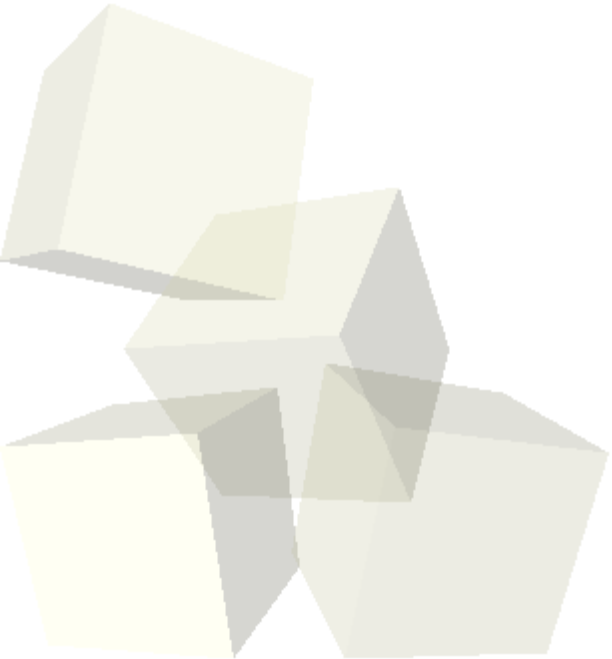


Cryptographie

Cours 3
Chiffrement asymétrique

Jérémy Briffaut
STI 2A

Plan

I. Histoire, définition et objectifs de la cryptographie
- Concepts et algorithmes de permutation et de substitution

II. Chiffrement Symétrique
- DES, 3DES, AES, IDEA

III. Chiffrement Asymétrique
- RSA, ElGamal

IV. Signature, Hachage et Scellement

V. Echange de clés
- Algorithme Deffie-Hellman

VI. Hachage : MD5, SHA-1, SHA-2

VII. Code d'Authentification & MAC

- **Cryptographie à clef publique / asymétrique**
  - Clefs de chiffrement et de déchiffrement distinctes
    - → Connaître la clef publique ne permet pas de retrouver la clef
    - → privée correspondante
  - Algorithmes trop lents pour une utilisation intensive (chiffrement de données)
    - → utilisés seulement pour l'échange de clef, la signature
  - Diffie & Hellman, 1976
  - RSA, 1978
  - Basée sur des problèmes difficiles à résoudre :
    - → logarithme discret
    - → factorisation de grands nombres

Les algorithmes asymétriques courants

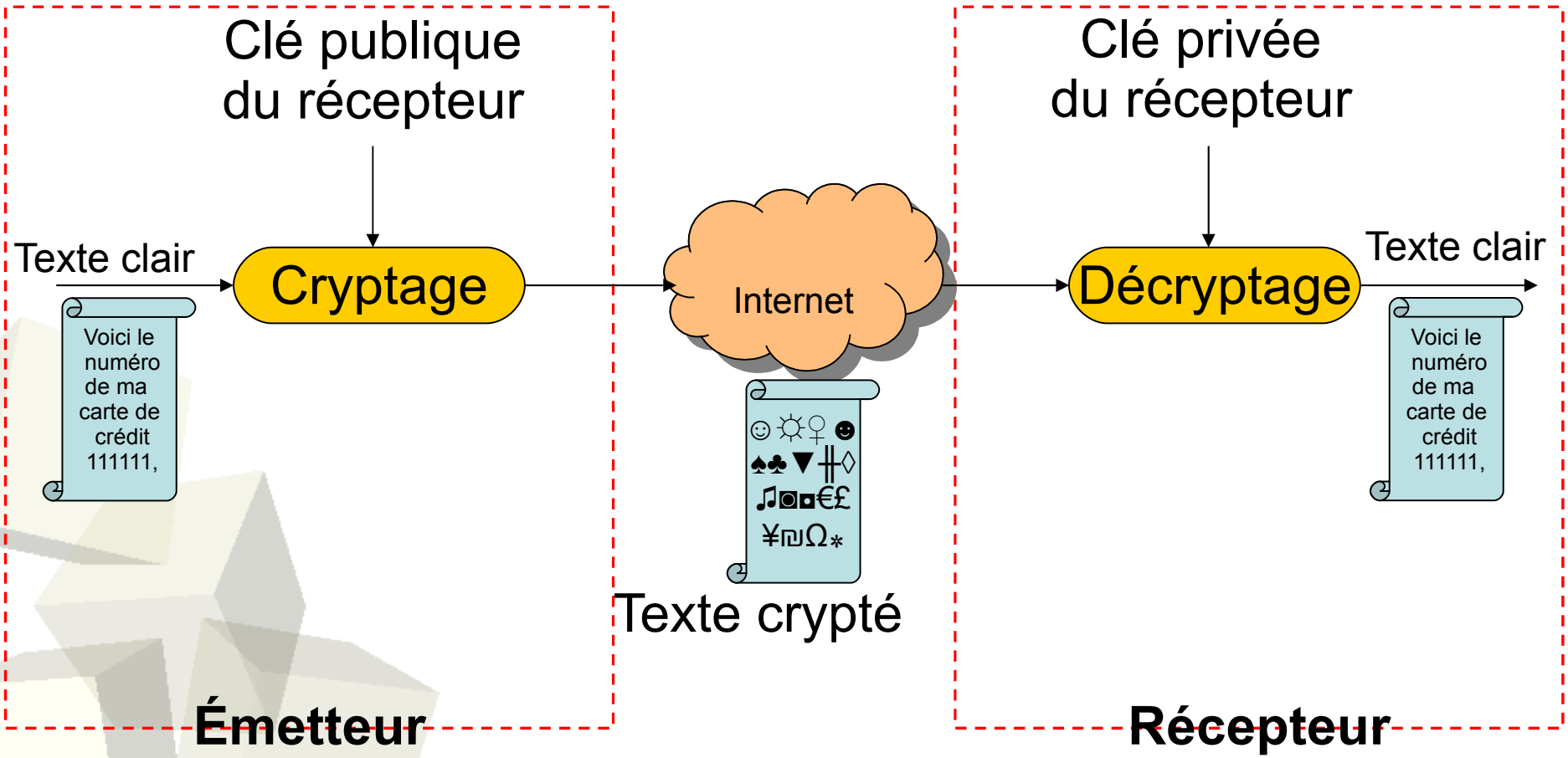
- *A clé publique (asymétrique)*
  - → On utilise une paire de clés
    - l'une **publique** qui chiffre le message, cette clé est inefficace pour le déchiffrer.
    - L'autre **privée** qui sert à décoder le texte.
- Ces techniques reposent sur des fonctions à sens uniques.

- Le plus connu **RSA** *(Ron Rivest,Adi Shamir et Leonard Adleman)*
  - → Particularité si l'une des deux clefs crypte les données, seule l'autre pourra décrypter le message.
  - → D'où un intérêt certain pour :
    - La *non-répudiation*
    - la *signature numérique*
  - → Basé sur la factorisation des grands nombres.

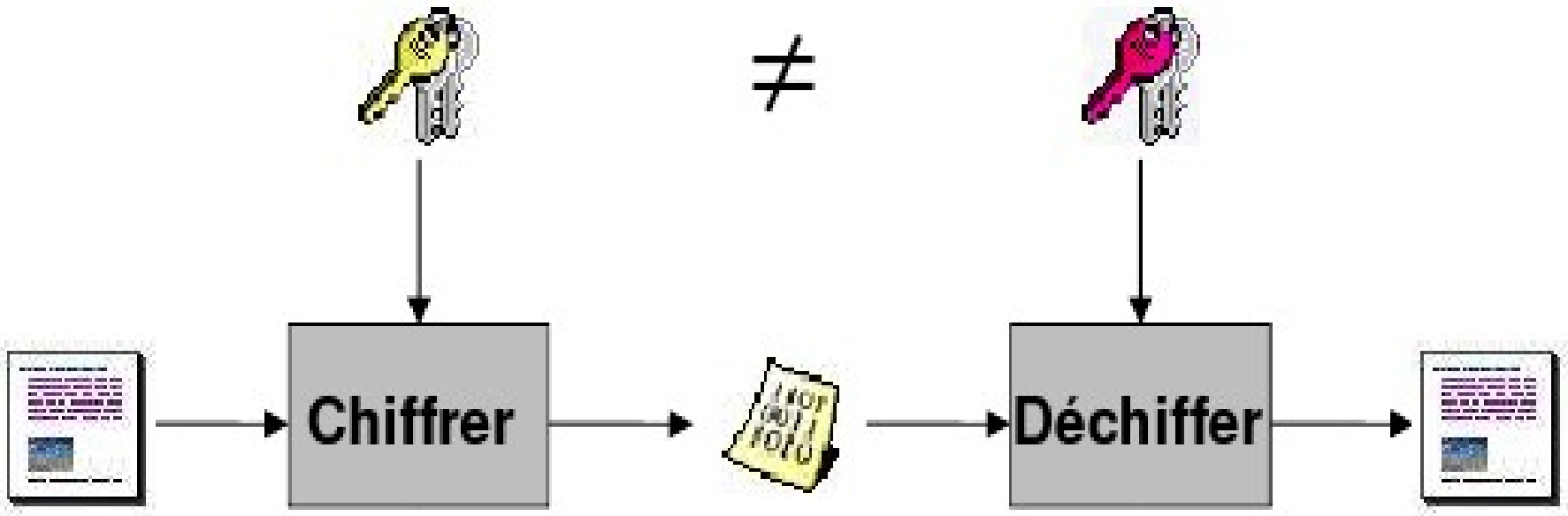
- **Autres algorithmes asymétriques courants :**
  - Un autre système de chiffrement asymétrique est El-Gamal du nom de son inventeur.
  - *Inconvénient*
    - Le texte brouillé représente deux fois la longueur du texte clair.
  - Ce principe est utilisé par **DSA (Digital Signature Algorithm)**
    - En fait DSA consiste à générer deux valeurs de 160 bits avec la clé privée, puis on démontre du coté du récepteur en utilisant la clé publique que seule la clé privée pouvait générer ces valeurs.Il n'y a donc pas de chiffrement proprement dit.
  - DSA utilise une fonction de hachage pour la signature **SHA (Secure Hash Algorithme)**

II. Confidentialité et algorithmes de chiffrement

- **Chiffrement**
  - Clef **publique** utilisée pour le **chiffrement**
  - seul le détenteur de la clef **privée** peut **déchiffrer**
-



Cryptographie asymétrique



Histoire

- Cryptographie symétrique :
  - Pas de signature digitale.

- Diffie-Hellman (1976) :
  - Introduction du concept de signature digitale et de la cryptographie à clé publique.

- Rivest-Shamir-Adleman (1978) :
  - Premier algorithme de cryptographie asymétrique.

Histoire ou légende ...

- NSA affirme connaître la cryptographie asymétrique depuis 1966.
  - Pas de preuve mais …

- Le département du chiffre anglais connaissait la cryptographie asymétrique depuis 1971.
  - Preuve depuis 1999.

Informatisation de ...

- Alphabet clair : A = {0,1}.

- Espace des messages (en clair) :

  $M = \{m=(m1\ldots mn) \mid \forall\ i,\ mi \in A \text{ et } m \text{ a un sens}\}$

- Espace des (messages) chiffrés :

  $C = \{c=(c1\ldots cn) \mid \forall\ i,\ ci \in A\}$

- Espace des clés :

  $K = \{(kp, ks) \mid kp \leftrightarrow ks\}$

… la cryptographie asymétrique ...

- Fonctions de chiffrement :
  - E : M x Kp → C
  - E(..,kp) = E[kp](..) = Ekp (..)
- Fonctions de déchiffrement :
  - D : C x Ks → M
  - D(..,ks) = D[ks](..) = Dks (..).

$\forall$ m $\in$M, $\forall$ (kp,ks) $\in$K, Dks (Ekp (m)) = m

… et signature digitale.

- Fonctions de signature :
  - $S : M \times Ks \rightarrow C$
  - $S(..,ks) = S[ks](..) = Sks\ (..)$
- Fonctions de vérification :
  - $V : C \times Kp \rightarrow M$
  - $V(..,kp) = V[kp](..) = Vkp\ (..)$

$\forall\ m \in M, \forall\ (kp,ks) \in K, Vkp\ (\ Sks\ (m)\ ) = m$

Outils mathématiques

- Théorie de la complexité :
  - Problèmes P, NP, NP-Complets.

- Théorie des nombres :
  - Nombreux problèmes NP à sens uniques.

Nombre premier et PGCD

- Nombre premier :
  - Nombre divisible uniquement par 1 et lui-même.

- PGCD (Plus Grand Commun Diviseur) :
  - Deux nombres a et b sont premiers entre eux ssi pgcd(a,b) = 1, i.e., il existe c et d tel que
    $ac + bd = 1$.

- Algorithme d'Euclide :
  - Permet de trouver le PGCD de deux nombres.

Factorisation

- Factorisation :
  - Trouver les facteurs premiers.
- Paradoxe de la factorisation :
  - Génération de nombres premiers : algorithme polynomial.
  - Calcul du PGCD de deux nombres : algorithme polynomial d'Euclide.
  - Factorisation de nombres : problème de complexité exponentiel.

Arithmétique modulaire

- Calcul modulaire :
  - Reste de la division Euclidienne : $37 \equiv 2 \bmod 5$.
  - Addition, multiplication, exponentiation modulaire.
  - $\mathbb{Z}/n\mathbb{Z}$: ensemble de tous les résidus modulo n muni des opérations modulaires.
- Division modulaire / Inverse :
  - Trouver b tel que $ab \equiv 1 \bmod n$.
  - Si pgcd(a,n) = 1, solution unique (algorithme d'Euclide) ; sinon, pas de solution.

Arithmétique modulaire

- Petit théorème de Fermat :
  - Si m premier, et pgcd(a,m) = 1, a^(m-1) ≡ 1 mod m.
- Fonction d'Euler :
  - φ(n) est le nombre de résidus premiers avec n.
  - Si n est premier, φ(n) = n-1 ; si n=pq, φ(n) = (p-1)(q-1).

Arithmétique modulaire

- Petit théorème de Fermat généralisé par Euler:
  - Si pgcd(a,n) = 1, a^(φ(n)) ≡ 1 mod n.

- Inverse modulaire :
  - Si pgcd(a,n) = 1, l'inverse de a est a^(φ(n)-1) mod n

Problèmes de référence

- Factorisation de nombres entiers :
  - Trouver les facteurs premiers n.
- Racine eième modulaire :
  - Trouver x tel que x^e ≡ c mod n.
- Logarithme discret :
  - Trouver x tel que a^x ≡ b mod p.

Problèmes de référence

- Résidu quadratique :
  - Décider si a est un résidu quadratique modulo n (i.e., il existe b tel que $b^2 \equiv a \bmod n$).
- Logarithme discret généralisé (Diffie-Hellman) :
  - Etant donnés a^x mod p et a^y mod p, trouver a^(xy) mod p.

Algorithmes asymétriques

- RSA (Rivest-Shamir-Adleman, 1978) :
  - Racine eième dans un corps finis.
- Rabin (Rabin, 1979) :
  - Racines carrées dans un corps finis.
- ElGamal (ElGamal, 1985) :
  - Logarithme discret généralisé.
- Courbes elliptiques (Koblitz et Miller, 1985).

Initialisation

1- p et q deux grands nombres premiers

2- $n = pq$ et $\varphi(n) = (p-1)(q-1)$

3- Entier e tq $1 < e < \varphi(n)$ et $gcd(e, \varphi(n))=1$

4- Calculer d tq $1 < d < \varphi(n)$ et $ed = 1 \bmod \varphi(n)$
(Algorithme d'Euclide).

5- Clé publique : (e,n).
Clé privée : d.

Chiffrement

1- Obtenir la clé publique (e,n) du destinataire

2- Représenter le message comme un entier m tel que 1 < m < n.

3- Calculer c = m^e mod n.

Déchiffrement

1- A l'aide de la clé privée d, calculer
m = c^d mod n.

Preuve :
c^d = (m^e)^d mod n = m^(ed) mod n = m mod n.

Signature digitale

1- Représenter le message comme un entier
m tel que 1 < m < n.

2- A l'aide de la clé privé d, calculer
s = m^d mod n.

Vérification d'une signature

1- Obtenir la clé publique (e,n) du signataire

2- Calculer m = s^e mod n

Preuve :

se = (m^d)^e mod n = m^(ed) mod n = m mod n.

Exemple – Initialisation

1- p = 31 et q = 137.

2- n = 4247 et φ(n) = 4080.

3- Entier e = 967

(1 < e < φ(n) et gcd(e,φ(n))=1)

4- Entier d = 2983

(1 < d < φ(n) et ed = 707x4080+1 = 1 mod φ(n))

5- Clé publique : (e,n) => (967,4247)
Clé privée : d => 2983

Exemple Chiffrement / Déchiffrement

1- Message en clair : m = 3333.

(1 < m < n)

2- Chiffrement :

c = m^e mod n = 3333^967 mod 4247 = 3790.

3- Déchiffrement :

m = c^d mod n = 3790^2983 mod 4247 = 3333.

Propriétés

- Propriétés multiplicatives :

  $(m1m2)^e \equiv m1^e\ m2^e \bmod n \equiv c1\ c2 \bmod n.$

  – Nécessité de formater les messages avant chiffrement / signature
  – ISO 9796 et PKCS #1.

- Existence de points fixes :

  Il existe m tel que $m^e \equiv m \bmod n$.

- Performance :
  – 1000 fois plus lent que le DES !

Sécurité

- Attaques possibles :
  - Factoriser de n : complexité exponentiel.
  - Trouver la valeur de φ(n) : aussi complexe que de factoriser n.
  - Trouver la valeur de d : la connaissance de n, e et d permet de factoriser n.
- Conjoncture :
  - La sécurité de RSA dépend du problème de factorisation.

Cryptanalyse

- Factorisation de n :
  - Record actuel : 512 bits mais …
  - … factorisation facile dans certain cas (trop petits facteurs premiers pour p-1 et q-1 …).
  - A titre d'exemple : Carte Bancaire (320 bits).
- Attaques au niveau des formatages :
  - ISO 9796 et PKCS #1 partiellement attaqués.

Note sur la longeur des clefs

- Ne pas mélanger les longueurs de clefs publiques et secrètes
- Les algorithmes reposent sur des principes différents et utilisent donc comme clef des éléments présentant des caractéristiques (notamment longueur) différentes
- ***Cryptanalyse*** et comparaisons de résistance :
  - Pour les clefs secrètes, la référence est la recherche exhaustive, qui nécessite 2^(n-1) essais en moyenne
  - Pour les clefs publiques, l'attaquant doit résoudre le problème mathématique sur lequel repose l'algorithme
  - Factorisation (RSA) : coût sous-exponentiel, 1024 bits
  - Courbes elliptiques : 160 bits équivalent à RSA-1024