Le RSA

Guillaume Hervé

Le RSA est un système de chiffrement :

Le RSA est un système de chiffrement :

- asymétrique ;

Le RSA est un système de chiffrement :

- asymétrique ;
- à clé publique.

Le RSA est un système de chiffrement :

- asymétrique ;
- à clé publique.

C'est-à-dire qu'une personne donne une clé à tout le monde qui permettra de LUI envoyer un message crypté.

Le RSA est un système de chiffrement :

- asymétrique ;
- à clé publique.

C'est-à-dire qu'une personne donne une clé à tout le monde qui permettra de LUI envoyer un message crypté.

remarque

Le RSA est sûr mais il est lent et limité en longueur de message :

Le RSA est un système de chiffrement :

- asymétrique ;
- à clé publique.

C'est-à-dire qu'une personne donne une clé à tout le monde qui permettra de LUI envoyer un message crypté.

remarque

Le RSA est sûr mais il est lent et limité en longueur de message : on l'utilisera essentiellement pour coder des messages cours - typiquement un code d'identification.

Un exemple

Situation

- Alice publie une clé permettant à chacun de lui envoyer un message codé ;

Un exemple

Situation

- Alice publie une clé permettant à chacun de lui envoyer un message codé ;
- Bob va coder son message et l'envoyer crypté à Alice qui seule pourra le décoder.

Un exemple

Situation

- Alice publie une clé permettant à chacun de lui envoyer un message codé ;
- Bob va coder son message et l'envoyer crypté à Alice qui seule pourra le décoder.

Exemple

- Alice publie les clés $n = 187$ et $e = 7$.

Un exemple

Situation

- Alice publie une clé permettant à chacun de lui envoyer un message codé ;
- Bob va coder son message et l'envoyer crypté à Alice qui seule pourra le décoder.

Exemple

- Alice publie les clés $n = 187$ et $e = 7$.
  Sa clé privée est $d = 23$.

Un exemple

Situation

- Alice publie une clé permettant à chacun de lui envoyer un message codé ;
- Bob va coder son message et l'envoyer crypté à Alice qui seule pourra le décoder.

Exemple

- Alice publie les clés $n = 187$ et $e = 7$.
  Sa clé privée est $d = 23$.
- Bob veut alors envoyer le code 10 à Alice.

Un exemple

Situation

- Alice publie une clé permettant à chacun de lui envoyer un message codé ;
- Bob va coder son message et l'envoyer crypté à Alice qui seule pourra le décoder.

Exemple

- Alice publie les clés $n = 187$ et $e = 7$.
  Sa clé privée est $d = 23$.
- Bob veut alors envoyer le code 10 à Alice.
  Pour cela, il calcule de envoie 10^7 [187], soit 175.

Un exemple

Situation

- Alice publie une clé permettant à chacun de lui envoyer un message codé ;
- Bob va coder son message et l'envoyer crypté à Alice qui seule pourra le décoder.

Exemple

- Alice publie les clés $n = 187$ et $e = 7$.
  Sa clé privée est $d = 23$.
- Bob veut alors envoyer le code 10 à Alice.
  Pour cela, il calcule de envoie 10^7 [187], soit 175.
- Alice va alors décoder en calculant 175^{23} [187], soit 10.

Description plus générale

Choix des clés d'Alice

- Elle choisit deux « grands » nombre premiers p et q et calcule $n = pq$.

Description plus générale

Choix des clés d'Alice

- Elle choisit deux « grands » nombre premiers p et q et calcule $n = pq$.
  Ici $p = 11$, $q = 27$ et $n = 11 \times 17 = 187$.

Description plus générale

Choix des clés d'Alice

- Elle choisit deux « grands » nombre premiers p et q et calcule $n = pq$.
  Ici $p = 11$, $q = 27$ et $n = 11 \times 17 = 187$.
- Elle calcule l'indicatrice d'Euler de n :

Description plus générale

Choix des clés d'Alice

- Elle choisit deux « grands » nombre premiers p et q et calcule $n = pq$.
  Ici $p = 11$, $q = 27$ et $n = 11 \times 17 = 187$.
- Elle calcule l'indicatrice d'Euler de n :
  $w = \varphi(n) = (p-1)(q-1) = 10 \times 16 = 160$.

Description plus générale

Choix des clés d'Alice

- Elle choisit deux « grands » nombre premiers p et q et calcule $n = pq$.
  Ici $p = 11$, $q = 27$ et $n = 11 \times 17 = 187$.
- Elle calcule l'indicatrice d'Euler de n :
  $w = \varphi(n) = (p-1)(q-1) = 10 \times 16 = 160$.
- Elle choisit d tel que $d \wedge w = 1$ et e tel que $de \equiv 1\,[w]$.

Description plus générale

Choix des clés d'Alice

- Elle choisit deux « grands » nombre premiers p et q et calcule $n = pq$.
  Ici $p = 11$, $q = 27$ et $n = 11 \times 17 = 187$.
- Elle calcule l'indicatrice d'Euler de n :
  $w = \varphi(n) = (p-1)(q-1) = 10 \times 16 = 160$.
- Elle choisit d tel que $d \wedge w = 1$ et e tel que $de \equiv 1\,[w]$.
  Ici $d = 23$, $e = 7$, puisque $23 \times 7 - 1 \times 160 = 1$.

Description plus générale

Choix des clés d'Alice

- Elle choisit deux « grands » nombre premiers p et q et calcule $n = pq$.
  Ici $p = 11$, $q = 27$ et $n = 11 \times 17 = 187$.
- Elle calcule l'indicatrice d'Euler de n :
  $w = \varphi(n) = (p-1)(q-1) = 10 \times 16 = 160$.
- Elle choisit d tel que $d \wedge w = 1$ et e tel que $de \equiv 1\,[w]$.
  Ici $d = 23$, $e = 7$, puisque $23 \times 7 - 1 \times 160 = 1$.

Cryptage/Décryptage

Description plus générale

Choix des clés d'Alice

- Elle choisit deux « grands » nombre premiers p et q et calcule $n = pq$.
  Ici $p = 11$, $q = 27$ et $n = 11 \times 17 = 187$.
- Elle calcule l'indicatrice d'Euler de n :
  $w = \varphi(n) = (p-1)(q-1) = 10 \times 16 = 160$.
- Elle choisit d tel que $d \wedge w = 1$ et e tel que $de \equiv 1\,[w]$.
  Ici $d = 23$, $e = 7$, puisque $23 \times 7 - 1 \times 160 = 1$.

Cryptage/Décryptage

- Pour envoyer le nombre M, Bob envoie $C \equiv M^e\,[n]$.

Description plus générale

Choix des clés d'Alice

- Elle choisit deux « grands » nombre premiers p et q et calcule $n = pq$.
  Ici $p = 11$, $q = 27$ et $n = 11 \times 17 = 187$.
- Elle calcule l'indicatrice d'Euler de n :
  $w = \varphi(n) = (p-1)(q-1) = 10 \times 16 = 160$.
- Elle choisit d tel que $d \wedge w = 1$ et e tel que $de \equiv 1\,[w]$.
  Ici $d = 23$, $e = 7$, puisque $23 \times 7 - 1 \times 160 = 1$.

Cryptage/Décryptage

- Pour envoyer le nombre M, Bob envoie $C \equiv M^e\,[n]$.
- Pour décrypter le message, Alice calcule $C^d\,[n]$.

Description plus générale

Choix des clés d'Alice

- Elle choisit deux « grands » nombre premiers p et q et calcule $n = pq$.
  Ici $p = 11$, $q = 27$ et $n = 11 \times 17 = 187$.
- Elle calcule l'indicatrice d'Euler de n :
  $w = \varphi(n) = (p-1)(q-1) = 10 \times 16 = 160$.
- Elle choisit d tel que $d \wedge w = 1$ et e tel que $de \equiv 1\,[w]$.
  Ici $d = 23$, $e = 7$, puisque $23 \times 7 - 1 \times 160 = 1$.

Cryptage/Décryptage

- Pour envoyer le nombre M, Bob envoie $C \equiv M^e\,[n]$.
- Pour décrypter le message, Alice calcule $C^d\,[n]$.
- L'algorithme repose donc sur le fait que $(M^e)^d \equiv M\,[n]$.

Théorème

Soit $(n, a) \in \mathbb{N}^2$ *tel que* $a \wedge n = 1$. *Alors*

$$a^{\varphi(n)} \equiv 1\,[n].$$

Théorème

Soit $(n, a) \in \mathbb{N}^2$ *tel que* $a \wedge n = 1$. *Alors*

$$a^{\varphi(n)} \equiv 1\,[n].$$

Indicatrice d'Euler

L'indicatrice d'Euler d'une entier n est

$$\varphi(n) = \text{Card}\{k \in [\![1, n]\!] \mid k \wedge n = 1\} = \text{Card}\left(\mathcal{U}(\mathbb{Z}/n.\mathbb{Z})\right).$$

Théorème

Soit $(n, a) \in \mathbb{N}^2$ *tel que* $a \wedge n = 1$. *Alors*

$$a^{\varphi(n)} \equiv 1\,[n].$$

Indicatrice d'Euler

L'indicatrice d'Euler d'une entier n est

$$\varphi(n) = \text{Card}\{k \in [\![1, n]\!] \mid k \wedge n = 1\} = \text{Card}\left(\mathcal{U}(\mathbb{Z}/n.\mathbb{Z})\right).$$

- Si $n \in \mathbb{P}$, $\varphi(n) = n - 1$.

Théorème

Soit $(n, a) \in \mathbb{N}^2$ *tel que* $a \wedge n = 1$. *Alors*

$$a^{\varphi(n)} \equiv 1\,[n].$$

Indicatrice d'Euler

L'indicatrice d'Euler d'une entier n est

$$\varphi(n) = \text{Card}\{k \in [\![1, n]\!] \mid k \wedge n = 1\} = \text{Card}\left(\mathcal{U}(\mathbb{Z}/n.\mathbb{Z})\right).$$

- Si $n \in \mathbb{P}$, $\varphi(n) = n - 1$.
- Si $n = pq$ avec $p, q \in \mathbb{P}$, alors $\varphi(n) = (p-1)(q-1)$.

Situation

On a

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

Situation

On a

- $n = pq$ et $\varphi(n) = w = (p-1)(q-1)$;
- $d \wedge w = 1$ donc (Bezout) on dispose de e tel que

$$de \equiv 1\,[w].$$

Situation

On a

- $n = pq$ et $\varphi(n) = w = (p-1)(q-1)$;
- $d \wedge w = 1$ donc (Bezout) on dispose de e tel que

$$de \equiv 1\,[w].$$

Preuve de l'algorithme

Pour tout entier M, on a $(M^e)^d \equiv M[n]$.

Situation

On a

- $n = pq$ et $\varphi(n) = w = (p-1)(q-1)$;
- $d \wedge w = 1$ donc (Bezout) on dispose de e tel que

$$de \equiv 1\,[w].$$

Preuve de l'algorithme

Pour tout entier M, on a $(M^e)^d \equiv M[n]$.

On note que si $M \wedge n = 1$, c'est le théorème précédent.

Situation

On a

- $n = pq$ et $\varphi(n) = w = (p-1)(q-1)$;
- $d \wedge w = 1$ donc (Bezout) on dispose de e tel que

$$de \equiv 1\,[w].$$

Preuve de l'algorithme

Pour tout entier M, on a $(M^e)^d \equiv M[n]$.

On note que si $M \wedge n = 1$, c'est le théorème précédent.
Comme $M < n = pq$,
Il suffit alors de traiter le cas $M = p^\alpha \times m$ avec $m \wedge pq = 1$.

Pour la recherche des clés, Alice a besoin de :

- deux gros nombres premiers p et q :

Pour la recherche des clés, Alice a besoin de :

- deux gros nombres premiers p et q :
  c'est un problème (difficile) à part entière.

Pour la recherche des clés, Alice a besoin de :

- deux gros nombres premiers p et q :
  c'est un problème (difficile) à part entière.
- de d tel que $d \wedge w = 1$ puis de e tel que $de \equiv 1\,[w]$:

Pour la recherche des clés, Alice a besoin de :

- deux gros nombres premiers p et q :
  c'est un problème (difficile) à part entière.
- de d tel que $d \wedge w = 1$ puis de e tel que $de \equiv 1\,[w]$:
  on utilise l'algorithme d'Euclide étendu.

Position du problème

- Pour attaquer le RSA, le hacker doit trouver la décomposition $n = p \times q$.

Position du problème

- Pour attaquer le RSA, le hacker doit trouver la décomposition $n = p \times q$.
- Pendant ce temps, Bob doit calculer $M^e\,[n]$ puis Alice doit calculer $(M^e)^d\,[n]$.

Position du problème

- Pour attaquer le RSA, le hacker doit trouver la décomposition $n = p \times q$.
- Pendant ce temps, Bob doit calculer $M^e\,[n]$ puis Alice doit calculer $(M^e)^d\,[n]$.
- Ces deux opérations doivent être les plus rapides possibles.

Position du problème

- Pour attaquer le RSA, le hacker doit trouver la décomposition $n = p \times q$.
- Pendant ce temps, Bob doit calculer $M^e\,[n]$ puis Alice doit calculer $(M^e)^d\,[n]$.
- Ces deux opérations doivent être les plus rapides possibles.
- Alice a tout le temps qu'elle veut pour choisir ses clés.

Position du problème

- Pour attaquer le RSA, le hacker doit trouver la décomposition $n = p \times q$.
- Pendant ce temps, Bob doit calculer $M^e\,[n]$ puis Alice doit calculer $(M^e)^d\,[n]$.
- Ces deux opérations doivent être les plus rapides possibles.
- Alice a tout le temps qu'elle veut pour choisir ses clés.

Solution

- Notons que l'on va toujours calculer modulo n : cela limite grandement les ordres de grandeurs des calculs !

Position du problème

- Pour attaquer le RSA, le hacker doit trouver la décomposition $n = p \times q$.
- Pendant ce temps, Bob doit calculer $M^e\,[n]$ puis Alice doit calculer $(M^e)^d\,[n]$.
- Ces deux opérations doivent être les plus rapides possibles.
- Alice a tout le temps qu'elle veut pour choisir ses clés.

Solution

- Notons que l'on va toujours calculer modulo n : cela limite grandement les ordres de grandeurs des calculs !
- On utilise l'algorithme d'exponentiation rapide pour calculer plus rapidement M^e (et $(M^e)^d$).

exemple : calcul de 10^7 [187]

- On note que $7 = 1 + 2^1 + 2^2$.

exemple : calcul de $10^7\,[187]$

- On note que $7 = 1 + 2^1 + 2^2$.
- On calcule : $10^2 \equiv 100\,[187]$

exemple : calcul de $10^7\,[187]$

- On note que $7 = 1 + 2^1 + 2^2$.
- On calcule : $10^2 \equiv 100\,[187]$ puis
  $10^4 = (10^2)^2 = 10000 = 53 * 187 + 89 \equiv 89\,[187]$;

exemple : calcul de $10^7\,[187]$

- On note que $7 = 1 + 2^1 + 2^2$.
- On calcule : $10^2 \equiv 100\,[187]$ puis
  $10^4 = (10^2)^2 = 10000 = 53 * 187 + 89 \equiv 89\,[187]$;
- Enfin, $10^7 \equiv (10 \times 10^2) \times 10^4 \equiv 65 \times 89 \equiv 5785 \equiv 175\,[187]$.

exemple : calcul de $10^7\,[187]$

- On note que $7 = 1 + 2^1 + 2^2$.
- On calcule : $10^2 \equiv 100\,[187]$ puis
  $10^4 = (10^2)^2 = 10000 = 53 * 187 + 89 \equiv 89\,[187]$;
- Enfin, $10^7 \equiv (10 \times 10^2) \times 10^4 \equiv 65 \times 89 \equiv 5785 \equiv 175\,[187]$.

exemple : calcul de $(10^7)^{23}\,[187] \equiv 175^{23}\,[187]$

- On note que $23 = 1 + 2 + 2^2 + 2^4$

exemple : calcul de $10^7\,[187]$

- On note que $7 = 1 + 2^1 + 2^2$.
- On calcule : $10^2 \equiv 100\,[187]$ puis
  $10^4 = (10^2)^2 = 10000 = 53 * 187 + 89 \equiv 89\,[187]$;
- Enfin, $10^7 \equiv (10 \times 10^2) \times 10^4 \equiv 65 \times 89 \equiv 5785 \equiv 175\,[187]$.

exemple : calcul de $(10^7)^{23}\,[187] \equiv 175^{23}\,[187]$

- On note que $23 = 1 + 2 + 2^2 + 2^4$
- On calcule $175^2 = 30625 \equiv 144\,[187]$

exemple : calcul de $10^7\,[187]$

- On note que $7 = 1 + 2^1 + 2^2$.
- On calcule : $10^2 \equiv 100\,[187]$ puis
  $10^4 = (10^2)^2 = 10000 = 53 * 187 + 89 \equiv 89\,[187]$;
- Enfin, $10^7 \equiv (10 \times 10^2) \times 10^4 \equiv 65 \times 89 \equiv 5785 \equiv 175\,[187]$.

exemple : calcul de $(10^7)^{23}\,[187] \equiv 175^{23}\,[187]$

- On note que $23 = 1 + 2 + 2^2 + 2^4$
- On calcule $175^2 = 30625 \equiv 144\,[187]$ puis $175^4 = 144^2 = 20736 \equiv 166\,[187]$,

exemple : calcul de $10^7\,[187]$

- On note que $7 = 1 + 2^1 + 2^2$.
- On calcule : $10^2 \equiv 100\,[187]$ puis
  $10^4 = (10^2)^2 = 10000 = 53 * 187 + 89 \equiv 89\,[187]$;
- Enfin, $10^7 \equiv (10 \times 10^2) \times 10^4 \equiv 65 \times 89 \equiv 5785 \equiv 175\,[187]$.

exemple : calcul de $(10^7)^{23}\,[187] \equiv 175^{23}\,[187]$

- On note que $23 = 1 + 2 + 2^2 + 2^4$
- On calcule $175^2 = 30625 \equiv 144\,[187]$ puis $175^4 = 144^2 = 20736 \equiv 166\,[187]$,
  puis $175^8 = 166^2 = 27556 \equiv 67\,[187]$,

exemple : calcul de $10^7\,[187]$

- On note que $7 = 1 + 2^1 + 2^2$.
- On calcule : $10^2 \equiv 100\,[187]$ puis
  $10^4 = (10^2)^2 = 10000 = 53 * 187 + 89 \equiv 89\,[187]$;
- Enfin, $10^7 \equiv (10 \times 10^2) \times 10^4 \equiv 65 \times 89 \equiv 5785 \equiv 175\,[187]$.

exemple : calcul de $(10^7)^{23}\,[187] \equiv 175^{23}\,[187]$

- On note que $23 = 1 + 2 + 2^2 + 2^4$
- On calcule $175^2 = 30625 \equiv 144\,[187]$ puis $175^4 = 144^2 = 20736 \equiv 166\,[187]$,
  puis $175^8 = 166^2 = 27556 \equiv 67\,[187]$, et $175^{16} = 67^2 = 4489 \equiv 1\,[187]$.

exemple : calcul de $10^7\,[187]$

- On note que $7 = 1 + 2^1 + 2^2$.
- On calcule : $10^2 \equiv 100\,[187]$ puis
  $10^4 = (10^2)^2 = 10000 = 53 * 187 + 89 \equiv 89\,[187]$;
- Enfin, $10^7 \equiv (10 \times 10^2) \times 10^4 \equiv 65 \times 89 \equiv 5785 \equiv 175\,[187]$.

exemple : calcul de $(10^7)^{23}\,[187] \equiv 175^{23}\,[187]$

- On note que $23 = 1 + 2 + 2^2 + 2^4$
- On calcule $175^2 = 30625 \equiv 144\,[187]$ puis $175^4 = 144^2 = 20736 \equiv 166\,[187]$,
  puis $175^8 = 166^2 = 27556 \equiv 67\,[187]$, et $175^{16} = 67^2 = 4489 \equiv 1\,[187]$.
- Enfin, $175^{23} = 175 \times 175^2 \times 175^4 \times 175^{16}$
  $\equiv 175 \times 144 \times 166 \times 1 \equiv 25200 \times 166$
  $\equiv 142 \times 166 \equiv 23572 \equiv 10\,[187]$.