Introduction à la cryptographie

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

Pierre-Alain.Fouque@ens.fr

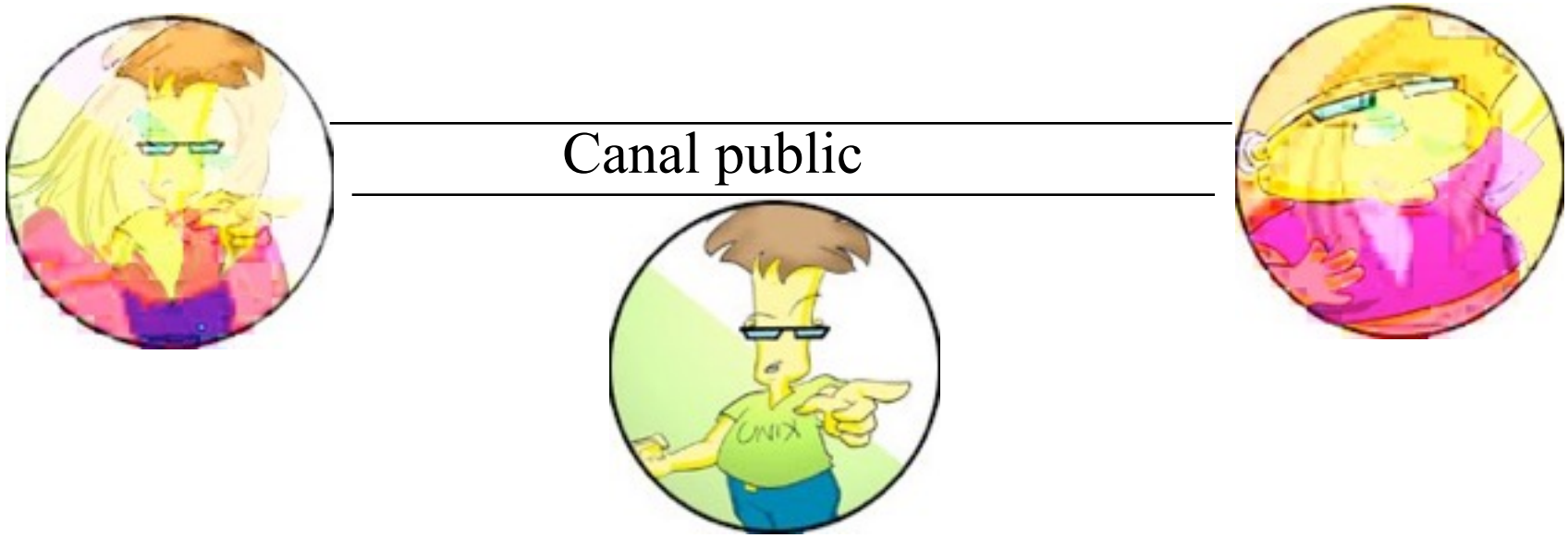
Introduction

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



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*

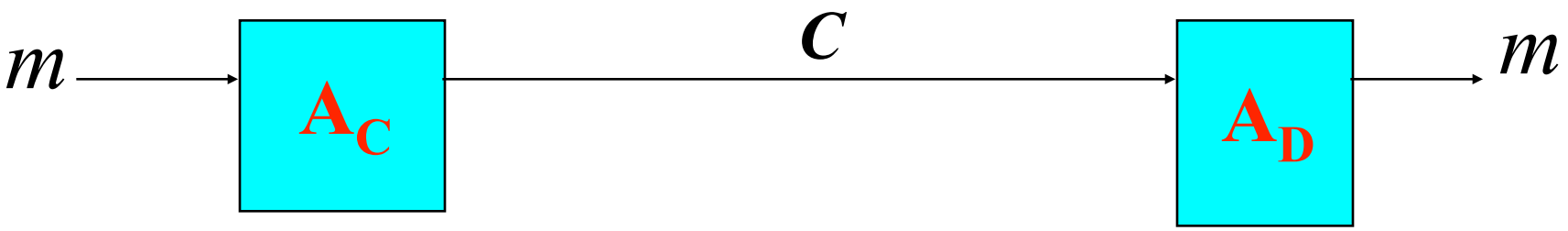
Généralités

Cryptographie à clé secrète
vs.
Cryptographie à clé publique

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:

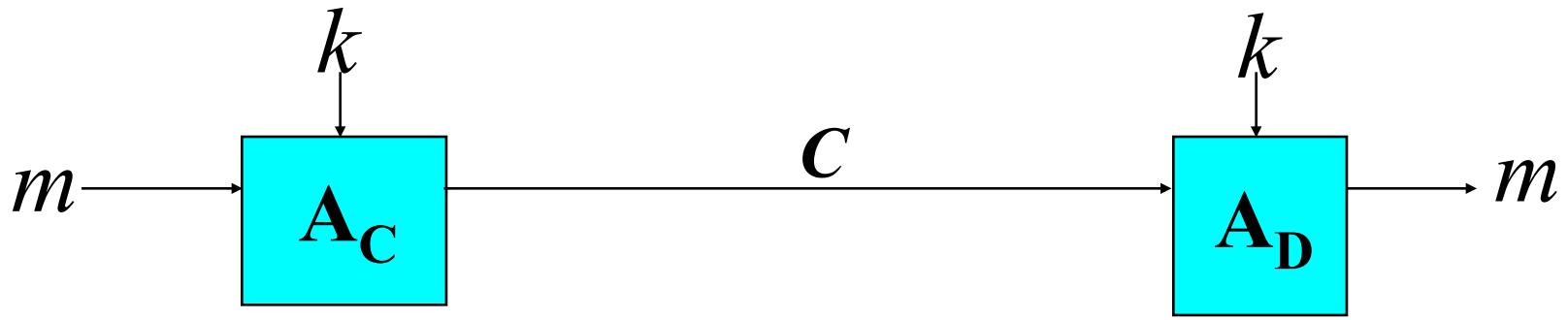
« *la sécurité d'un système ne doit pas être fondée sur son caractère secret* »

« *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

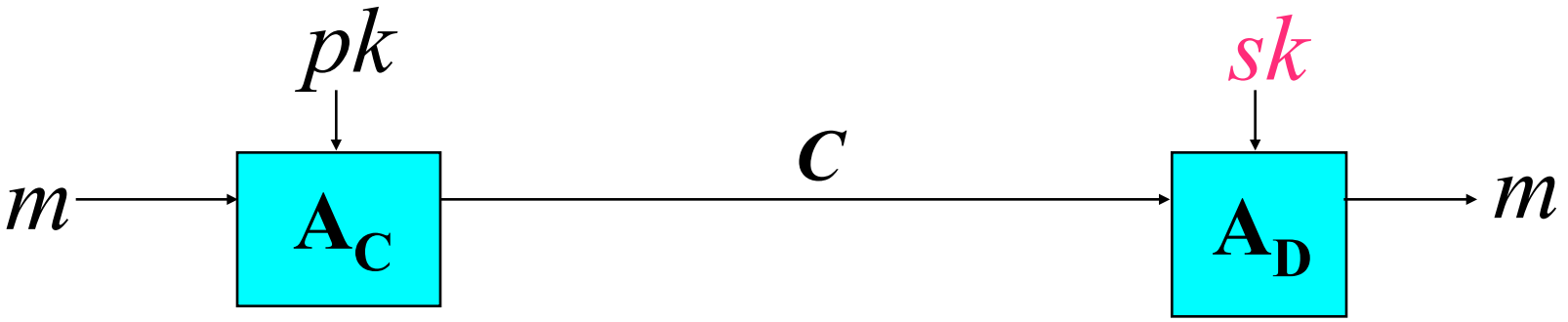
⇒ Problème de l'échange de clé

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 s*k* *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
- $2^{90}=10^{27}=4.10^{11}$ 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^{128} opérations représente aujourd'hui un niveau *fort* de sécurité
- Suivant les applications, on préfèrera 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 pour RSA et 256 bits pour les courbes elliptiques
- Problème pratique: Plus la taille des clés augmente, plus les algorithmes sont lents surtout en cryptographie asymétrique

Schéma hybride

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

Avantage / inconvénient des systèmes symétriques et asymétriques

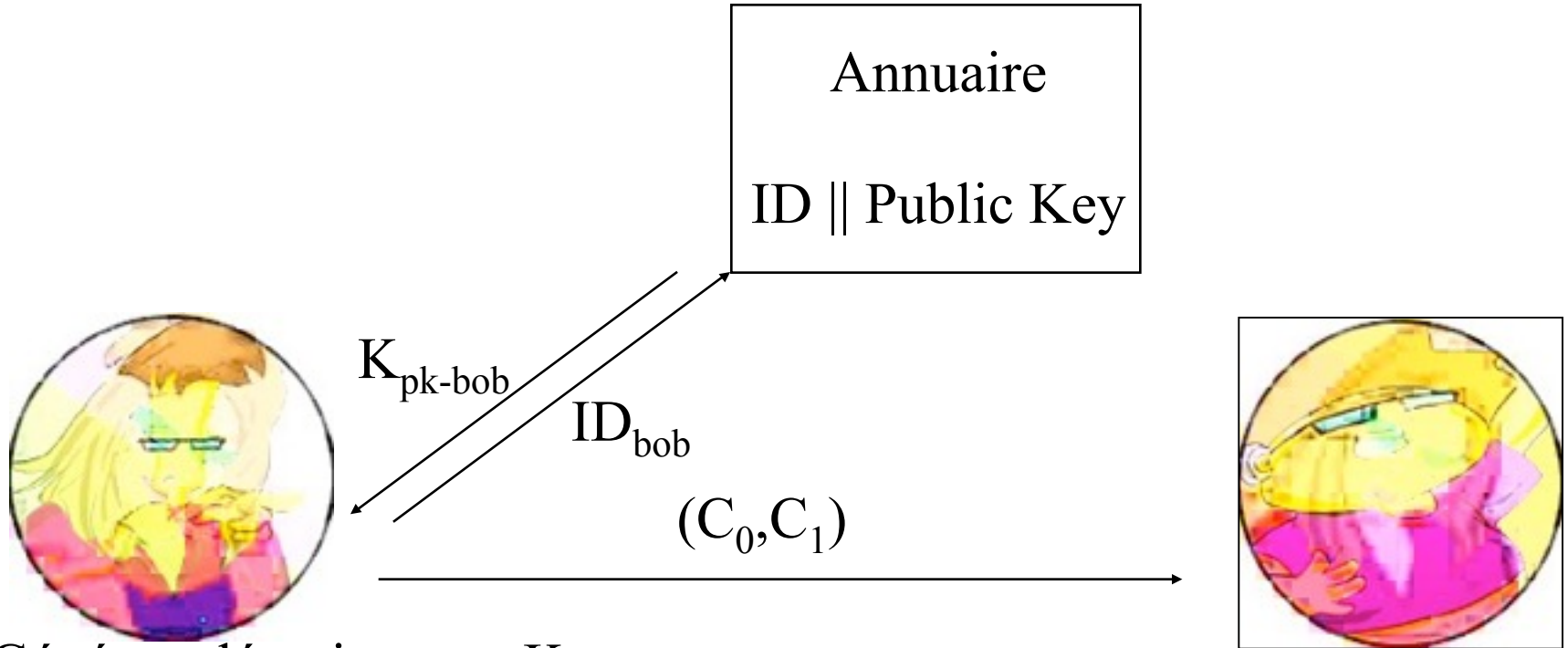
Clé asymétrique:

- 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



Générer aléatoirement K_s

$C_0 = E_{RSA}(K_{pk\text{-}bob},K_s)$

$C_1 = E_{AES}(K_s,M)$

$K_s = D_{RSA}(K_{sk\text{-}bob},C_0)$

$M = D_{AES}(K_s,C_1)$

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)

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=lsb(r) et Y=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