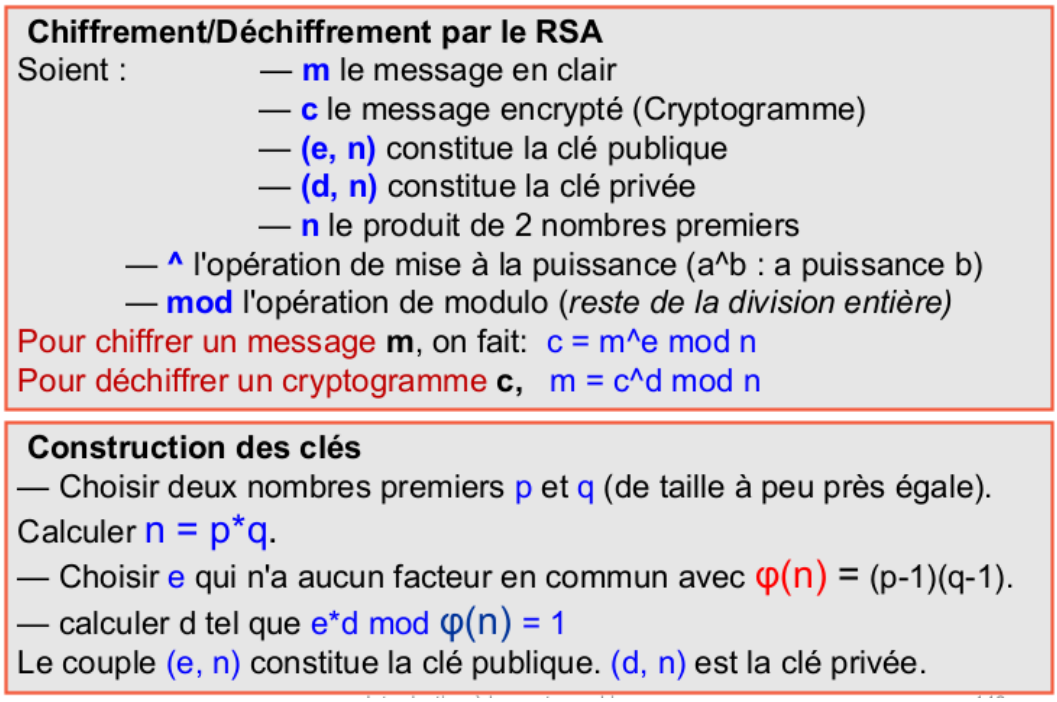
SECU



Chiffrement/Déchiffrement par le RSA

Soient :
- **m** le message en clair
- **c** le message encrypté (Cryptogramme)
- **(e, n)** constitue la clé publique
- **(d, n)** constitue la clé privée
- **n** le produit de 2 nombres premiers
- **^** l'opération de mise à la puissance (a^b : a puissance b)
- **mod** l'opération de modulo (*reste de la division entière)*

Pour chiffrer un message **m**, on fait: c = m^e mod n

Pour déchiffrer un cryptogramme **c**, m = c^d mod n

Construction des clés

— Choisir deux nombres premiers p et q (de taille à peu près égale).

Calculer n = p*q.

— Choisir e qui n'a aucun facteur en commun avec φ(n) = (p-1)(q-1).

— calculer d tel que e*d mod φ(n) = 1

Le couple (e, n) constitue la clé publique. (d, n) est la clé privée.

Calcul de l’exponentiation

Soit le calcul de V = A^B :

Methode indienne

Initialiser V = 1

Tant que B ≥ 1 faire

- si B est impair, multiplier V par A et retrancher 1 à B
- sinon, élever A au carré et diviser B par 2

Methode Binaire

Initialiser V = 1

Pour chaque bit de l'exposant B, en commençant par les poids forts:

- élever V au carré

- si ce bit vaut 1, multiplier V par A

Exponentiation modulaire binaire

Initialiser V = 1

Pour chaque bit de l'exposant B, en commençant par les poids forts:

- élever V au carré mod n
- si ce bit vaut 1, multiplier V par A mod n

Chiffrement ECC

Begin

1. $C = \infty$

2. For *i* ***from*** *0* ***to*** *n-1*

3. $P = 2 \times P$ *//ECPD*

4. If $(k_i = 1)$ then $C = C + P$ *//ECPA*

End For

1. Return C

- Le chiffré est un point Q, $Q \in E(\mathbb{F}_p)$.

Chiffrement hybride

La plupart des systèmes hybrides procèdent de la manière suivante. Une clé aléatoire, appelée clé de session, est générée pour l'algorithme symétrique (3DES, IDEA, AES et bien d'autres encore), cette clé fait généralement entre 128 et 512 bits selon les algorithmes. L'algorithme de chiffrement symétrique est ensuite utilisé pour chiffrer le message. Dans le cas d'un chiffrement par blocs, on doit utiliser un mode d'opération comme CBC, cela permet de chiffrer un message de taille supérieure à celle d'un bloc.
La clé de session quant à elle, se voit chiffrée grâce à la clé publique du destinataire, c'est ici qu'intervient la cryptographie asymétrique (RSA ou ElGamal). Comme la clé est courte, ce chiffrement prend peu de temps. Chiffrer l'ensemble du message avec un algorithme asymétrique serait bien plus coûteux, c'est pourquoi on préfère passer par un algorithme symétrique. Il suffit ensuite d'envoyer le message chiffré avec l'algorithme symétrique et accompagné de la clé chiffrée correspondante. Le destinataire déchiffre la clé symétrique avec sa clé privée et via un déchiffrement symétrique, retrouve le message.

Diffie-Hellman

n : premier; g : générateur

Alice	Bob
Choisie a	Choisie b
A = g^a mod n	B = g^b mod n
K = B^a = (g^b)a mod n	K’ = A^a = (g^a)b mod n

K = K’

> La sécurité de ce protocole réside dans la difficulté du problème du logarithme discret sur un corps fini. Ceci dit, il faut une phase préliminaire d'authentification pour remedier a l’attque du Man in the middle !

El Gamal

Destinataire (Alice)

1. Choisit un nombre premier p et un générateur g de Zp
2. Sélectionne aléatoirement un nombre a Є Zp
3. Publie (p, g, ga mod p)

Expéditeur (Bob)

1. soit m le message avec m < p; choisit aléatoirement un entier b Є Zp
2. calcule c1 = gb mod p et c2 = m.(ga)b mod p
3. envoie c = (c1, c2)

Destinataire

1. calcule d1 = (c1)−a mod p = (c1)p−1−a mod p = g−ab mod p
2. puis calcule d2 = d1.c2 mod p = g−ab.m.(ga)b mod p = m

Signature électronique

Les conditions suivantes doivent être réunies:

Authentique : l'identité du signataire doit pouvoir être retrouvée de manière certaine ;

infalsifiable : Quelqu'un ne peut se faire passer pour un autre ;

non réutilisable : Elle fait partie du document signé et ne peut être déplacée sur un autre document;

inaltérable : Une fois qu'il est signé, on ne peut plus le modifier ;

irrévocable : La personne qui a signé ne peut le nier.

Authentification (challenge/response)

Alice envoie à Bob un message aléatoire (challenge)

- Chiffrement symétrique:
  1. Alice et Bob partage une même clé secrète ;
  2. Bob renvoie à Alice le message chiffré à l'aide de la clé
- Chiffrement asymétrique:
  1. Bob renvoie à Alice le message chiffré à l'aide de sa clé privée (réponse) ;
  2. Alice peut alors déchiffrer ce message, à l'aide de la clé publique de Bob… c'est donc Bob ! C’est la signature

Probleme: Signer des documents de grande taille prend beaucoup de temps et peut mettre en perile la cle privee en essayant avec des messages bien choisis → utiliser le une fonction de hashage qui, quelque soit la taille du message, retourne toujours un message de taille n.

Une bonne fonction de hachage doit être:

- publique (pas de notion de secret)
- rapide à calculer
- à sortie de taille fixe.
- bien répartie en sortie.

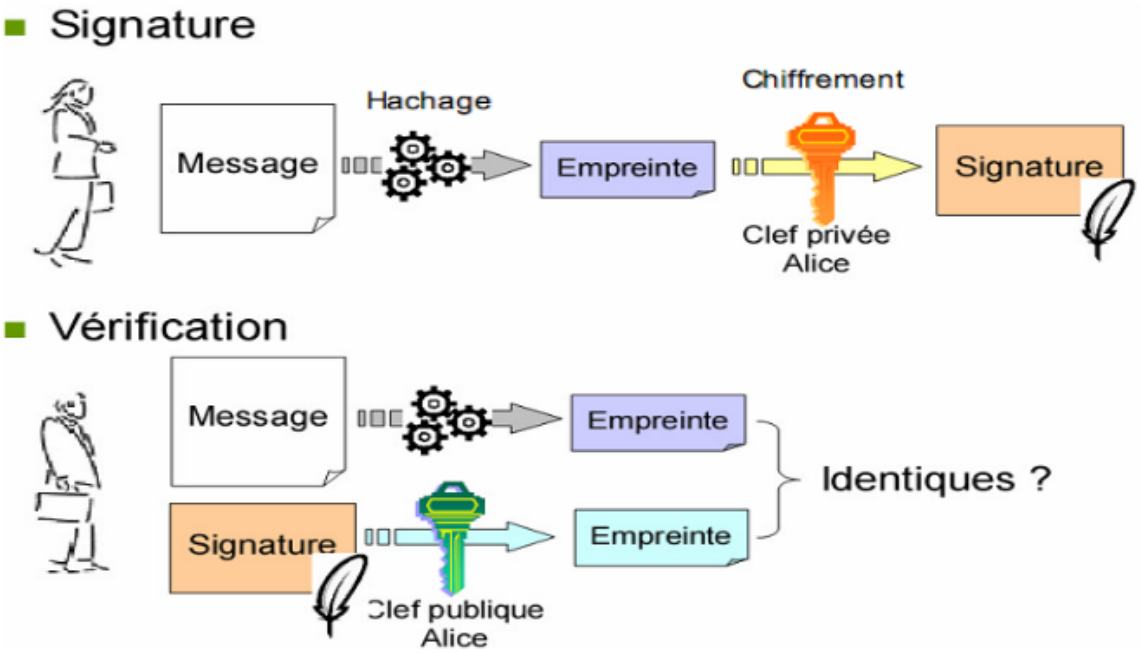
Propriete Fonction hashage

Résistance à la préimage
Étant donnée y = H(m), il est difficile de retrouver m à partir de y !

Résistance à la seconde préimage
Étant donnée m et H(m), il est difficile de trouver m’ ≠ m tel que H(m’)= H(m)

Résistance aux collisions
Il est difficile de trouver m et m’ vérifiant: m’ ≠ m tel que H(m’)= H(m)

Verification des signatures



Signature electronique

Fonctionnement

1. L'expéditeur calcule l'empreinte de son texte en clair à l'aide d'une fonction de hachage ;
2. L'expéditeur chiffre l'empreinte avec sa clé privée .Le chiffrement du document est optionnel si la confidentialité n'est pas nécessaire.
3. L'expéditeur chiffre le texte en clair et l'empreinte chiffrée à l'aide de la clé publique du destinataire.
4. L'expéditeur envoie le document chiffré au destinataire ;
5. Le destinataire déchiffre le document avec sa clé privée ;
6. Le destinataire déchiffre l'empreinte avec la clé publique de l'expéditeur (authentification) + (Non-répudiation)
7. Le destinataire calcule l'empreinte du texte clair à l'aide de la même fonction de hachage que l'expéditeur ;
8. Le destinataire compare les deux empreintes. Deux empreintes identiques impliquent que le texte en clair n'a pas étémodifié (intégrité).