RSA

Rivest, Shamir, Adleman

Yann Rotella

UVSQ - Université Paris-Saclay

2 avril 2026

Plan du Cours

Arithmétique nécessaire

RSA

ARITHMÉTIQUE NÉCESSAIRE

RSA

Classes de congruence

$$(\mathbb{Z}, +, \times)$$

Soit $n \in \mathbb{N}^*$, on considère la relation $\mathcal{R}$ suivante :

$$a \mathcal{R} b \text{ si et seulement si } a = b \mod n$$

Classes de congruence

$$(\mathbb{Z}, +, \times)$$

Soit $n \in \mathbb{N}^*$, on considère la relation $\mathcal{R}$ suivante :

$$a\mathcal{R}b \text{ si et seulement si } a = b \mod n$$

✍ Rappeler ce qu'est une relation d'équivalence

CLASSES DE CONGRUENCE

$$(\mathbb{Z}, +, \times)$$

Soit $n \in \mathbb{N}^*$, on considère la relation $\mathcal{R}$ suivante :

$$a \mathcal{R} b \text{ si et seulement si } a = b \mod n$$

- ✍ Rappeler ce qu'est une relation d'équivalence
- ✍ Montrer que la relation $\mathcal{R}$ est une relation d'équivalence

Classes de congruence

$$(\mathbb{Z}, +, \times)$$

Soit $n \in \mathbb{N}^*$, on considère la relation $\mathcal{R}$ suivante :

$$a\mathcal{R}b \text{ si et seulement si } a = b \mod n$$

✍ Rappeler ce qu'est une relation d'équivalence

✍ Montrer que la relation $\mathcal{R}$ est une relation d'équivalence

Pour tout $a \in \mathbb{Z}$, on note $C(a)$ la classe d'équivalence de a.

Classes de congruence

$$(\mathbb{Z}, +, \times)$$

Soit $n \in \mathbb{N}^*$, on considère la relation $\mathcal{R}$ suivante :

$$a \mathcal{R} b \text{ si et seulement si } a = b \mod n$$

- ✍ Rappeler ce qu'est une relation d'équivalence
- ✍ Montrer que la relation $\mathcal{R}$ est une relation d'équivalence

Pour tout $a \in \mathbb{Z}$, on note $C(a)$ la classe d'équivalence de a. Pour tout $a, b \in \mathbb{Z}$, on a

$$C(a) + C(b) = C(a + b)$$

et

$$C(a) \times C(b) = C(a \times b)$$

CLASSES DE CONGURENCE

Soit $n \in \mathbb{N}^*$,

$$\mathbb{Z}/n\mathbb{Z} = \{C(0), C(1), C(2), \ldots, C(n-1)\}$$

Classes de congruence

Soit $n \in \mathbb{N}^*$,

$$\mathbb{Z}/n\mathbb{Z} = \{C(0), C(1), C(2), \ldots, C(n-1)\}$$

$$\mathbb{Z}/n\mathbb{Z} = \{0, 1, 2, \cdots, n-1\}$$

Classes de congurence

Soit $n \in \mathbb{N}^*$,

$$\mathbb{Z}/n\mathbb{Z} = \{C(0), C(1), C(2), \ldots, C(n-1)\}$$

$$\mathbb{Z}/n\mathbb{Z} = \{0, 1, 2, \cdots, n-1\}$$

La loi $+$ et la loi $\times$ se définissent aussi sur cet espace appelé espace quotienté par la relation $\mathcal{R}$.

CLASSES DE CONGURENCE

Soit $n \in \mathbb{N}^*$,

$$\mathbb{Z}/n\mathbb{Z} = \{C(0), C(1), C(2), \ldots, C(n-1)\}$$

$$\mathbb{Z}/n\mathbb{Z} = \{0, 1, 2, \cdots, n-1\}$$

La loi $+$ et la loi $\times$ se définissent aussi sur cet espace appelé espace quotienté par la relation $\mathcal{R}$.

$$\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$$

Le théorème de Sun-Zi (restes chinois)

Théorème (de Sun-Zi)

Soit n et m deux entiers premiers entre eux, i.e. $\mathrm{pgcd}(n,m) = 1$. Alors pour tout $a, b \in \mathbb{Z}$ il existe une unique solution modulo nm au système d'équation

$$\begin{cases} x = a \mod n \\ x = b \mod m \end{cases}$$

Le théorème de Sun-Zi (restes chinois)

Théorème (de Sun-Zi)

Soit n et m deux entiers premiers entre eux, i.e. $\mathrm{pgcd}(n,m) = 1$*. Alors pour tout $a, b \in \mathbb{Z}$ il existe une unique solution modulo nm au système d'équation*

$$\begin{cases} x = a \mod n \\ x = b \mod m \end{cases}$$

✍ Preuve

Le théorème de Sun-Zi (restes chinois)

Théorème (de Sun-Zi)

Soit n *et* m *deux entiers premiers entre eux, i.e.* $\mathrm{pgcd}(n,m) = 1$*. Alors pour tout* $a, b \in \mathbb{Z}$ *il existe une unique solution modulo* nm *au système d'équation*

$$\begin{cases} x = a \mod n \\ x = b \mod m \end{cases}$$

- ✍ Preuve
- ✍ Que se passe t'il quand n et m ne sont pas premiers entre eux ?

ÉLÉMENTS INVERSIBLES

$(\mathbb{Z}_n, +, \times)$ est un anneau. Il se peut que des éléments ne soient pas inversibles pour la loi $\times$.

Rappel :

PROPRIÉTÉ (IDENTITÉ DE BÉZOUT)

Soit a et b deux entiers. a et b sont premiers entre eux ***si et seulement si*** *il existe $(u,v) \in \mathbb{Z}^2$ tel que*

$$au + bv = 1$$

✍ Montrer pourquoi les éléments inversibles dans $\mathbb{Z}_n$ pour la loi $\times$ sont tous les éléments premiers avec n.

Le groupe multiplicatif

Définition (Le groupe multiplicatif)

$$(\mathbb{Z}_n)^\times = \{x \in \mathbb{Z}_n \text{ inversibles pour } \times\}$$

Le groupe multiplicatif

Définition (Le groupe multiplicatif)

$$(\mathbb{Z}_n)^\times = \{x \in \mathbb{Z}_n \textit{ inversibles pour } \times\}$$

c'est-à-dire tous les éléments premiers avec n dans $\{0, 1, \cdots, n-1\}$.

L'indicatrice d'Euler

Définition (L'indicatrice d'Euler)

L'indicatrice d'Euler notée ϕ *est une fonction de* $\mathbb{N}^*$ *dans* $\mathbb{N}^*$ *qui « compte » le nombre d'éléments premiers et inférieurs ou égaux à* n *où* n *est l'entrée de la fonction :*

$$\begin{aligned}\varphi : \mathbb{N}^* &\to \mathbb{N}^* \\ n &\mapsto |\{m \in \mathbb{N}^* | m \leq n \text{ et } m \text{ premiers avec } n\end{aligned}$$

c'est-à-dire exactement le cardinal de $(\mathbb{Z}_n)^\times$

L'indicatrice d'Euler

Définition (L'indicatrice d'Euler)

L'indicatrice d'Euler notée ϕ *est une fonction de* $\mathbb{N}^*$ *dans* $\mathbb{N}^*$ *qui « compte » le nombre d'éléments premiers et inférieurs ou égaux à* n *où* n *est l'entrée de la fonction :*

$$\begin{aligned} \varphi : \mathbb{N}^* &\to \mathbb{N}^* \\ n &\mapsto |\{m \in \mathbb{N}^* | m \leq n \text{ et } m \text{ premiers avec } n \end{aligned}$$

c'est-à-dire exactement le cardinal de $(\mathbb{Z}_n)^\times$

On peut montrer les propriétés suivantes :

L'indicatrice d'Euler

Définition (L'indicatrice d'Euler)

L'indicatrice d'Euler notée ϕ est une fonction de $\mathbb{N}^*$ dans $\mathbb{N}^*$ qui « compte » le nombre d'éléments premiers et inférieurs ou égaux à n où n est l'entrée de la fonction :

$$\begin{aligned} \varphi : \mathbb{N}^* &\to \mathbb{N}^* \\ n &\mapsto |\{m \in \mathbb{N}^* | m \leq n \text{ et } m \text{ premiers avec } n \end{aligned}$$

c'est-à-dire exactement le cardinal de $(\mathbb{Z}_n)^\times$

On peut montrer les propriétés suivantes :

- $\varphi(1) = 1$

L'indicatrice d'Euler

Définition (L'indicatrice d'Euler)

L'indicatrice d'Euler notée ϕ est une fonction de $\mathbb{N}^*$ dans $\mathbb{N}^*$ qui « compte » le nombre d'éléments premiers et inférieurs ou égaux à n où n est l'entrée de la fonction :

$$\begin{aligned}\varphi : \mathbb{N}^* &\to \mathbb{N}^* \\ n &\mapsto |\{m \in \mathbb{N}^* | m \leq n \text{ et } m \text{ premiers avec } n\end{aligned}$$

c'est-à-dire exactement le cardinal de $(\mathbb{Z}_n)^\times$

On peut montrer les propriétés suivantes :

- $\varphi(1) = 1$
- $\varphi(p) = p - 1$ pour p un nombre premier

L'INDICATRICE D'EULER

DÉFINITION (L'INDICATRICE D'EULER)

L'indicatrice d'Euler notée ϕ est une fonction de $\mathbb{N}^*$ dans $\mathbb{N}^*$ qui « compte » le nombre d'éléments premiers et inférieurs ou égaux à n où n est l'entrée de la fonction :

$$\begin{aligned} \varphi : \mathbb{N}^* &\to \mathbb{N}^* \\ n &\mapsto |\{m \in \mathbb{N}^* | m \leq n \text{ et } m \text{ premiers avec } n \end{aligned}$$

c'est-à-dire exactement le cardinal de $(\mathbb{Z}_n)^\times$

On peut montrer les propriétés suivantes :

- $\varphi(1) = 1$
- $\varphi(p) = p - 1$ pour p un nombre premier
- $\varphi(p^\alpha) = p^\alpha - p^(\alpha - 1)$ pour p premier et $\alpha \in \mathbb{N}^*$

L'indicatrice d'Euler

Définition (L'indicatrice d'Euler)

L'indicatrice d'Euler notée ϕ est une fonction de $\mathbb{N}^*$ dans $\mathbb{N}^*$ qui « compte » le nombre d'éléments premiers et inférieurs ou égaux à n où n est l'entrée de la fonction :

$$\begin{aligned} \varphi : \mathbb{N}^* &\to \mathbb{N}^* \\ n &\mapsto |\{m \in \mathbb{N}^* | m \leq n \text{ et } m \text{ premiers avec } n \end{aligned}$$

c'est-à-dire exactement le cardinal de $(\mathbb{Z}_n)^\times$

On peut montrer les propriétés suivantes :

- $\varphi(1) = 1$
- $\varphi(p) = p - 1$ pour p un nombre premier
- $\varphi(p^\alpha) = p^\alpha - p^(\alpha - 1)$ pour p premier et $\alpha \in \mathbb{N}^*$
- $\varphi(n \times m) = \phi(n) \times \phi(m)$ pour n et m premiers entre eux.

Théorème d'Euler

Théorème (Euler)

Pour tout entier $n > 0$ et tout entier a premier avec n,

$$a^{\varphi(n)} = 1 \mod n$$

Théorème d'Euler

Théorème (Euler)

Pour tout entier $n > 0$ et tout entier a premier avec n,

$$a^{\varphi(n)} = 1 \mod n$$

✍ Rappeler le théorème de Lagrange

Théorème d'Euler

Théorème (Euler)

Pour tout entier $n > 0$ et tout entier a premier avec n,

$$a^{\varphi(n)} = 1 \mod n$$

- ✍ Rappeler le théorème de Lagrange
- ✍ Rappeler l'ordre d'un élément dans un groupe

Théorème d'Euler

Théorème (Euler)

Pour tout entier $n > 0$ et tout entier a premier avec n,

$$a^{\varphi(n)} = 1 \mod n$$

- ✍ Rappeler le théorème de Lagrange
- ✍ Rappeler l'ordre d'un élément dans un groupe
- ✍ En déduire une preuve du théorème d'Euler

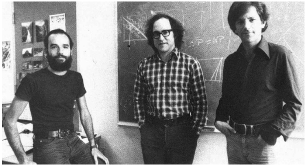
Arithmétique nécessaire

- Congruence
- Le théorème de Sun-Zi
- Le groupe multiplicatif
- L'indicatrice d'Euler

RSA

- Construction
- Sécurité de RSA
- RSA randomisé

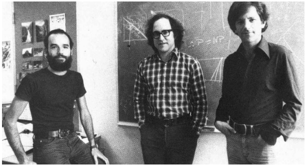
RSA - Rivest Shamir Adleman (1977)



Génération de clefs :

- p, q deux nombres premiers, $N = p \times q$, e un entier premier avec $\varphi(N)$
- $pk = (N, e)$
- $sk = d$ (et p et q et $\varphi(N)$) où d est l'inverse de e modulo $\varphi(N)$.
- $m \in \mathcal{M} = \mathbb{Z}_N = \mathcal{C}$

RSA - RIVEST SHAMIR ADLEMAN (1977)



Génération de clefs :

- p, q deux nombres premiers, $N = p \times q$, e un entier premier avec $\varphi(N)$
- $pk = (N, e)$
- $sk = d$ (et p et q et $\varphi(N)$) où d est l'inverse de e modulo $\varphi(N)$.
- $m \in \mathcal{M} = \mathbb{Z}_N = \mathcal{C}$

Chiffrement :

$$\begin{aligned} Enc : (\mathbb{N} \times \mathbb{N}) \times \mathbb{Z}_N &\to \mathbb{Z}_N \\ (N, e), m) &\mapsto c = m^e \mod N \end{aligned}$$

RSA - Rivest Shamir Adleman (1977)

p, q premiers, $N = p \times q$, e tel que $\mathrm{pgcd}(e, \varphi(N)_{)} = 1$. d l'inverse de e modulo $\varphi(N)$.

RSA - Rivest Shamir Adleman (1977)

p, q premiers, $N = p \times q$, e tel que $\mathrm{pgcd}(e, \varphi(N)_{)} = 1$. d l'inverse de e modulo $\varphi(N)$.

$$de = 1 \mod \varphi(N)$$

RSA - Rivest Shamir Adleman (1977)

p, q premiers, $N = p \times q$, e tel que $\mathrm{pgcd}(e, \varphi(N)_{)} = 1$. d l'inverse de e modulo $\varphi(N)$.

$$de = 1 \mod \varphi(N)$$

i.e. il existe $k \in \mathbb{Z}$ tel que $de = 1 + k\varphi(N)$.

RSA - Rivest Shamir Adleman (1977)

p, q premiers, $N = p \times q$, e tel que $\mathrm{pgcd}(e, \varphi(N)_)) = 1$. d l'inverse de e modulo $\varphi(N)$.

$$de = 1 \mod \varphi(N)$$

i.e. il existe $k \in \mathbb{Z}$ tel que $de = 1 + k\varphi(N)$.

$$\mathrm{pgcd}(e, \varphi(N)) = 1$$

RSA - Rivest Shamir Adleman (1977)

p, q premiers, $N = p \times q$, e tel que $\mathrm{pgcd}(e, \varphi(N)_{)} = 1$. d l'inverse de e modulo $\varphi(N)$.

$$de = 1 \mod \varphi(N)$$

i.e. il existe $k \in \mathbb{Z}$ tel que $de = 1 + k\varphi(N)$.

$$\mathrm{pgcd}(e, \varphi(N)) = 1$$

Identité de Bézout :

RSA - Rivest Shamir Adleman (1977)

p, q premiers, $N = p \times q$, e tel que $\text{pgcd}(e, \varphi(N)_{)} = 1$. d l'inverse de e modulo $\varphi(N)$.

$$de = 1 \mod \varphi(N)$$

i.e. il existe $k \in \mathbb{Z}$ tel que $de = 1 + k\varphi(N)$.

$$\text{pgcd}(e, \varphi(N)) = 1$$

Identité de Bézout : il existe (u, v) tels que

$$ue + v\varphi(N) = 1$$

RSA - Rivest Shamir Adleman (1977)

p, q premiers, $N = p \times q$, e tel que $\mathrm{pgcd}(e, \varphi(N)_{)} = 1$. d l'inverse de e modulo $\varphi(N)$.

$$de = 1 \mod \varphi(N)$$

i.e. il existe $k \in \mathbb{Z}$ tel que $de = 1 + k\varphi(N)$.

$$\mathrm{pgcd}(e, \varphi(N)) = 1$$

Identité de Bézout : il existe (u, v) tels que

$$ue + v\varphi(N) = 1$$

et

$$de + k\varphi(N) = 1$$

RSA - Rivest Shamir Adlemann (1977)

- p, q premiers
- $N = p \times q$
- e tel que $\text{pgcd}(e, \varphi(N)_{)} = 1$
- $de = 1 \mod \varphi(N)$

Chiffrement :

$$\begin{aligned} Enc : (\mathbb{N} \times \mathbb{N}) \times \mathbb{Z}/N\mathbb{Z} &\to \mathbb{Z}/N\mathbb{Z} \\ ((N, e), m) &\mapsto c = m^e \mod N \end{aligned}$$

RSA - Rivest Shamir Adlemann (1977)

- p, q premiers
- $N = p \times q$
- e tel que $\mathrm{pgcd}(e, \varphi(N)_{)} = 1$
- $de = 1 \mod \varphi(N)$

Chiffrement :

$$\begin{aligned} Enc : (\mathbb{N} \times \mathbb{N}) \times \mathbb{Z}/N\mathbb{Z} &\to \mathbb{Z}/N\mathbb{Z} \\ ((N, e), m) &\mapsto c = m^e \mod N \end{aligned}$$

Déchiffrement :

$$\begin{aligned} Dec : \mathbb{N} \times \mathbb{Z}/N\mathbb{Z} &\to \mathbb{Z}/N\mathbb{Z} \\ (d, c) &\mapsto m = c^d \mod N \end{aligned}$$

RSA - Rivest Shamir Adlemann (1977)

- p, q premiers
- $N = p \times q$
- e tel que $\text{pgcd}(e, \varphi(N)_{)} = 1$
- $de = 1 \mod \varphi(N)$

Chiffrement :

$$\begin{aligned} Enc : (\mathbb{N} \times \mathbb{N}) \times \mathbb{Z}/N\mathbb{Z} &\to \mathbb{Z}/N\mathbb{Z} \\ ((N, e), m) &\mapsto c = m^e \mod N \end{aligned}$$

Déchiffrement :

$$\begin{aligned} Dec : \mathbb{N} \times \mathbb{Z}/N\mathbb{Z} &\to \mathbb{Z}/N\mathbb{Z} \\ (d, c) &\mapsto m = c^d \mod N \end{aligned}$$

✍ Montrer quand m est premier avec N que le chiffrement est correct. (cas non premier en TD)

RSA - Rivest Shamir Adlemann (1977)

- p, q premiers
- $N = p \times q$
- e tel que $\mathrm{pgcd}(e, \varphi(N)_{)} = 1$
- $de = 1 \mod \varphi(N)$

Chiffrement :

$$\begin{aligned} Enc : (\mathbb{N} \times \mathbb{N}) \times \mathbb{Z}/N\mathbb{Z} &\to \mathbb{Z}/N\mathbb{Z} \\ ((N, e), m) &\mapsto c = m^e \mod N \end{aligned}$$

Déchiffrement :

$$\begin{aligned} Dec : \mathbb{N} \times \mathbb{Z}/N\mathbb{Z} &\to \mathbb{Z}/N\mathbb{Z} \\ (d, c) &\mapsto m = c^d \mod N \end{aligned}$$

✍ Montrer quand m est premier avec N que le chiffrement est correct. (cas non premier en TD)

✍ Montrer pourquoi, même si $sk = d$, les autres valeurs q, p et $\varphi(N)$ doivent aussi rester secrètes.

RSA EST-IL IND-CPA ?

✍ Rappeler la définition d'IND-CPA.

RSA EST-IL IND-CPA ?

- ✍ Rappeler la définition d'IND-CPA.
- ✍ RSA et-il IND-CPA ?

RSA EST-IL IND-CPA ?

- ✍ Rappeler la définition d'IND-CPA.
- ✍ RSA et-il IND-CPA ?
- ✍ En une phrase dire pourquoi RSA n'est pas IND-CPA.

RSA EST-IL IND-CPA ?

- ✍ Rappeler la définition d'IND-CPA.
- ✍ RSA et-il IND-CPA ?
- ✍ En une phrase dire pourquoi RSA n'est pas IND-CPA.

On doit « randomiser » le chiffrement !

RSA randomisé - un essai à la ElGamal

Chiffrement ElGamal :

$$\begin{aligned} Enc : G \times G &\to G \times \mathbb{Z}/n\mathbb{Z} \\ (pk, m) &\mapsto (m \cdot pk^r, g^r) = (m \cdot g^{rsk}, g^r) \end{aligned}$$

où r est une valeur tirée aléatoirement dans $\mathbb{Z}_n$.

RSA randomisé - un essai à la ElGamal

Chiffrement ElGamal :

$$\begin{aligned} Enc : G \times G &\to G \times \mathbb{Z}/n\mathbb{Z} \\ (pk, m) &\mapsto (m \cdot pk^{r}, g^{r}) = (m \cdot g^{rsk}, g^{r}) \end{aligned}$$

où r est une valeur tirée aléatoirement dans $\mathbb{Z}_n$.

Proposition avec RSA :

RSA randomisé - un essai à la ElGamal

Chiffrement ElGamal :

$$\begin{aligned} Enc : G \times G &\to G \times \mathbb{Z}/n\mathbb{Z} \\ (pk, m) &\mapsto (m \cdot pk^r, g^r) = (m \cdot g^{rsk}, g^r) \end{aligned}$$

où r est une valeur tirée aléatoirement dans $\mathbb{Z}_n$.

Proposition avec RSA :

$$c_1 = r + m^e \mod N$$

RSA RANDOMISÉ - UN ESSAI À LA ELGAMAL

Chiffrement ElGamal :

$$Enc : G \times G \to G \times \mathbb{Z}/n\mathbb{Z}$$
$$(pk, m) \mapsto (m \cdot pk^r, g^r) = (m \cdot g^{rsk}, g^r)$$

où r est une valeur tirée aléatoirement dans $\mathbb{Z}_n$.

Proposition avec RSA :

$$c_1 = r + m^e \mod N$$

$$c_2 = r^e \mod N$$

RSA randomisé - un essai à la ElGamal

Chiffrement ElGamal :

$$\begin{aligned} Enc : G \times G &\to G \times \mathbb{Z}/n\mathbb{Z} \\ (pk, m) &\mapsto (m \cdot pk^r, g^r) = (m \cdot g^{rsk}, g^r) \end{aligned}$$

où r est une valeur tirée aléatoirement dans $\mathbb{Z}_n$.

Proposition avec RSA :

$$c_1 = r + m^e \mod N$$

$$c_2 = r^e \mod N$$

$$c = (c_1, c_2)$$

RSA randomisé - un essai à la ElGamal

Chiffrement ElGamal :

$$Enc : G \times G \to G \times \mathbb{Z}/n\mathbb{Z}$$
$$(pk, m) \mapsto (m \cdot pk^r, g^r) = (m \cdot g^{rsk}, g^r)$$

où r est une valeur tirée aléatoirement dans $\mathbb{Z}_n$.

Proposition avec RSA :

$$c_1 = r + m^e \mod N$$

$$c_2 = r^e \mod N$$

$$c = (c_1, c_2)$$

- ✍ Donner la procédure de déchiffrement (cf TD)
- ✍ Montrer que ce chiffrement n'est toujours pas IND-CPA (début du TD TODO NUMBER)

RSA randomisé - concaténation d'aléa

PKCS#1v1.5 :

RSA randomisé - concaténation d'aléa

PKCS#1v1.5 :

PKCS : Public-Key Cryptography Standards

$$c = (\texttt{0x00}||\texttt{0x02}||v||\texttt{0x00}||m)^e \mod N$$

RSA randomisé - concaténation d'aléa

PKCS#1v1.5 :
PKCS : Public-Key Cryptography Standards

$$c = (\texttt{0x00}||\texttt{0x02}||v||\texttt{0x00}||m)^e \mod N$$

Cassé - Bleichenbacher (cf TD)

RSA OAEP

OAEP : Optimal Asymmetric Encryption Padding
Soit $n = \lfloor \log_2(N) \rfloor$. Soit $\ell < n$.

RSA OAEP

OAEP : Optimal Asymmetric Encryption Padding
Soit $n = \lfloor \log_2(N) \rfloor$. Soit $\ell < n$.
Soit

$$G : \{0,1\}^\ell \to \{0,1\}^n$$

un générateur pseudo-aléatoire.

RSA OAEP

OAEP : Optimal Asymmetric Encryption Padding

Soit $n = \lfloor \log_2(N) \rfloor$. Soit $\ell < n$.

Soit

$$G : \{0,1\}^{\ell} \to \{0,1\}^{n}$$

un générateur pseudo-aléatoire.

Et soit

$$H : \{0,1\}^{n} \to \{0,1\}^{\ell}$$

une fonction de compression.

RSA OAEP

OAEP : Optimal Asymmetric Encryption Padding
Soit $n = \lfloor \log_2(N) \rfloor$. Soit $\ell < n$.
Soit

$$G : \{0,1\}^{\ell} \to \{0,1\}^{n}$$

un générateur pseudo-aléatoire.
Et soit

$$H : \{0,1\}^{n} \to \{0,1\}^{\ell}$$

une fonction de compression.
$\mathcal{M} = \{0,1\}^{n-\ell}$ et $\mathcal{C} = \mathbb{Z}_N \approx \{0,1\}^{n}$

$$\begin{aligned} Enc : (\mathbb{N} \times \mathbb{N}) \times \{0,1\}^{n-\ell} &\to \mathbb{Z}_N \\ (N, e, m) &\mapsto (m \oplus G(r) || r \oplus H(m \oplus G(r)))^{e} \end{aligned}$$

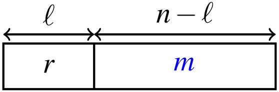
RSA OAEP

$$\begin{aligned} Enc : (\mathbb{N} \times \mathbb{N}) \times \{0,1\}^{n-\ell} &\to \mathbb{Z}_N \\ (N, e, m) &\mapsto (m \oplus G(r) || r \oplus H(m \oplus G(r)))^e \end{aligned}$$

r	m

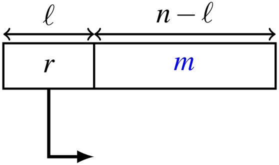
RSA OAEP

$$
\begin{aligned}
Enc : (\mathbb{N} \times \mathbb{N}) \times \{0,1\}^{n-\ell} &\to \mathbb{Z}_N \\
(N, e, m) &\mapsto (m \oplus G(r) || r \oplus H(m \oplus G(r)))^e
\end{aligned}
$$



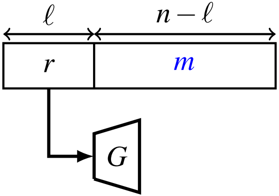
RSA OAEP

$$\begin{aligned} Enc : (\mathbb{N} \times \mathbb{N}) \times \{0,1\}^{n-\ell} &\to \mathbb{Z}_N \\ (N, e, m) &\mapsto (m \oplus G(r) || r \oplus H(m \oplus G(r)))^e \end{aligned}$$



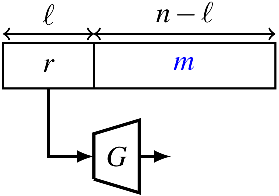
RSA OAEP

$$\begin{aligned} Enc : (\mathbb{N} \times \mathbb{N}) \times \{0,1\}^{n-\ell} &\to \mathbb{Z}_N \\ (N, e, m) &\mapsto (m \oplus G(r) || r \oplus H(m \oplus G(r)))^e \end{aligned}$$



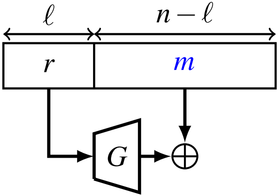
RSA OAEP

$$\begin{aligned} Enc : (\mathbb{N} \times \mathbb{N}) \times \{0,1\}^{n-\ell} &\to \mathbb{Z}_N \\ (N, e, m) &\mapsto (m \oplus G(r) || r \oplus H(m \oplus G(r)))^e \end{aligned}$$



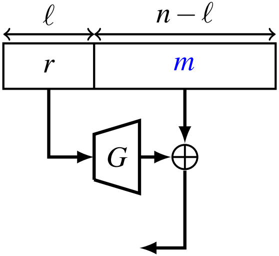
RSA OAEP

$$Enc : (\mathbb{N} \times \mathbb{N}) \times \{0,1\}^{n-\ell} \to \mathbb{Z}_N$$
$$(N, e, m) \mapsto (m \oplus G(r) || r \oplus H(m \oplus G(r)))^e$$



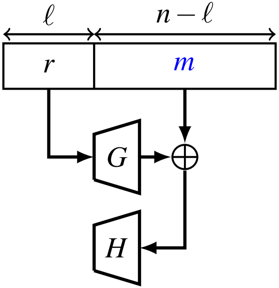
RSA OAEP

$$
\begin{aligned}
Enc : (\mathbb{N} \times \mathbb{N}) \times \{0,1\}^{n-\ell} &\to \mathbb{Z}_N \\
(N, e, m) &\mapsto (m \oplus G(r) || r \oplus H(m \oplus G(r)))^e
\end{aligned}
$$



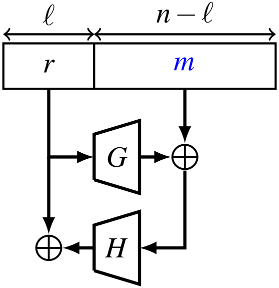
RSA OAEP

$$Enc : (\mathbb{N} \times \mathbb{N}) \times \{0,1\}^{n-\ell} \to \mathbb{Z}_N$$
$$(N, e, m) \mapsto (m \oplus G(r) || r \oplus H(m \oplus G(r)))^e$$



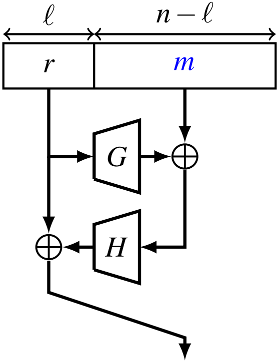
RSA OAEP

$$
\begin{aligned}
Enc : (\mathbb{N} \times \mathbb{N}) \times \{0,1\}^{n-\ell} &\to \mathbb{Z}_N \\
(N, e, m) &\mapsto (m \oplus G(r) || r \oplus H(m \oplus G(r)))^e
\end{aligned}
$$



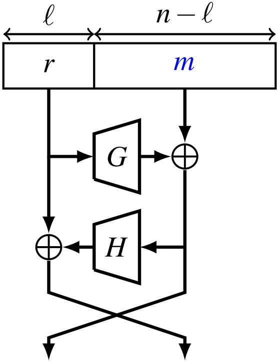
RSA OAEP

$$
\begin{aligned}
Enc : (\mathbb{N} \times \mathbb{N}) \times \{0,1\}^{n-\ell} &\to \mathbb{Z}_N \\
(N, e, m) &\mapsto (m \oplus G(r) || r \oplus H(m \oplus G(r)))^e
\end{aligned}
$$



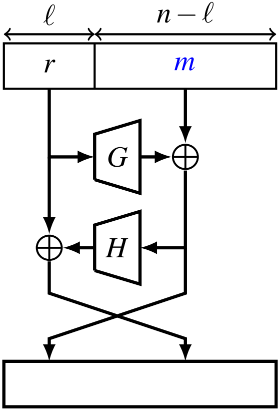
RSA OAEP

$$Enc : (\mathbb{N} \times \mathbb{N}) \times \{0,1\}^{n-\ell} \to \mathbb{Z}_N$$
$$(N, e, m) \mapsto (m \oplus G(r) || r \oplus H(m \oplus G(r)))^e$$



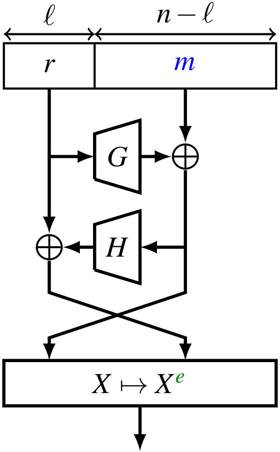
RSA OAEP

$$Enc : (\mathbb{N} \times \mathbb{N}) \times \{0,1\}^{n-\ell} \to \mathbb{Z}_N$$
$$(N, e, m) \mapsto (m \oplus G(r) || r \oplus H(m \oplus G(r)))^e$$



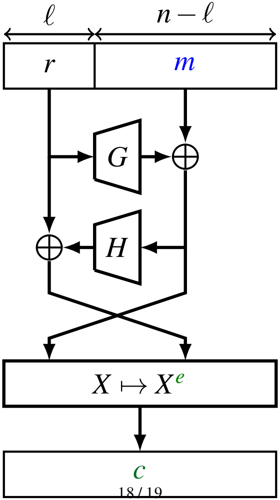
RSA OAEP

$$Enc : (\mathbb{N} \times \mathbb{N}) \times \{0,1\}^{n-\ell} \to \mathbb{Z}_N$$
$$(N, e, m) \mapsto (m \oplus G(r) || r \oplus H(m \oplus G(r)))^e$$



RSA OAEP

$$\begin{aligned} Enc : (\mathbb{N} \times \mathbb{N}) \times \{0,1\}^{n-\ell} &\to \mathbb{Z}_N \\ (N, e, m) &\mapsto (m \oplus G(r) || r \oplus H(m \oplus G(r)))^e \end{aligned}$$



CONCLUSION

- Rappels congruence : modulos à comprenadre et connaître ++

Conclusion

- Rappels congruence : modulos à comprenadre et connaître ++
- Théorème de Sun-Zi (restes chinois)

CONCLUSION

- Rappels congruence : modulos à comprenadre et connaître ++
- Théorème de Sun-Zi (restes chinois)
- Éléments inversibles, groupe multiplicatif, indicatrice d'Euler
  $a^{\varphi(n)} = 1 \mod n$ si a inversible modulo n.

Conclusion

- Rappels congruence : modulos à comprenadre et connaître ++
- Théorème de Sun-Zi (restes chinois)
- Éléments inversibles, groupe multiplicatif, indicatrice d'Euler
  $a^{\varphi(n)} = 1 \mod n$ si a inversible modulo n.
- RSA : e, N, d, p, q, $\varphi(N)$

Conclusion

- Rappels congruence : modulos à comprenadre et connaître ++
- Théorème de Sun-Zi (restes chinois)
- Éléments inversibles, groupe multiplicatif, indicatrice d'Euler $a^{\varphi(n)} = 1 \mod n$ si a inversible modulo n.
- RSA : e, N, d, p, q, $\varphi(N)$
- Malléable (pas IND-CPA)

CONCLUSION

- Rappels congruence : modulos à comprenadre et connaître ++
- Théorème de Sun-Zi (restes chinois)
- Éléments inversibles, groupe multiplicatif, indicatrice d'Euler
  $a^{\varphi(n)} = 1 \mod n$ si a inversible modulo n.
- RSA : e, N, d, p, q, $\varphi(N)$
- Malléable (pas IND-CPA)
- à randomiser

Conclusion

- Rappels congruence : modulos à comprenadre et connaître ++
- Théorème de Sun-Zi (restes chinois)
- Éléments inversibles, groupe multiplicatif, indicatrice d'Euler
  $a^{\varphi(n)} = 1 \mod n$ si a inversible modulo n.
- RSA : e, N, d, p, q, $\varphi(N)$
- Malléable (pas IND-CPA)
- à randomiser
- Et pas n'importe comment !

Conclusion

- Rappels congruence : modulos à comprenadre et connaître ++
- Théorème de Sun-Zi (restes chinois)
- Éléments inversibles, groupe multiplicatif, indicatrice d'Euler
  $a^{\varphi(n)} = 1 \mod n$ si a inversible modulo n.
- RSA : e, N, d, p, q, $\varphi(N)$
- Malléable (pas IND-CPA)
- à randomiser
- Et pas n'importe comment !

Problème
La factorisation est un problème « difficile ».

CONCLUSION

- Rappels congruence : modulos à comprenadre et connaître ++
- Théorème de Sun-Zi (restes chinois)
- Éléments inversibles, groupe multiplicatif, indicatrice d'Euler
  $a^{\varphi(n)} = 1 \mod n$ si a inversible modulo n.
- RSA : e, N, d, p, q, $\varphi(N)$
- Malléable (pas IND-CPA)
- à randomiser
- Et pas n'importe comment !

PROBLÈME

La factorisation est un problème « difficile ».

✍ Est-ce que RSA - OAEP est IND-CPA si H et G sont sécurisés sous la factorisation ?