Comment sécuriser nos échanges de données ? Confidentialité et anonymat

David Pointcheval

Ecole normale supérieure, CNRS & INRIA CASCADE

Olympiades de mathématiques – Sorbonne – Paris
19 Juin 2009

Sommaire

Confidentialité des communications

On a toujours souhaité masquer le contenu de certaines communications

Alice

Bob

Alice

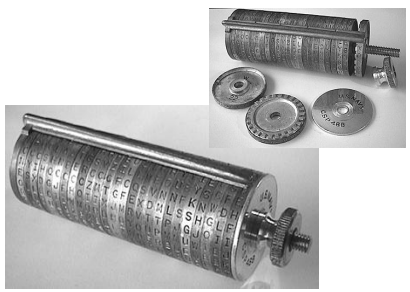
Avec le tout-numérique, l'espionnage a changé d'échelle
les besoins en sécurité se sont amplifiés et diversifiés

Méthodes anciennes

Scytale - Permutation

Substitutions et permutations
La **sécurité** repose
sur le secret du mécanisme

Cadran d'Alberti
Substitution mono-alphabétique



Cylindre – M 94 (CSP 488)
Substitution poly-alphabétique

Utilisation d'une clé (secrète)

Une information partagée (clé secrète) entre l'émetteur et le récepteur sert de paramètre au mécanisme de chiffrement :

- Vigenère : chaque lettre de la clé précise le décalage
- Enigma : les branchements et les rotors

La sécurité **semble** meilleure : mais cassé (Alan Turing *et al.*)

Confidentialité parfaite ?

Tout cela s'effondre sous des attaques statistiques !

Existe-t-il une méthode de chiffrement parfaitement sûre ?

Chiffrement de Vernam (1929)

- Chiffrement de $m \in \{0,1\}^n$ sous la clé $k \in \{0,1\}^n$:

$m =$	1 0 0 1 0 1 1	Message clair
	$\oplus$	Ou exclusif (+ modulo 2)
$k =$	1 1 0 1 0 0 0	Clé = Masque aléatoire
	=	
$c =$	0 1 0 0 0 1 1	Message chiffré

- Déchiffrement de $c \in \{0,1\}^n$ sous la clé $k \in \{0,1\}^n$:

$$c \oplus k = (m \oplus k) \oplus k = m \oplus (k \oplus k) = m$$

Théorie de l'information

Quel message est contenu dans le chiffré $c \in \{0,1\}^n$?
Pour tout candidat $m \in \{0,1\}^n$, la clé $k = c \oplus m$ conduit à c
$\Rightarrow$ aucune information sur m n'est contenue dans c !

Inconvénients

- La clé doit être aussi longue que le message
- Cette clé ne doit être utilisée qu'une fois (masque jetable)

Théorème (Shannon – 1949)

Pour s'échanger des messages avec confidentialité parfaite, A et B doivent partager une chaîne partaitement aléatoire et aussi longue que l'ensemble des informations à transmettre.

Ainsi, cette technique du masque jetable est optimale...

Confidentialité pratique

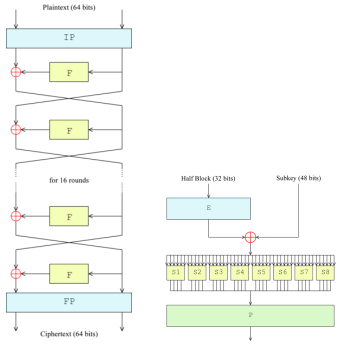
Confidentialité parfaite vs. confidentialité pratique

- Aucune information sur le clair m n'est contenue dans le chiffré c sans la connaissance de la clé k
  $\Rightarrow$ théorie de l'information
  Aucune information sur le clair ne peut être extraite du chiffré, même après un temps illimité, ou avec une puissance de calcul infinie : confidentialité parfaite
- En pratique : attaquant limité en temps/puissance
  $\Rightarrow$ théorie de la complexité

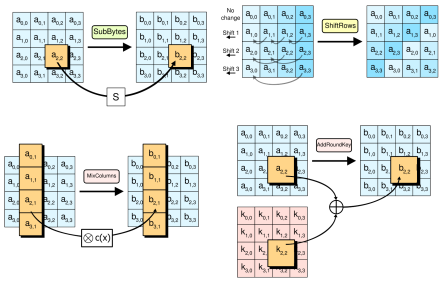
Shannon a aussi montré qu'une bonne combinaison de permutations et de substitutions permettait de rendre l'extraction d'information très complexe

Chiffrement symétrique : DES et AES

Combinaisons de substitutions et permutations



DES (1977)
Data Encryption Standard

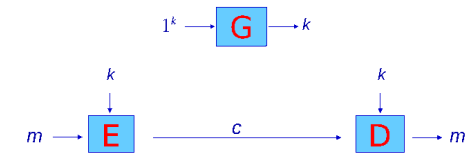


AES (2001)
Advanced Encryption Standard

Chiffrement symétrique : Formalisme

Chiffrement symétrique - chiffrement à clè secrète

Une seule clé secrète partagée entre Alice et Bob :
sert de paramètre commun au chiffrement et au déchiffrement
Cette clé secrète a un pouvoir symétrique



Le secret de la clé *k* garantit la confidentialité des échanges mais nécessite une clé secrète commune !

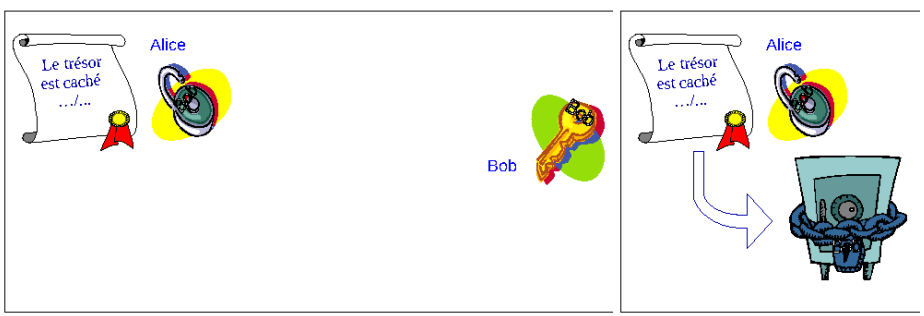
Comment établir ce secret commun initial ?
Ou comment s'en passer ?

Chiffrement asymétrique : Intuition

Confidentialité

- Seul le destinataire peut prendre connaissance du contenu
- Aucune contrainte sur l'émetteur

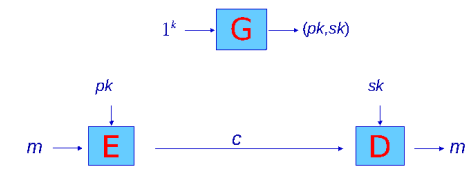
Pourquoi avoir besoin d'un secret pour chiffrer un message ?



Chiffrement asymétrique : Formalisme

Cryptographie à clé publique – Diffie-Hellman (1976)

- la clé publique de Bob sert de paramètre pour chiffrer les messages à destination de Bob
- sa clé privée lui sert à déchiffrer



Le secret de la clé privée *sk* garantit la confidentialité

Cryptographie moderne

Chiffrement asymétrique

Nous avons besoin d'une fonction publique f,
spécifique à Bob (le destinataire) : la clé publique de Bob

- Chiffrement de m : $m \mapsto c = f(m)$, calculable par tous
- Décryptement de c : $c = f(m) \mapsto m$, difficile pour tous
- Déchiffrement de c : $c \mapsto m = g(c)$, facile pour Bob

La fonction g doit exister, mais son calcul effectif doit nécessiter un secret : la clé privée de Bob

Est-ce possible ? ?

Fonctions à sens-unique

Fonction à sens-unique

Une (famille de) fonction f est dite à sens-unique si

- $x \longrightarrow y = f(x)$: facile à calculer
- $y \longrightarrow x$ tel que $y = f(x)$: difficile à calculer

Facile / Difficile à calculer ! !

Théorie de la complexité

- facile à calculer = algorithme polynomial
- difficile à calculer = pas d'algorithme polynomial

Fonctions à sens-unique : candidats

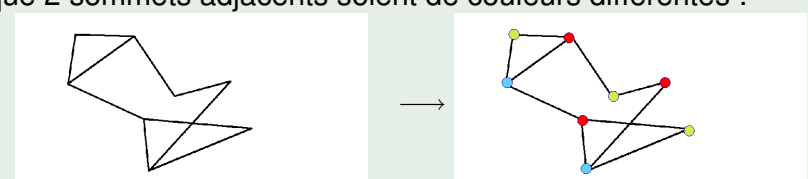
Problèmes $\mathcal{NP}$-Complets

Un problème $\mathcal{NP}$-complet est un problème pour lequel trouver un algorithme polynomial fournirait un algorithme polynomial pour tous les problèmes *vérifiables* en temps polynomial

$\Rightarrow$ très peu probable $\qquad \mathcal{P} \stackrel{?}{=} \mathcal{NP}$

Exemple (La 3-coloriabilité)

Colorier un graphe avec 3 couleurs, de telle manière que 2 sommets adjacents soient de couleurs différentes :



Fonctions à sens-unique

Problèmes $\mathcal{NP}$-Complets

- Pas d'algorithme efficace pour décider/résoudre
- Facile de générer un problème, en partant de la solution : $x \mapsto f(x)$
- Difficile de retrouver *une* solution : $y \mapsto x$ tel que $y = f(x)$

Exemples

Voyageur de commerce, Sac à dos, 3-Sat, ...

Inconvénients

- Existence d'instances difficiles à résoudre mais pas difficile en moyenne...
- Nécessite de très grandes tailles pour être difficile

Un peu de mathématiques...

Multiplication / Factorisation

- Multiplier 2 entiers premiers est facile
- Décomposer en facteurs premiers est difficile, surtout pour des entiers produits de 2 premiers de même taille : appelés modules RSA

Records

Année	1990	1994	1999	1999	2003	2005
Chiffres	116	129	140	155	174	200
Temps (1Ghz)	3 M	5 A	2 A	8 A	13 A	121 A

Recommandations : 310 chiffres, soit 1024 bits, minimum voire 617 chiffres, soit 2048 bits, pour être hors de portée.

Permutation à sens-unique à trappe

Permutation à sens-unique à trappe

Une (famille de) permutation f est dite à sens-unique si
$x \to y = f(x)$: facile $\quad y = f(x) \to x$: difficile
et à trappe, s'il existe une trappe g secrète (réciproque de f)
$y = f(x) \to x = g(y)$: facile à calculer

Chiffrement asymétrique

- Clés de Bob
  - Clé publique : fonction f
  - Clé privée : fonction g
- Algorithmes
  - Chiffrement pour Bob : $c = f(m)$, facile à calculer
  - Décryptement de c : $c \to m$: difficile à calculer
  - Déchiffrement par Bob : $m = g(c)$: facile à calculer

Plus de mathématiques...

RSA = Rivest-Shamir-Adleman – 1978

- Clés de Bob
  - Clé publique : $n = p \times q$, exposant e
  - Clé privée : p et q
- Algorithmes
  - Chiffrement pour Bob : $c = m^e \bmod n$
  - Décryptement de c : racine e-ième modulaire

    Difficile sans la factorisation du module
  - Déchiffrement par Bob : racine e-ième modulaire

    Facile avec la factorisation du module

Cryptographie asymétrique

Chiffrement = confidentialité de données

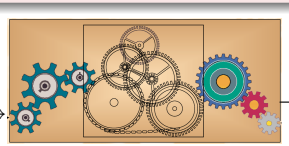
Nul ne peut apprendre un bit d'information sur m à la vue de c, même s'il a pu demander le déchiffrement de tout chiffré $c' \neq c$.

Signature = authentification de données

Nul ne peut générer une nouvelle signature valide, même s'il a pu demander les signatures de messages de son choix.

Sécurité prouvée

- Si un adversaire peut mettre en défaut ces notions
- Alors on peut résoudre un problème difficile sous-jacent

instance difficile →  → solution

Anonymat

Sécurité des communications

- Confidentialité des échanges
  Avoir la garantie que seul le destinataire va pouvoir prendre connaissance du contenu
- Authentification des personnes et des données
  Être sûr de l'identité de son interlocuteur et/ou de l'émetteur d'un message
- Anonymat
  Ne transmettre que les informations personnelles nécessaires et suffisantes

Contrôle d'accès

Pourquoi fournir son identité pour accéder à un service ?
Prouver que l'on a droit à cet accès est suffisant

- Clé publique associée au service : Instance difficile = y
- Information secrète x prouvant le droit d'accès, associée à mon identité Id, telle que $f(\mathrm{Id}, x) = y$

Propriété à sens-unique

Pour y fixé, pour tout Id, il existe x tel que $f(\mathrm{Id}, x) = y$

- pour l'autorité, qui connaît une trappe associée à y, pour tout Id, il est facile de calculer x tel que $f(\mathrm{Id}, x) = y$
- sans cette trappe, il est difficile de générer un nouveau couple (Id, x) valide

Exemple : RSA

n, e fixés $\quad m \mapsto m^e \bmod n$

RSA Flexible

Un module $n = p \times q$ est fixé :

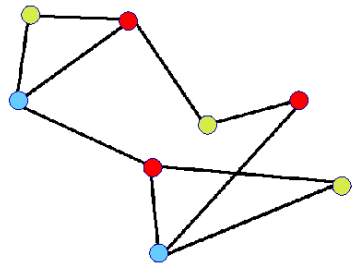
- $(m, e) \mapsto m^e \bmod n$ facile
- $c \mapsto (m, e)$, avec e premier, tel que $c = m^e \bmod n$ est difficile sans la factorisation de n
- $c \mapsto (m, e)$, facile avec la factorisation de n

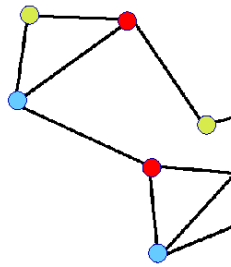
Id est encodée en e premier, et x est tel que $y = x^e \bmod n$

Peut-on prouver sa connaissance d'un secret (Id, x)
sans mettre ce secret en danger (anonymat) ?

Preuve Zero-Knowledge

Comment prouver que je connais ce 3-coloriage,
sans le révéler ?





Je choisis une permutation sur les couleurs
et l'applique aux sommets Je masque les sommets
et communique le tout au vérifieur Le vérifieur désigne une
arête (2 sommets adjacents), l'enlève les masques

Preuve Zero-Knowledge

Théorème

Ce protocole garantit que

- *si on ne connaît pas de solution, la probabilité d'être accepté après plusieurs itérations est négligeable*
- *le vérifieur n'apprend aucune information*

Applications

Ces preuves ont de nombreuses applications à l'anonymat :

- signature de groupe
- contrôle de droit d'accès anonyme
- vote électronique universellement vérifiable
- etc. . .

Conclusion

La cryptographie fait appel

- à la théorie de l'information
- à la théorie de la complexité
- à la théorie algorithmique des nombres

pour atteindre des objectifs *a priori* paradoxaux

- chiffrer publiquement pour un destinataire unique
- s'authentifier anonymement
- prouver que l'on sait, sans ne rien dire