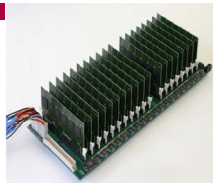
Au menu

1. Chiffrement symétrique
2. Chiffrement asymétrique
3. Fonctions de hashage
4. Signature de messages
5. Authentification de messages
6. Echange de clés

Longueur de clé

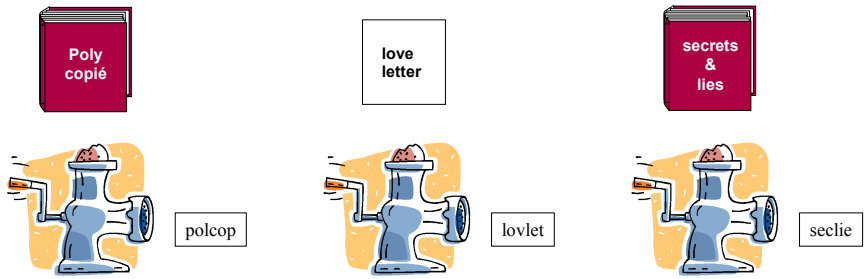


Copacobana, University of Kiel

- Pour algorithmes symétriques:
  - 40 bits : 2^{40} possibilités (1 million de millions)
  - 56 bits : 2^{56}, 9 jours avec du matériel coûtant $9000
  - 128 bits: 2^{128}, 1000x1000x1000x1000x1000x1000x1000 plus que 56 bits
- Pour RSA:
  - il n'y a que les nombres premiers qui peuvent être des candidats
  - 512 bits équivaut à 56 bits
  - 2048 bits équivaut à 128 bits

Les fonctions de hashage

- Les fonctions de hashage prennent un grand nombre de données et créent un résumé de longueur fixe.

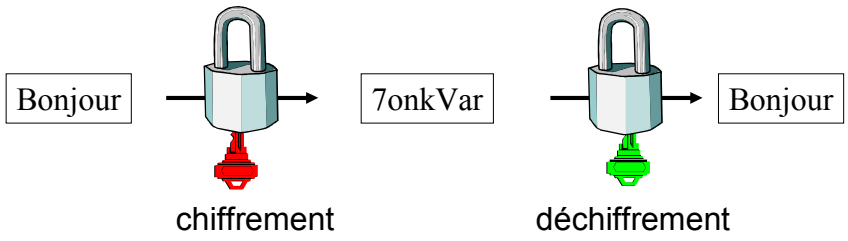


Les fonctions de hashage

- Les fonctions de hashage sont irréversibles
  - Résistance à la pré-image
- Elles peuvent générer des collisions
  - Inévitable si le hash est plus court que les données
- Les fonctions de hashage cryptographiques sont résistantes au collisions
  - A l'aide d'un message et de son hash, il n'est pas possible de créer un deuxième message avec le même hash (résitance à la seconde pré-image)
  - Il n'est pas possible de créer deux messages avec le même hash (résistance au collisions)
- Exemples: SHA-1 (160 bits), MD5 (128 bits), SHA-256 (256 bits)
  - MD5 et SHA-1 on les deux été cassés (il est possible de générer des collisions) c.f Arjen Lenstra

La signature

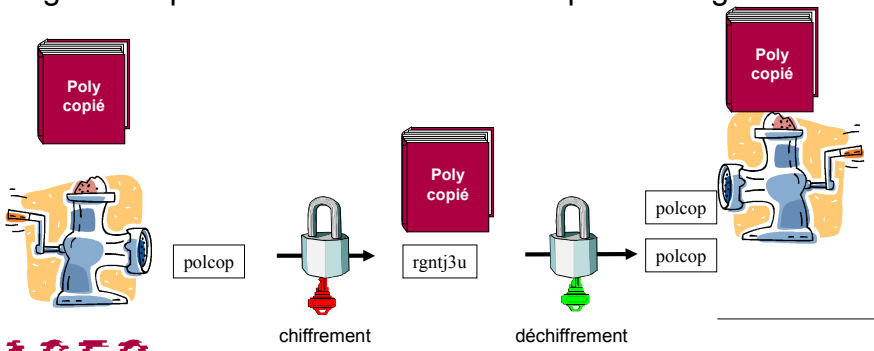
- Pour signer un message, on peut le chiffrer avec la clé privée



- Le déchiffrement avec la clé publique prouve que seul le détenteur de la clé privée à pu créer la signature

La signature (suite)

- Il n'est pas nécessaire de chiffrer tout un document pour le signer, il suffit de chiffrer son hash
- La résistance aux collisions de la fonction de hashage garantit que c'est bien ce document qui a été signé

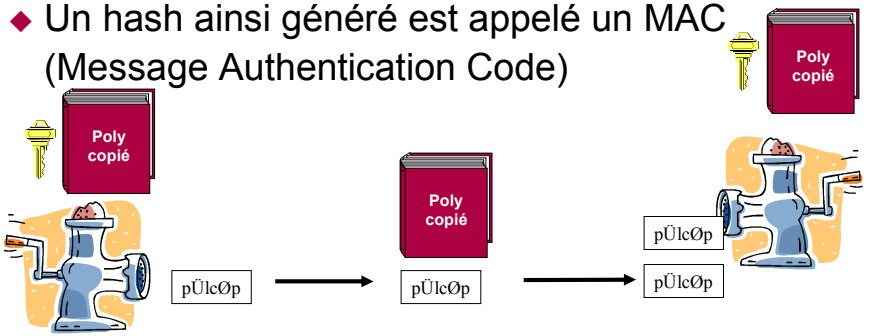


Authentification des messages

- Si on utilise un chiffrement symétrique pour chiffrer le hash on obtient une authentification, pas une signature
- La clé nécessaire pour vérifier la signature permet aussi de la créer!
- Si la clé n'est connue que par les deux partenaires, alors elle permet d'authentifier l'expéditeur du message.
- Exemples HMAC-SHA, HMAC-MD5

Authentification (suite)

- Plutôt que de chiffrer le hash, on fait intervenir la clé lors du calcul du hash
- Un hash ainsi généré est appelé un MAC (Message Authentication Code)



Comparaison

- Le chiffrement asymétrique est plus utile
  - Elimine le problème du transfert de la clé
  - Permet de signer des messages
- Le chiffrement symétrique et beaucoup plus performant
- On combine souvent les deux types de chiffrements pour profiter des avantages de chacun.

L'échange de clés

- Pour pouvoir utiliser des algorithmes symétriques (chiffrement, MAC) il faut d'abord échanger une clé symétrique avec son partenaire
- **Echange de clé RSA**
  - On génère une clé symétrique aléatoire
  - On la chiffre avec la clé publique du partenaire et on lui la transmet

Echange Diffie-Hellman

- Diffie-Hellman permet de générer une clé symétrique sans avoir à la transmettre
- DH est basé sur les logarithmes discrets (RSA aussi)
- On utilise un modulo *p* et un générateur *g*

Diffie-Hellman (suite)

- Alice choisit un chiffre *a*, Bob un chiffre *b*
- Alice calcule $A = g^a \bmod p$
- Bob calcule $B = g^b \bmod p$
- Alice et Bob s'échangent *A* et *B,* font encore une exponentiation et obtiennent le même résultat *K*

$$B^a \bmod p = g^{ba} \bmod p = K$$

$$A^b \bmod p = g^{ab} \bmod p = K$$

- Il n'est pas possible de trouver la clé à partir des valeurs échangées *A* et *B*

Diffie-Hellman (exemple)

- générateur: 3, modulo: 7

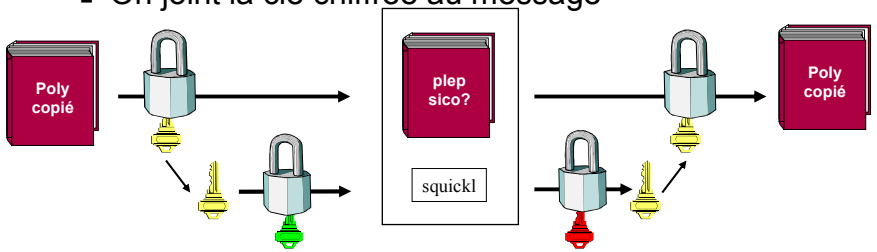
Alice		Bob
$a = 3$		$b = 2$
$A = 3^3 \bmod 7 = 6$	6 →	$B = 3^2 \bmod 7 = 2$
	← 2	
$K = 2^3 \bmod 7 = 1$		$K = 6^2 \bmod 7 = 1$

Résumé:

- chiffrement symétrique (DES, 3DES, AES) et asymétrique (RSA)
- longueur de clés: 40 bits très faible,
  56 moyen, 128 absolu (pour RSA 256, 512, 2048)
- Hash: résumé d'un message
- MAC: hash dans lequel intervient une clé (pour authentifier le message)
- signature: chiffrement d'un hash (MD5, SHA) du message avec clé privée
- Echange de clé par chiffrement asymétrique (RSA) ou Diffie-Hellman

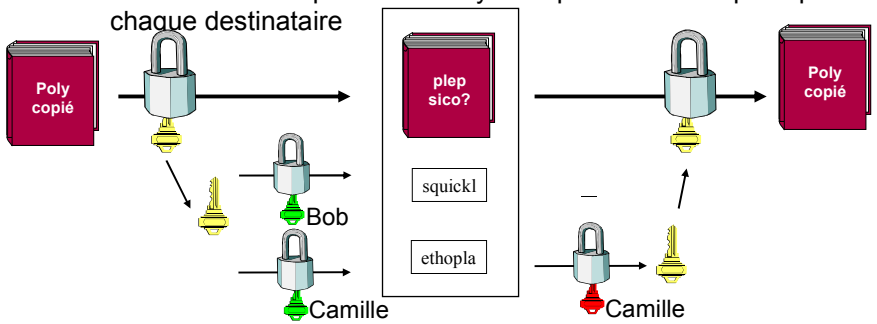
Chiffrement Hybride

- Pour profiter de l'efficacité du chiffrement symétrique et des avantages de l'asymétrique
  - On chiffre le message avec une clé symétrique
  - On chiffre la clé avec la clé publique du destinataire
  - On joint la clé chiffrée au message



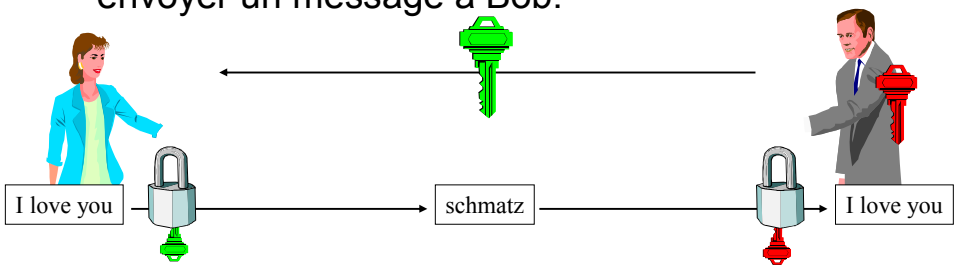
Chiffrement Hybride multi-clé

- Le chiffrement hybride permet aussi d'envoyer efficacement un message chiffré à plusieurs destinataires.
  - On chiffre une copie de la clé symétrique avec la clé publique de chaque destinataire



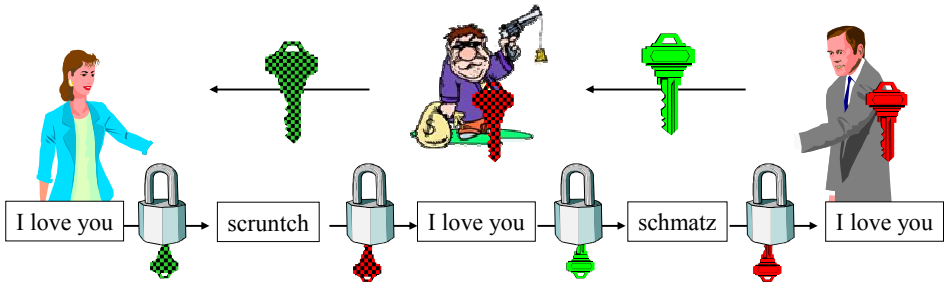
5.3.3 Certificats

- La distribution de clés publiques est sujette à l'attaque d'un intermédiaire (Man in the Middle)
- Voilà ce qui devrait se passer lorsqu'Alice veut envoyer un message à Bob:



Man in the middle

- Voilà ce qui peut se produire:



Le Certificat

- Un certificat est un document qui sert à prouver qu'une clé appartient bien à qui de droit.
- Le certificat est signé par un tiers dont on connaît la clé publique (notez la récursion)
- Un certificat contient au moins les informations suivantes:
  - Identité (Nom et adresse e-mail de la personne)
  - Clé publique
  - Date d'expiration
  - Signature du certificat
- Il existe deux types de certificats prévalents: (Open)PGP et X.509

Certificat: Exemple

- Un tiers de confiance (Trent) à signé un certificat liant la clé de Bob à son nom
- Si Alice est en possession de la clé publique de Trent elle peut vérifier le certificat