines
- **Inconvénients:**
 - Gestion des clés (n^2)
 - Échange préalable à toute comm.
 - Pas de non-répudiation

Tirer avantage de la cryptographie symétrique et asymétrique



- Introduction à la cryptographie

Une science rigoureuse

- 3 étapes en cryptographie:
 1. Spécifier précisément le **modèle de sécurité (menace)**
 2. Proposer une **construction**
 3. **Prouver que casser la construction dans le modèle de sécurité** se ramène à résoudre un problème difficile (réduction)

Quelques exemples historiques (tous cassés ...)

- Chiffrement par Substitution
- Chiffrement de César (décalage)
 - quelle est la lettre la plus fréquente en français ?

Vigenère

- **Chiffrement polyalphabétique**: éviter de toujours chiffrer avec la même lettre

	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

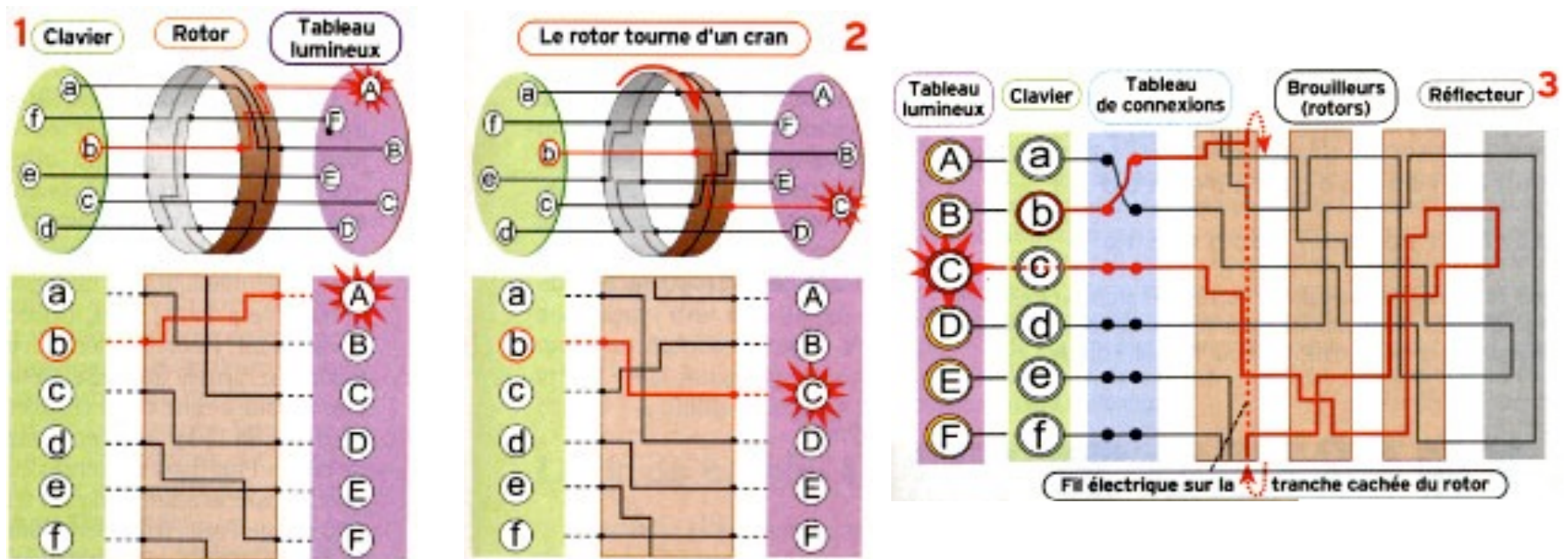
Key: ABCDABCDABCDABCDABCDABCDABCD

Plaintext: **CRYPTO**ISSHORTFOR**CRYPTO**GRAPHY

Ciphertext: **CSASTP**KVSIQUTGQU**CSASTP**IUAQJB

Pouvez-vous le déchiffrer ?

Rotor machines (1870-1943)



- #keys enigma = $10^{16} \approx 2^{53}$
- Today:
 - #keys DES = 2^{56}
 - #keys AES = 2^{128}

Probabilité Discrète

- U : ensemble fini (e.g. $U = \{0, 1\}^n$)
- Prob. distr. P sur U est une fonction $P: U \rightarrow [0, 1]$ t.q. $\sum_{x \in U} P(x) \in [0, 1]$
- $A \subseteq U$ un événement et $\Pr[A] = \sum_{x \in A} P(x)$
- A variable aléatoire est une fonction $X: U \rightarrow V$
- X prend ses valeurs dans V et définit une distribution sur V : $\Pr[X=b] = \sum_{a: X(a)=b} P(a)$

Indépendance de variables aléatoires

- Def: A et B deux événements sont **indépendant** si
 - $\Pr[A \text{ et } B] = \Pr[A].\Pr[B]$
- Deux variables aléatoires X, Y à valeurs dans V sont indépendante si $\forall a, b \in V, \Pr[X=a \text{ et } Y=b] = \Pr[X=a].\Pr[Y=b]$
- Exemple: $U = \{0, 1\}^2 = \{00, 01, 10, 11\}$ et $r \leftarrow_R U$, définissons $X = \text{lsb}(r)$ et $Y = \text{msb}(r)$ $\Pr[X=0 \text{ and } Y=0] = ?$

Conclusion

- La cryptographie est la science du secret
- Elle permet de résoudre certains problèmes dû à la forme électronique des documents
- Les services de sécurité garantis sont :
 - la *confidentialité*,
 - l'*intégrité*, et
 - l'*authentification de document et de personne*

Bibliographie

- Livres:
 - La Guerre des Codes (David Kahn)
 - Histoire des Codes Secrets (Simon Singh)
 - La Science du Secret (Jacques Stern)
 - Cryptographie Appliquée (Bruce Schneier)
 - Cryptographie: Théorie et Pratique (Stinson)
- Pointeurs internet
 - Handbook of Applied Cryptography
www.cacr.math.uwaterloo.ca/hac