INITIATION À LA RECHERCHE · L1 INFORMATIQUE

Le Cryptosystème RSA

Fondements Mathématiques et Analyse de Sécurité

Walaa Mansouri
Encadrante : Mireille Fouquet
Université Paris Cité · 2025–2026

Avec les remerciements à Jean-Yves Ducloux pour sa recommandation.

Plan de l'exposé

01 **Introduction à la cryptographie**

Chiffrements classiques · Diffie-Hellman

02 **Fondements mathématiques**

Arithmétique modulaire · Euler · Euclide étendu

03 **L'algorithme RSA**

Génération des clés · Chiffrement

04 **Analyse de sécurité & Attaques**

Factorisation · Module commun · Bleichenbacher

05 **Conclusion & Perspectives**

Évolution pratique de RSA · Abandon dans TLS 1.3 au profit d'ECDHE

01 Introduction à la cryptographie

La cryptographie transforme un message lisible (plaintext) en un message incompréhensible (ciphertext), accessible uniquement à un destinataire autorisé.

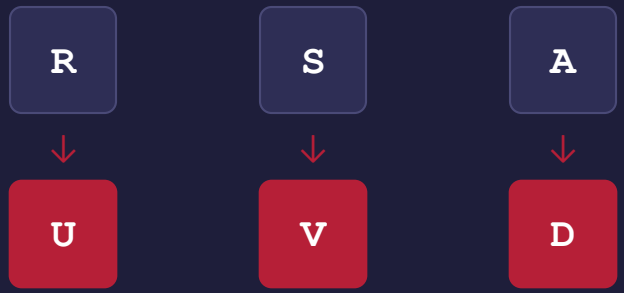
Objectifs fondamentaux

1. **Confidentialité**
   Seul le destinataire lit le message
2. **Intégrité**
   Le message n'a pas été modifié
3. **Authenticité**
   L'expéditeur est bien celui qu'il dit être
4. **Non-répudiation**
   Impossible de nier avoir signé

Exemple : le chiffrement de César

Le plus ancien chiffrement par substitution : chaque lettre est décalée de 3 positions dans l'alphabet.

$$y \equiv x + 3 \pmod{26}$$



RSA → UVD

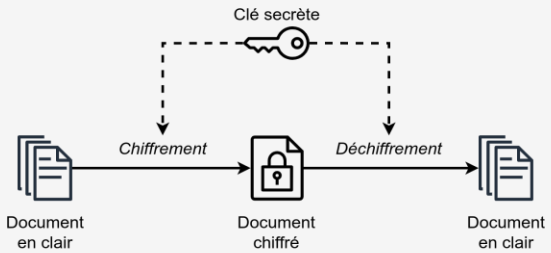
⚠ *Cassable par recherche exhaustive (26 clés)*

Symétrique vs Asymétrique

Chiffrement symétrique

- Même clé pour chiffrer et déchiffrer
- Exemples : AES (128/192/256 bits), DES (56 bits)
- Très rapide idéal pour grandes données
- Problème : comment partager la clé ?

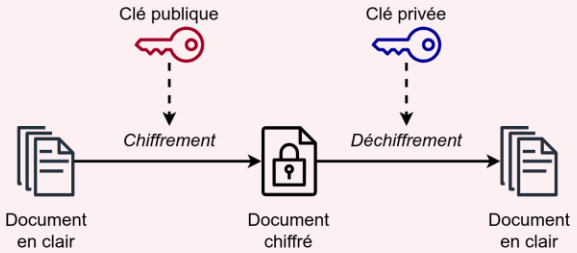
AES · DES



Chiffrement asymétrique

- Paire de clés : publique + privée
- Clé publique diffusée librement
- Seule la clé privée déchiffre
- Exemples : RSA, Diffie-Hellman
- **Résout le problème de distribution !**

RSA · Diffie-Hellman



02 Fondements mathématiques de RSA

1	**Arithmétique modulaire** `a ≡ b (mod n)  ↔  n | (a-b)`	→ *Base de tous les calculs RSA*
2	**Algorithme d'Euclide étendu** `Calcule pgcd(a,b) et les coefficients de Bézout`	→ *Calcul de l'inverse modulaire d*
3	**Indicatrice d'Euler ϕ(n)** `φ(pq) = (p-1)(q-1)`	→ *Définit l'espace des exposants*
4	**Théorème d'Euler** `a^φ(n) ≡ 1 (mod n)  si pgcd(a,n)=1`	→ *Garantit la correction de RSA*
5	**Théorème des restes chinois** `x≡a (mod p), x≡b (mod q) → solution unique mod pq`	→ *Preuve de correction*
6	**Exponentiation rapide** `a^e mod n en O(log e) multiplications`	→ *Rend RSA utilisable en pratique*

03 L'algorithme RSA

Génération des clés

1. Choisir deux grands premiers p et q
2. Calculer $N = pq$ (module RSA, public)
3. Calculer $\phi(N) = (p-1)(q-1)$ (secret)
4. Choisir e tel que $\text{pgcd}(e, \phi(N)) = 1$ → clé publique (N, e)
5. Calculer $d = e^{-1} \bmod \phi(N)$ → clé privée (N, d)

Clé publique (N,e) = (143, 7)
Clé privée (N,d) = (143, 103)

Exemple numérique

$p = 11, \quad q = 13$

$N = 11 \times 13 = 143$

$\varphi(N) = 10 \times 12 = 120$

$e = 7 \quad (\text{pgcd}(7,120)=1)$

Inverse de 7 mod 120 :

$7 \times 103 = 721$

$= 6 \times 120 + 1$

→ **d = 103**

03 Chiffrement & Déchiffrement

Chiffrement

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

Avec la clé publique (N, e). Tout le monde peut chiffrer un message pour le destinataire.

$M = 9, \quad e = 7, \quad N = 143$

$$C = 9^7 \bmod 143 = 48$$

Message chiffré transmis : C = 48

Déchiffrement

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

Avec la clé privée (N, d). Seul le détenteur de d peut retrouver le message original.

$C = 48, \quad d = 103, \quad N = 143$

$$M = 48^{103} \bmod 143 = 9$$

Message original retrouvé : M = 9 ✓

Preuve de correction (théorème d'Euler)

$$ed = 1 + k \cdot \varphi(N) \implies C^d = M^{(ed)} = M \cdot M^{(\varphi(N))k} \equiv M \cdot 1^k \equiv M \pmod N$$

04 Analyse de sécurité & Attaques

Factorisation du module N

Méthode : ρ Pollard

Si N = pq est factorisé → ϕ(N) → d. Protection : N ≥ 2048 bits.

Module commun

Méthode : Identité de Bézout

Si deux utilisateurs partagent N avec pgcd(eB,eC)=1 → M retrouvé directement.

Attaque par masquage (Blinding)

Méthode : Homomorphisme multiplicatif

C' = C·r^e soumis au serveur, résultat divisé par r → M retrouvé.

Attaque de Bleichenbacher

Méthode : serveur PKCS#1 · ~10^6 requêtes

Une réponse binaire valide/invalide suffit à retrouver M. A affecté TLS.

05 Conclusion & Perspectives

- RSA repose sur la difficulté de factoriser N = pq
- Correct grâce au théorème d'Euler : $M^{(ed)} \equiv M \pmod{N}$
- Sûr si N ≥ 2048 bits et bien implémenté
- L'attaque de Bleichenbacher prouve : les maths ne suffisent pas
- TLS 1.3 (2018) abandonne RSA pour l'échange de clé au profit d'ECDHE, suite aux attaques Bleichenbacher
- RSA reste utilisé pour signer les certificats, mais plus pour échanger les clés depuis TLS 1.3.

Merci de votre attention

Remerciements

MF

Mireille Fouquet

Encadrante

Pour son accompagnement et ses conseils tout au long de ce projet d'initiation à la recherche.

JD

Jean-Yves Ducloux

Recommandation

Pour avoir recommandé ce sujet passionnant et orienté mes premiers pas en cryptographie.