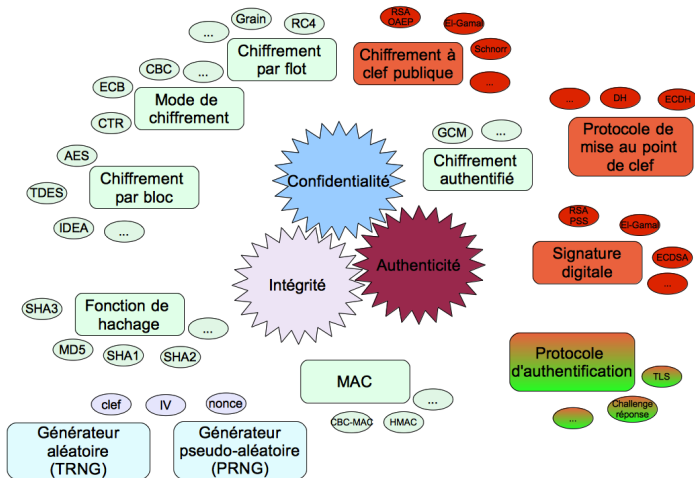


Cryptographie Asymétrique

Alexandre Duc

Vue Synoptique



1. Authentication

2. Protocole de Diffie-Hellman

3. Chiffrement d'El Gamal

4. Chiffrement RSA

5. Signature RSA

6. Signature DSA

7. Cryptographie Asymétrique en Pratique

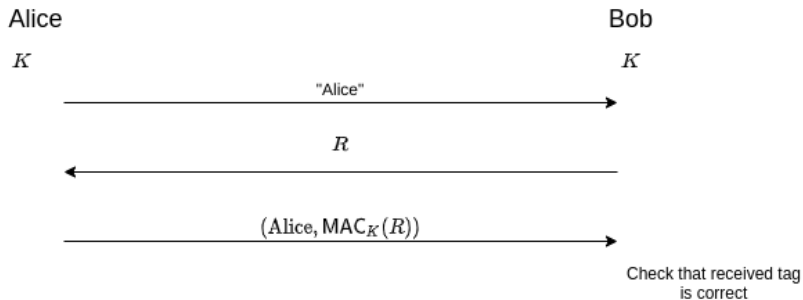
Protocoles d'Authentication

- Il existe 3 catégories de protocoles d'authentification :
 - authentification faible ;
 - authentification forte ;
 - (authentification de type «zero-knowledge»).

Mots de Passe

- Authentification basée sur un mot de passe
- Authentification **faible**
- L'utilisateur exhibe un secret (un mot de passe, un «cookie», etc.) préalablement partagé avec le serveur pour s'authentifier.

Authentication Forte : «Challenge-Response»



Authentication Forte : «Challenge-Response»

1. Alice et Bob partagent un secret symétrique commun (mot de passe, clef cryptographique, etc.) K .
2. Alice **s'identifie** auprès du serveur
3. Bob génère un «challenge», c'est-à-dire une valeur aléatoire R à **usage unique** et envoie R à Alice.
4. Alice calcule $\tau = \text{MAC}_K(R)$ et envoie ("Alice", τ) à Bob.
5. Bob reçoit la paire (X, τ') , récupère le secret K ainsi que la valeur R correspondant à l'identité X , et calcule $\tau = \text{MAC}_K(R)$.
6. Si $\tau = \tau'$, alors Bob considère qu'Alice s'est authentifiée avec succès.

1. Authentification
2. Protocole de Diffie-Hellman
3. Chiffrement d'El Gamal
4. Chiffrement RSA
5. Signature RSA
6. Signature DSA
7. Cryptographie Asymétrique en Pratique

Protocole de Mise au Point de Clef

- Le but d'un protocole de mise au point de clef («key-agreement protocol») consiste à obtenir un **secret partagé** entre deux entités au moyen d'un canal non-confidentiel.
- Le canal de communication doit cependant être **authentique**, pour éviter l'attaque de l'homme dans le milieu («**man-in-the-middle attack**»).
- L'idée principale consiste à utiliser une **fonction à sens unique** («one-way function»).

Fonction à Sens Unique

Définition (Fonction à sens unique)

Une **fonction à sens unique** est une fonction $f : \mathcal{D} \longrightarrow \mathcal{R}$ telle que

- Pour tout $x \in \mathcal{D}$, calculer $f(x)$ peut être effectué de manière efficace.
- Pour pratiquement toutes les valeurs $y \in \mathcal{R}$, calculer x tel que $y = f(x)$ est impossible à effectuer en pratique.

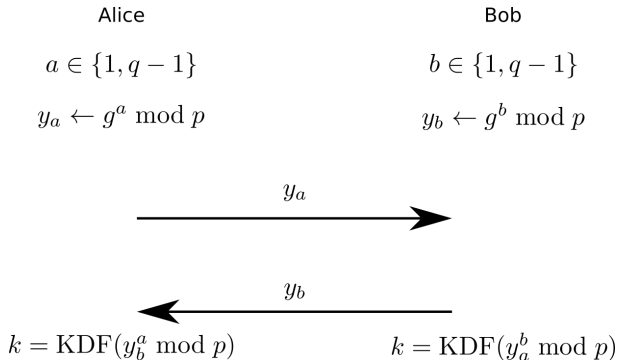
Logarithme Discret

Diffie et Hellman ont proposé en 1976 la fonction de **logarithme discret** comme fonction à sens unique :

- $p = cq + 1$ est un nombre premier de taille suffisante, typiquement plusieurs milliers de bits, où q est également un nombre premier plus petit (quelques centaines de bits).
- g est un élément d'ordre q du groupe multiplicatif \mathbb{Z}_p^* .
- On note $\langle g \rangle$ l'ensemble des éléments engendrés par g .
- La fonction $f : x \mapsto g^x \bmod p$ est conjecturée comme étant à sens unique.

Protocole de Diffie-Hellman

Paramètres publics : q , grand nombre premier, g élément d'ordre q dans \mathbb{Z}_p^*

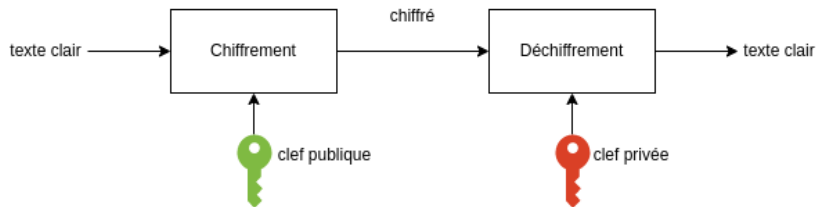


Protocole de Diffie-Hellman

- Se mettre d'accord sur un groupe multiplicatif \mathbb{Z}_p^* cryptographiquement sûr et sur un élément $g \in \mathbb{Z}_p^*$ d'ordre q , avec q premier.
- Alice génère une valeur secrète $a \in \{1, \dots, q-1\}$ uniformément au hasard, calcule $y_a = g^a \bmod p$, et envoie y_a à Bob via le canal authentique.
- Bob génère une valeur secrète $b \in \{1, \dots, q-1\}$ uniformément au hasard, calcule $y_b = g^b \bmod p$, et envoie y_b à Alice via le canal authentique.
- Alice calcule $k = \text{KDF}(y_b^a \bmod p)$ tandis que Bob calcule $k = \text{KDF}(y_a^b \bmod p)$, où KDF est une “key derivation function” (typiquement, une fonction de hashage répétée plusieurs fois).
- La clef secrète partagée est k . Elle pourra être ensuite employée pour établir un canal de communication confidentiel et authentique en utilisant de la cryptographie symétrique.

1. Authentification
2. Protocole de Diffie-Hellman
3. Chiffrement d'El Gamal
4. Chiffrement RSA
5. Signature RSA
6. Signature DSA
7. Cryptographie Asymétrique en Pratique


Rappel Chiffrement Asymétrique



Question

On veut utiliser Diffie-Hellman pour chiffrer directement un message. Comment peut-on le faire ?

Chiffrement d'El Gamal – Génération des Clefs

- Utilisation de Diffie-Hellman comme un masque jetable dans un groupe multiplicatif.
 - On fixe les paramètres du receptrer (e.g. Alice) dans Diffie-Hellman pour obtenir une pair de clefs publique/privée.
 - On travaille dans un groupe multiplicatif \mathbb{Z}_p^* cryptographiquement sûr et avec un élément $g \in \mathbb{Z}_p^*$ d'ordre q , avec q premier.
 - Clef privée : $a \in \mathbb{Z}_q$, clef publique : $A = g^a \bmod p$.
-  Comme g est d'ordre q , **on peut travailler mod q dans l'exposant !**

Chiffrement d'El Gamal – Chiffrement

- Pour chiffrer un message $M \in \langle g \rangle$, on tire un $k \in \mathbb{Z}_q$ uniformément au hasard.
- Le chiffré est la paire $(g^k \bmod p, MA^k \bmod p)$.

 **Chiffrement non-déterministe !**

Question

Comment déchiffrer ?

1. Authentification
2. Protocole de Diffie-Hellman
3. Chiffrement d'El Gamal
4. Chiffrement RSA
5. Signature RSA
6. Signature DSA
7. Cryptographie Asymétrique en Pratique

Chiffrement RSA

- L'algorithme de chiffrement RSA a été publié en 1978 par Adi Shamir, Ron Rivest et Len Adleman.
- L'idée est d'utiliser une fonction à sens unique munie d'une **trappe** ("trapdoor function"), c'est-à-dire d'une valeur qui, quand elle est connue, permet de l'inverser facilement.

Génération de Clef RSA

- Générer deux nombres premiers p et q aléatoires de taille suffisante (c.f. suite du cours).
- Calculer $n = pq$.
- Choisir un petit nombre e tel que $\text{pgcd}(e, \varphi(n)) = 1$, avec $\varphi(n) = (p - 1)(q - 1)$.
- Calculer $d = e^{-1} \bmod \varphi(n)$, et effacer p , q et $\varphi(n)$.
- La paire (n, e) est définie comme étant la clef publique.
- La paire (n, d) est définie comme étant la clef privée.

Chiffrement et Déchiffrement RSA

- Le texte chiffré c est obtenu par $c = m^e \bmod n$.
- Le message m est obtenu par $m = c^d \bmod n$.
- Cette méthode est appelée «**textbook RSA**», et ne doit **jamais** être utilisée en pratique, pour des raisons de sécurité : le message doit être **formaté** convenablement avant.

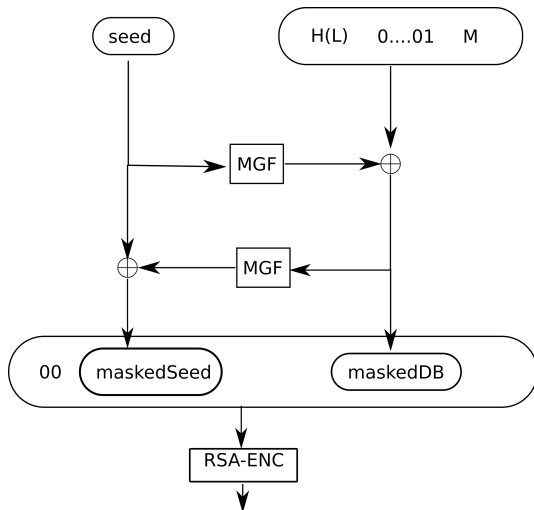
Textbook RSA

Question

Vous observez un message chiffré qui est le salaire de l'un de vos collègues. Récupérez son salaire. Quel est le problème par rapport à AES ?

RSA-OAEP

- Une méthode de formatage de message répandue en pratique et standardisée est **RSA-OAEP** :



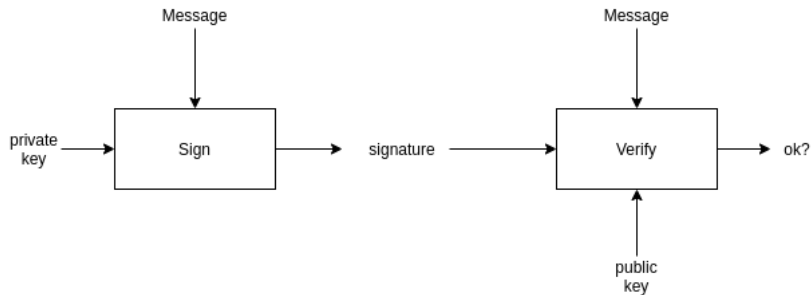
Exposant Public RSA

Exposant

En pratique, l'exposant public e utilisé dans RSA vaut souvent $e = 65537$. Il permet de chiffrer de manière plus efficace. De plus, il s'agit d'un nombre premier.

1. Authentification
2. Protocole de Diffie-Hellman
3. Chiffrement d'El Gamal
4. Chiffrement RSA
5. Signature RSA
6. Signature DSA
7. Cryptographie Asymétrique en Pratique

Rappel : Signatures Digitales



Erreur Classique

- Une signature digitale n'est **pas** l'inverse du chiffrement.
- On ne “chiffre” pas avec la clef privée” pour signer un message.

Origine

Cette erreur provient d'un cas particulier : les signatures textbook RSA.

Signature et Vérification RSA

- On génère les clefs de la même manière que pour le chiffrement.
- On obtient la signature s d'un message m en calculant $s = m^d \bmod n$.
- On vérifie une signature s en calculant $m' = s^e \bmod n$ et on accepte la signature si et seulement si $m = m'$.

Signatures RSA en Pratique

- Les signatures “textbook” RSA sont **malléables** (voir slide suivante).
- Pour éviter cela, il faut **formater** la signature : par exemple **RSA-PSS**.
- En pratique, on ne signe pas un message m directement, qui est souvent trop long, mais une **empreinte cryptographique** h de ce message.

Malléabilité des Signatures RSA

Question

Une application bancaire signe le montant à envoyer à l'aide de "textbook" RSA. Plus précisément, soit m le montant qui vous est envoyé, $(m, m^d \bmod n)$ est envoyé à la banque. Augmentez ce montant.

1. Authentification
2. Protocole de Diffie-Hellman
3. Chiffrement d'El Gamal
4. Chiffrement RSA
5. Signature RSA
6. Signature DSA
7. Cryptographie Asymétrique en Pratique

Signatures d'El Gamal


- Les signatures d'El Gamal ont été inventées par Taher El Gamal en 1984.
- Leur sécurité repose sur la difficulté de résoudre le problème du logarithme discret.
- Le design initial souffre de quelques problèmes de sécurité qui ont été corrigés dans le standard DSA ("digital signature algorithm").

DSA : Génération de la Clef

- On génère un nombre premier $p = cq + 1$ suffisamment grand (plusieurs milliers de bits), où q est également un nombre premier plus petit (plusieurs centaines bits), ainsi qu'un élément $g \in \mathbb{Z}_p^*$ d'ordre q .
- On génère une valeur secrète $1 \leq a \leq q - 1$ uniformément aléatoire.
- On calcule $A = g^a \bmod p$.
- La clef publique est A .
- La clef privée est a .

Comme g est d'ordre q , **on peut travailler mod q dans l'exposant !**

DSA : Signature

- On utilise une fonction de hachage cryptographiquement sûre $h : \{0, 1\}^* \longrightarrow \{1, \dots, q - 1\}$.
 - On génère un nombre uniformément aléatoire $k \in \{1, \dots, q - 1\}$.
 - Pour signer un message m , on calcule $r = (g^k \bmod p) \bmod q$ ainsi que $s = k^{-1}(h(m) + ar) \bmod q$.
 - La signature du message m est la paire (r, s) .
-  Le mod q final dans le calcul de r sert uniquement à réduire la taille de la signature. Il n'a aucun sens mathématique.

DSA : Vérification

- Pour vérifier la signature (r, s) attachée à un message m , on vérifie d'abord que ni r ni s sont nuls. Ensuite, on vérifie que $r = \left(g^{h(m)s^{-1}} A^{rs^{-1}} \bmod p\right) \bmod q$.
- Le processus de vérification fonctionne, car

$$\begin{aligned} \left(g^{h(m)s^{-1}} A^{rs^{-1}} \bmod p\right) \bmod q &= \left(g^{(h(m)+ar)s^{-1}} \bmod p\right) \bmod q \\ &= \left(g^k \bmod p\right) \bmod q = r . \end{aligned}$$

Paramètres, clefs, etc..

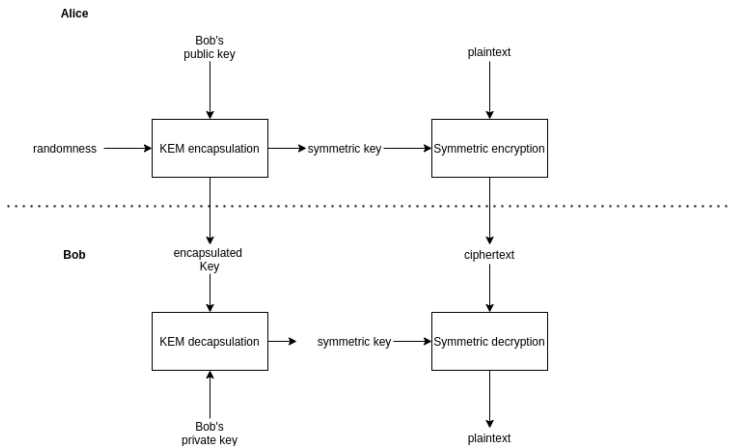
- Les paramètres g , p et q sont des paramètres **globaux** au système. Ils sont publics et fixés pour **tous** les utilisateurs.
- Les clefs a et A sont liées à **un utilisateur** et ne changent typiquement que très rarement.
- Le paramètre k doit, lui, changer à **chaque message**.

1. Authentification
2. Protocole de Diffie-Hellman
3. Chiffrement d'El Gamal
4. Chiffrement RSA
5. Signature RSA
6. Signature DSA
7. Cryptographie Asymétrique en Pratique

Cryptographie Asymétrique en Pratique

- En pratique, la chiffrement asymétrique est utilisé **uniquement** pour échanger des clefs symétriques.
- Le chiffrement asymétrique est beaucoup trop peu efficace.
- **Chiffrement hybride** : le texte chiffré contient deux parties, une clef symétrique chiffrée de manière asymétrique et le contenu chiffré de manière symétrique.
- Par contre, les **signatures** digitales sont beaucoup utilisées (même sur des gros documents).

Chiffrement Hybride



Solutions

Chiffrement d'El Gamal – Déchiffrement

Solution

Soit un texte chiffré (u, v) et une clef privée a , on calcule simplement $v/u^a \bmod p$.

Textbook RSA

Solution

On peut simplement bruteforcer le salaire en essayant pour chaque salaire s possible $s^e \bmod n$. Contrairement à AES, nous pouvons faire ce bruteforce car la clef publique est connue. Cela nous donne un accès à un oracle de chiffrement.

Malléabilité des Signatures RSA

Solution

On peut facilement signer le carré du montant m . Pour cela, étant donné (m, σ) avec σ la signature de m , on retourne simplement la paire (m^2, σ^2) .