

Memento RSA

Malika More

(malika.more@iut.u-clermont1.fr)

Yannick Do - Gisèle Provost - Chafik Samir

1A - IUT Info - Clermont 1

Cryptographie et Codes

Année 2011-2012

- 1 La pratique
 - Fabrication d'un chiffre RSA
 - Chiffrement
 - Déchiffrement
 - Attaques de RSA

- 2 La théorie
 - Qui a inventé le système RSA ?
 - Pourquoi le déchiffrement marche-t-il ?
 - Qu'est-ce-qui garantit la sécurité du système RSA ?

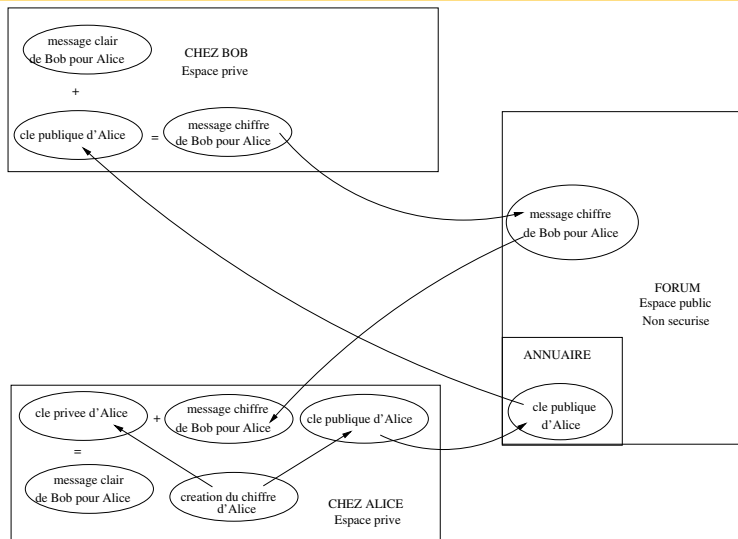
1 La pratique

- Fabrication d'un chiffre RSA
- Chiffrement
- Déchiffrement
- Attaques de RSA

2 La théorie

- Qui a inventé le système RSA ?
- Pourquoi le déchiffrement marche-t-il ?
- Qu'est-ce-qui garantit la sécurité du système RSA ?

Schéma général



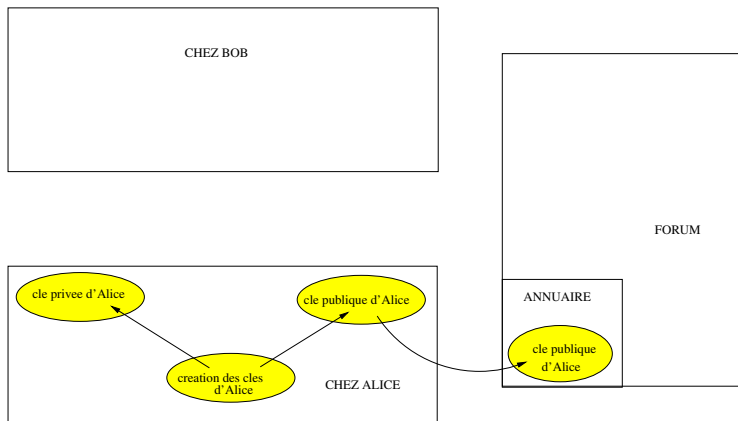
1 La pratique

- Fabrication d'un chiffre RSA
- Chiffrement
- Déchiffrement
- Attaques de RSA

2 La théorie

- Qui a inventé le système RSA ?
- Pourquoi le déchiffrement marche-t-il ?
- Qu'est-ce-qui garantit la sécurité du système RSA ?

Alice crée son chiffre RSA



Alice crée son chiffre RSA

Chez Alice

- $p = 11$
- $q = 17$
- $N = pq = 187$
- $\varphi = (p - 1) \cdot (q - 1) = 160$
- $E = 13$
- $\text{pgcd}(E, \varphi) = 1$
- $D = E^{-1} \bmod \varphi = 37$

Sur le forum

- Clé publique
d'Alice : $E = 13$
 $N = 187$

Chez Bob

Alice crée son chiffre RSA

Alice choisit deux nombres premiers différents p et q

Chez Alice

- $p = 11$
- $q = 17$
- $N = pq = 187$
- $\varphi = (p - 1) \cdot (q - 1) = 160$
- $E = 13$
- $\text{pgcd}(E, \varphi) = 1$
- $D = E^{-1} \bmod \varphi = 37$

Sur le forum

- Clé publique
d'Alice : $E = 13$
 $N = 187$

Chez Bob

Alice crée son chiffre RSA

Alice calcule le module $N = p \cdot q$

Chez Alice

- $p = 11$
- $q = 17$
- $N = pq = 187$
- $\varphi = (p - 1) \cdot (q - 1) = 160$
- $E = 13$
- $\text{pgcd}(E, \varphi) = 1$
- $D = E^{-1} \bmod \varphi = 37$

Sur le forum

- Clé publique
d'Alice : $E = 13$
 $N = 187$

Chez Bob

Alice crée son chiffre RSA

Alice calcule le nombre $\varphi(N) = (p - 1) \cdot (q - 1)$

Chez Alice

- $p = 11$
- $q = 17$
- $N = pq = 187$
- $\varphi = (p - 1) \cdot (q - 1) = 160$
- $E = 13$
- $\text{pgcd}(E, \varphi) = 1$
- $D = E^{-1} \bmod \varphi = 37$

Sur le forum

- Clé publique
d'Alice : $E = 13$
 $N = 187$

Chez Bob

Alice crée son chiffre RSA

Alice choisit son compliqueur E

Chez Alice

- $p = 11$
- $q = 17$
- $N = pq = 187$
- $\varphi = (p - 1) \cdot (q - 1) = 160$
- **$E = 13$**
- $\text{pgcd}(E, \varphi) = 1$
- $D = E^{-1} \bmod \varphi = 37$

Sur le forum

- Clé publique d'Alice : $E = 13$
 $N = 187$

Chez Bob

Alice crée son chiffre RSA

Alice vérifie que le compliceur est acceptable : $\text{pgcd}(E, \varphi) = 1$

Chez Alice

- $p = 11$
- $q = 17$
- $N = pq = 187$
- $\varphi = (p - 1) \cdot (q - 1) = 160$
- $E = 13$
- $\text{pgcd}(E, \varphi) = 1$
- $D = E^{-1} \bmod \varphi = 37$

Sur le forum

- Clé publique
d'Alice : $E = 13$
 $N = 187$

Chez Bob

Alice crée son chiffre RSA

Alice calcule son facilitateur $D = E^{-1} \bmod \varphi$

Chez Alice

- $p = 11$
- $q = 17$
- $N = pq = 187$
- $\varphi = (p - 1) \cdot (q - 1) = 160$
- $E = 13$
- $\text{pgcd}(E, \varphi) = 1$
- $D = E^{-1} \bmod \varphi = 37$

Sur le forum

- Clé publique
d'Alice : $E = 13$
 $N = 187$

Chez Bob

Alice crée son chiffre RSA

Alice publie sa clé publique E et N et garde secrète sa clé privée D

Chez Alice

- Clé privée
d'Alice : $D = 37$

Sur le forum

- Clé publique
d'Alice : $E = 13$
 $N = 187$

Chez Bob

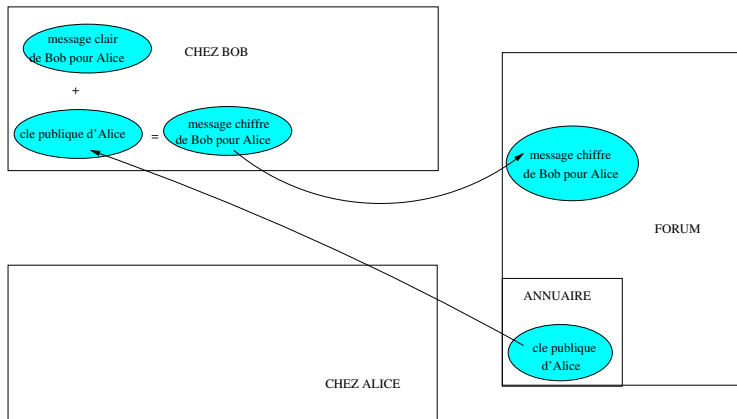
1 La pratique

- Fabrication d'un chiffre RSA
- **Chiffrement**
- Déchiffrement
- Attaques de RSA

2 La théorie

- Qui a inventé le système RSA ?
- Pourquoi le déchiffrement marche-t-il ?
- Qu'est-ce-qui garantit la sécurité du système RSA ?

Bob envoie un message secret à Alice



Bob envoie un message secret à Alice

Chez Alice

Sur le forum

- Clé publique d'Alice : $E = 13$
 $N = 187$
- Cryptogramme pour Alice : $C = 174$

Chez Bob

- $M = 4$
- $M < N$
- $C = M^E \bmod N = 174$

Bob envoie un message secret à Alice

Bob écrit son message en clair M

Chez Alice

Sur le forum

- Clé publique d'Alice : $E = 13$
 $N = 187$
- Cryptogramme pour Alice : $C = 174$

Chez Bob

- $M = 4$
- $M < N$
- $C = M^E \bmod N = 174$

Bob envoie un message secret à Alice

Bob vérifie la taille de son message $M < N$

Chez Alice

Sur le forum

- Clé publique d'Alice : $E = 13$
 $N = 187$
- Cryptogramme pour Alice : $C = 174$

Chez Bob

- $M = 4$
- $M < N$
- $C = M^E \bmod N = 174$

Bob envoie un message secret à Alice

Bob chiffre son message à l'aide de la clé publique d'Alice

$$C = M^E \bmod N$$

Chez Alice

Sur le forum

- Clé publique d'Alice : $E = 13$
 $N = 187$
- Cryptogramme pour Alice : $C = 174$

Chez Bob

- $M = 4$
- $M < N$
- $C = M^E \bmod N = 174$

Bob envoie un message secret à Alice

Bob publie son cryptogramme C

Chez Alice

Sur le forum

- Clé publique d'Alice : $E = 13$
 $N = 187$
- Cryptogramme pour Alice : $C = 174$

Chez Bob

- $M = 4$
- $M < N$
- $C = M^E \bmod N = 174$

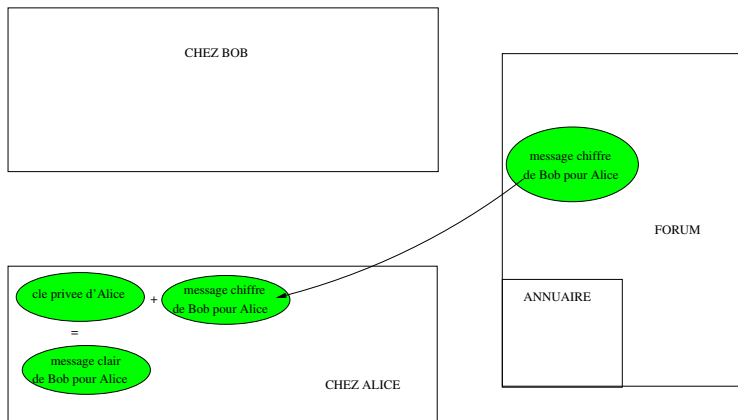
1 La pratique

- Fabrication d'un chiffre RSA
- Chiffrement
- Déchiffrement
- Attaques de RSA

2 La théorie

- Qui a inventé le système RSA ?
- Pourquoi le déchiffrement marche-t-il ?
- Qu'est-ce-qui garantit la sécurité du système RSA ?

Alice reçoit un message secret



Alice reçoit un message secret

Chez Alice

- $C = 174$
- $D = 37$
- $M' = C^D$
mod $N = 4$
- $M' = 4$

Sur le forum

- Clé publique
d'Alice : $E = 13$
 $N = 187$
- Cryptogramme pour
Alice : $C = 174$

Chez Bob

Alice reçoit un message secret

Alice récupère un cryptogramme C qui lui est adressé

Chez Alice

- $C = 174$
- $D = 37$
- $M' = C^D \pmod N = 4$
- $M' = 4$

Sur le forum

- Clé publique d'Alice : $E = 13$
 $N = 187$
- Cryptogramme pour Alice : $C = 174$

Chez Bob

Alice reçoit un message secret

Alice déchiffre le cryptogramme à l'aide de sa clé privée

$$M' = C^D \bmod N$$

Chez Alice

- $C = 174$
- $D = 37$
- $M' = C^D \bmod N = 4$
- $M' = 4$

Sur le forum

- Clé publique d'Alice : $E = 13$
 $N = 187$
- Cryptogramme pour Alice : $C = 174$

Chez Bob

Alice reçoit un message secret

Alice lit le message déchiffré M'

Chez Alice

- $C = 174$
- $D = 37$
- $M' = C^D \bmod N = 4$
- $M' = 4$

Sur le forum

- Clé publique d'Alice : $E = 13$
 $N = 187$
- Cryptogramme pour Alice : $C = 174$

Chez Bob

1 La pratique

- Fabrication d'un chiffre RSA
- Chiffrement
- Déchiffrement
- Attaques de RSA

2 La théorie

- Qui a inventé le système RSA ?
- Pourquoi le déchiffrement marche-t-il ?
- Qu'est-ce-qui garantit la sécurité du système RSA ?

Mr X espionne Alice et Bob

Mr X espionne Alice et Bob

Chez Alice

- $D = 37$
- $M' = C^D \bmod N = 4$

Sur le forum

- Clé publique d'Alice : $E = 13$
 $N = 187$
- Cryptogramme pour Alice : $C = 174$

Chez Bob

- $M = 4$
- $C = M^E \bmod N = 174$

Mr X espionne Alice et Bob

Mr X connaît la clé publique d'Alice E et N

Chez Alice

- $D = 37$
- $M' = C^D \bmod N = 4$

Sur le forum

- Clé publique d'Alice : $E = 13$
 $N = 187$
- Cryptogramme pour Alice : $C = 174$

Chez Bob

- $M = 4$
- $C = M^E \bmod N = 174$

Mr X espionne Alice et Bob

Mr X connaît le cryptogramme de Bob C

Chez Alice

- $D = 37$
- $M' = C^D \pmod{N = 4}$

Sur le forum

- Clé publique d'Alice : $E = 13$
 $N = 187$
- Cryptogramme pour Alice : $C = 174$

Chez Bob

- $M = 4$
- $C = M^E \pmod{N = 174}$

Mr X espionne Alice et Bob

Mr X n'est pas capable de calculer la clé privée d'Alice D

Chez Alice

- $D = 37$
- $M' = C^D \mod N = 4$

Sur le forum

- Clé publique d'Alice : $E = 13$
 $N = 187$
- Cryptogramme pour Alice : $C = 174$

Chez Bob

- $M = 4$
- $C = M^E \mod N = 174$

Mr X espionne Alice et Bob

Mr X ne peut pas décrypter le cryptogramme C

Chez Alice

- $D = 37$
- $M' = C^D \pmod{N = 4}$

Sur le forum

- Clé publique d'Alice : $E = 13$
 $N = 187$
- Cryptogramme pour Alice : $C = 174$

Chez Bob

- $M = 4$
- $C = M^E \pmod{N = 174}$

Mme Y espionne aussi Alice et Bob

Chez Alice

- $D = 37$
- $M' = C^D \bmod N = 4$

Sur le forum

- Clé publique d'Alice : $E = 13$
 $N = 187$
- Cryptogramme pour Alice : $C = 174$

Chez Bob

- $M = 4$
- $C = M^E \bmod N = 174$

Mme Y espionne aussi Alice et Bob

Mme Y n'est pas capable de calculer la clé privée d'Alice D

Chez Alice

- $D = 37$
- $M' = C^D \mod N = 4$

Sur le forum

- Clé publique d'Alice : $E = 13$
 $N = 187$
- Cryptogramme pour Alice : $C = 174$

Chez Bob

- $M = 4$
- $C = M^E \mod N = 174$

Mme Y espionne aussi Alice et Bob

Mme Y utilise la technique appelée [man-in-the-middle attack](#)

Je vous laisse vous souvenir de quoi il s'agit

Chez Alice

- $D = 37$
- $M' = C^D \mod N = 4$

Sur le forum

- Clé publique d'Alice : $E = 13$
 $N = 187$
- Cryptogramme pour Alice : $C = 174$

Chez Bob

- $M = 4$
- $C = M^E \mod N = 174$

1 La pratique

- Fabrication d'un chiffre RSA
- Chiffrement
- Déchiffrement
- Attaques de RSA

2 La théorie

- Qui a inventé le système RSA ?
- Pourquoi le déchiffrement marche-t-il ?
- Qu'est-ce-qui garantit la sécurité du système RSA ?

Qui a inventé le système RSA ?

1 La pratique

- Fabrication d'un chiffre RSA
- Chiffrement
- Déchiffrement
- Attaques de RSA

2 La théorie

- Qui a inventé le système RSA ?
- Pourquoi le déchiffrement marche-t-il ?
- Qu'est-ce-qui garantit la sécurité du système RSA ?

Qui a inventé le système RSA ?

Origine



Idée présentée en 1978 par
Ronald Rivest, Adi Shamir
et Leonard Adleman dans
l'article :

R.L. Rivest, A. Shamir, and L. Adleman. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the Association for Computing Machinery*, 21(2) :120-126, 1978.

Le nom de ce procédé est composé des initiales des noms de famille de ses inventeurs : **R**(ivest)**S**(hamir)**A**(dleman).

Pourquoi le déchiffrement marche-t-il ?

1 La pratique

- Fabrication d'un chiffre RSA
- Chiffrement
- Déchiffrement
- Attaques de RSA

2 La théorie

- Qui a inventé le système RSA ?
- Pourquoi le déchiffrement marche-t-il ?
- Qu'est-ce-qui garantit la sécurité du système RSA ?

Premier outil mathématique pour RSA

Propriété

*Pour tous entiers naturels a, b, c, d ,
si c et d sont premiers entre eux, et si*
$$\begin{cases} a \equiv b \pmod{c} \\ a \equiv b \pmod{d} \end{cases}$$
alors on a

$$a \equiv b \pmod{c \times d}$$

Deuxième outil mathématique pour RSA

Théorème (Fermat)

Soit p un nombre premier et soit a un entier premier avec p . Alors on a

$$a^{(p-1)} \equiv 1 \pmod{p}$$

Déchiffrement RSA

Question

- Pour déchiffrer, on calcule $M' \equiv C^D \pmod N$
- Pour chiffrer, on a calculé $C \equiv M^E \pmod N$
- Donc on a

$$M' \equiv M^{ED} \pmod N$$

- Pourquoi retrouve-t-on M ?

Déchiffrement RSA

Rappels

- On a $N = p \times q$ où p et q sont deux nombres premiers différents
- Et aussi $D \equiv E^{-1} \pmod{\varphi}$
- Ce qui peut s'écrire $ED \equiv 1 \pmod{\varphi}$
- Avec $\varphi = (p - 1) \times (q - 1)$

Déchiffrement RSA

Finalement, la question est :

Pourquoi a-t-on

$$M^{ED} \equiv M \pmod{pq}$$

lorsque

$$ED \equiv 1 \pmod{(p-1)(q-1)}$$

et que p et q sont deux nombres premiers différents ?

Déchiffrement RSA

Utilisation du premier outil

Comme p et q sont des nombres premiers différents, ils sont premiers entre eux, donc si on montre que

$$\begin{cases} M^{ED} \equiv M \pmod{p} \\ M^{ED} \equiv M \pmod{q} \end{cases}$$

alors on peut conclure que

$$M^{ED} \equiv M \pmod{pq}$$

Déchiffrement RSA

Commençons par p

Pourquoi a-t-on $M^{ED} \equiv M \pmod{p}$
lorsque $ED \equiv 1 \pmod{(p-1)(q-1)}$
et que p est un nombre premier ?

Premier cas : si p divise M

- Alors on a $M \equiv 0 \pmod{p}$
- Et bien sûr aussi $M^{ED} \equiv 0 \pmod{p}$
- Donc on a bien $M^{ED} \equiv M \pmod{p}$
- Ça ne dépend même pas de E et D

Déchiffrement RSA

Commençons par p

Pourquoi a-t-on $M^{ED} \equiv M \pmod{p}$
lorsque $ED \equiv 1 \pmod{(p-1)(q-1)}$
et que p est un nombre premier ?

Deuxième cas : si p ne divise pas M

- Comme p est premier, M est en fait premier avec p
- On peut utiliser le deuxième outil : le théorème de Fermat
- On a donc $M^{p-1} \equiv 1 \pmod{p}$

Déchiffrement RSA

Commençons par p

Pourquoi a-t-on $M^{ED} \equiv M \pmod{p}$
lorsque $ED \equiv 1 \pmod{(p-1)(q-1)}$
et que p est un nombre premier ?

Deuxième cas : si p ne divise pas M (fin)

- D'un autre côté, $ED \equiv 1 \pmod{(p-1)(q-1)}$ signifie qu'il existe un entier $k \geq 1$ tel que $ED = 1 + k(p-1)(q-1)$
- Et donc

$$M^{ED} = M^{1+k(p-1)(q-1)} = M \times (M^{p-1})^{k(q-1)}$$

Déchiffrement RSA

Commençons par p

Pourquoi a-t-on $M^{ED} \equiv M \pmod{p}$
lorsque $ED \equiv 1 \pmod{(p-1)(q-1)}$
et que p est un nombre premier ?

Deuxième cas : si p ne divise pas M (suite)

- On vient de voir que $M^{p-1} \equiv 1 \pmod{p}$
- Et aussi que $M^{ED} = M \times (M^{p-1})^{k(q-1)}$
- Autrement dit

$$M^{ED} \equiv M \times (1)^{k(q-1)} \equiv M \pmod{p}$$

Pourquoi le déchiffrement marche-t-il ?

Déchiffrement RSA

Ensuite occupons-nous de q

C'est pareil...

Déchiffrement RSA

Conclusion

Lorsque p et q sont deux nombres premiers différents et que

$$ED \equiv 1 \pmod{(p-1)(q-1)}$$

alors quelque soit l'entier naturel M , on a

$$M^{ED} \equiv M \pmod{pq}$$

c'est bien ce qu'on voulait montrer

Déchiffrement RSA

Dernière remarque

- Pour déchiffrer, on calcule $M' \equiv C^D \pmod N$
- Et on vient de voir que $M' \equiv M \pmod N$
- Comme en plus on a pris soin au départ que le message M satisfasse $M < N$, ce $\equiv$ est en fait un $=$, c.-à-d. $M' = M$
- Autrement dit on récupère bien le message d'origine

Qu'est-ce-qui garantit la sécurité du système RSA ?

1 La pratique

- Fabrication d'un chiffre RSA
- Chiffrement
- Déchiffrement
- Attaques de RSA

2 La théorie

- Qui a inventé le système RSA ?
- Pourquoi le déchiffrement marche-t-il ?
- Qu'est-ce-qui garantit la sécurité du système RSA ?

Qu'est-ce-qui garantit la sécurité du système RSA ?

Espionner = factoriser

Pour décrypter le cryptogramme C ,

- Il suffit à Mr X de connaître la clé privée d'Alice D .
- Or il sait que $D = E^{-1} \bmod \varphi(N)$.
- Comme E et N sont publics, il lui suffit de calculer $\varphi(N)$.
- Comme il sait que $N = pq$ avec p et q premiers, il sait aussi que $\varphi(N) = (p - 1)(q - 1)$
- Donc il lui suffit de calculer p et q
- Finalement, il lui suffit de factoriser $N = pq$

Pourquoi Mr X n'est-il pas capable de factoriser $N = pq$?

Qu'est-ce-qui garantit la sécurité du système RSA ?

Espionner = factoriser

- Actuellement, des facteurs premiers de 300 chiffres environ sont considérés comme sûrs car
 - les meilleurs algorithmes de factorisation connus,
 - tournant sur les meilleurs ordinateurs du marché,mettraient plusieurs années à factoriser un produit de deux nombres premiers de 300 chiffres inconnus.
- C'est pourquoi **en pratique** Mr X n'est pas capable de calculer la clé privée d'Alice.
- Moralité : La sécurité du système RSA repose sur une course-poursuite matérielle et logicielle entre
 - produire des nombres premiers aléatoires de plus en plus grands
 - factoriser de plus en plus vite

Qu'est-ce-qui garantit la sécurité du système RSA ?

Espionner = factoriser

Mais...

- On ne sait pas si une attaque du système RSA qui ne serait pas basée sur la factorisation ne pourrait pas marcher !

FIN