Chapitre 4

Cryptographie asymétrique: l'algorithme RSA

Dr.Wafa Berrayana | AU: 2025-2026

2025

Introduction

- RSA est un algorithme de cryptographie asymétrique inventé en 1977 par Ronald Rivest, Adi Shamir et Leonard Adleman
- Il repose sur une paire de clés
  - une clé publique utilisée pour chiffrer les données
  - une clé privée disponible uniquement pour le destinataire, qui permet de déchiffrer ces données
  - Les clés publique et privée sont mathématiquement liées

- Le fonctionnement de RSA s'appuie sur des propriétés mathématiques des grands nombres premiers
- La sécurité de RSA dépend de la difficulté à factoriser ce grand produit ***n*** ce qui est actuellement très difficile pour des clés suffisamment longues (2048 bits ou plus).

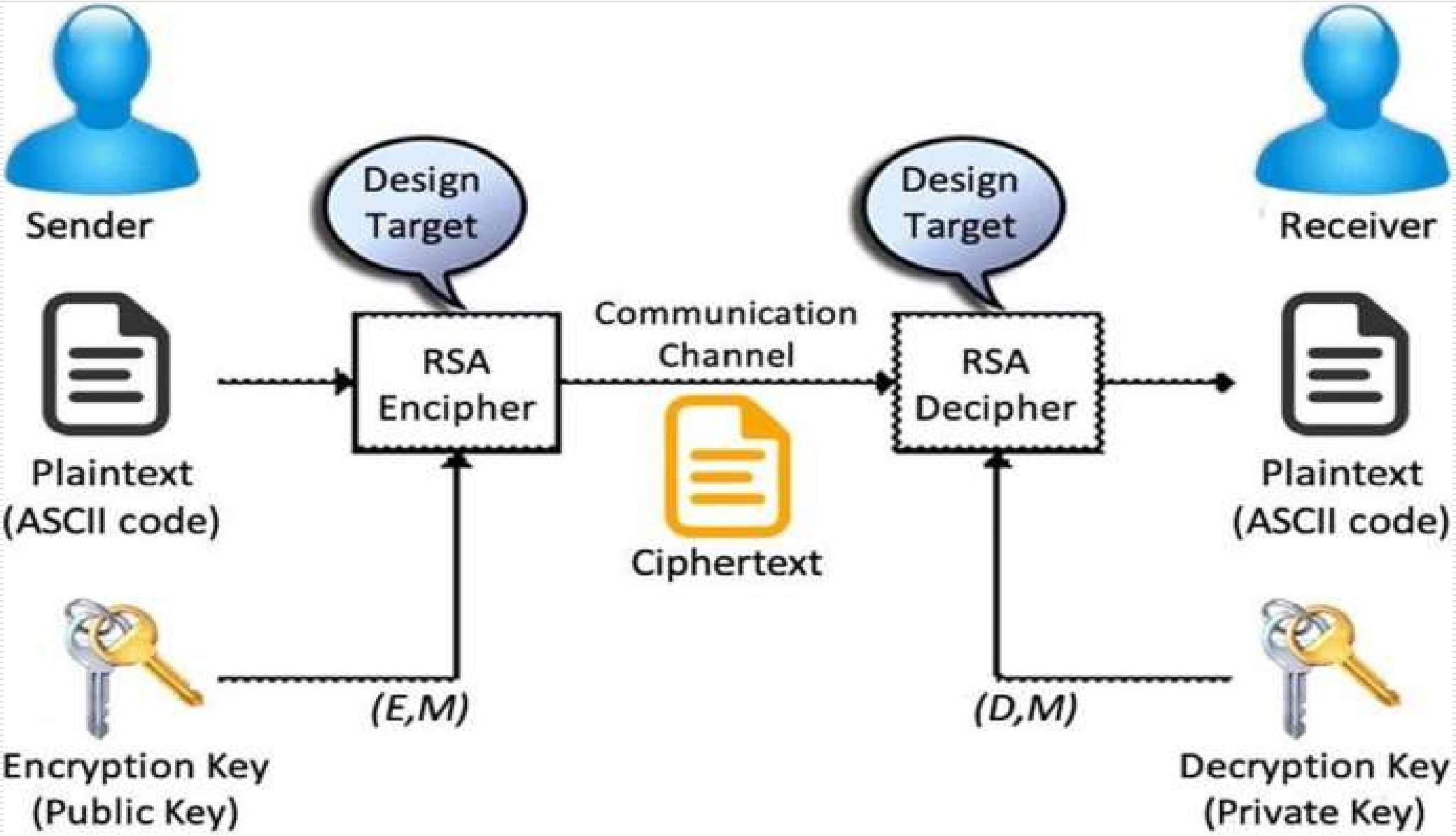
Domaines d’utilisation de RSA

- **Sécurisation des communications Internet :** RSA est largement utilisé dans les protocoles HTTPS/TLS pour établir des connexions sécurisées entre navigateurs web et serveurs, garantissant la confidentialité des échanges.
- **Signature numérique :** RSA permet de générer des signatures numériques qui attestent l'authenticité, l'intégrité et la non-répudiation d'un document ou message.
- **Chiffrement des emails et messagerie**
- **VPN (Réseaux privés virtuels)** : RSA assure l'authentification et la confidentialité dans de nombreux VPN.

Domaines d’utilisation de RSA

- **Transactions financières et commerce électronique :** RSA protège les données sensibles des cartes de crédit et les transactions sur les plateformes de paiement en ligne.
- **Gestion d'identité et authentification :** RSA est utilisé dans les systèmes d'authentification multifactorielle et la gestion des accès en entreprise
- **Protection des données dans le Cloud :** RSA chiffre les données stockées dans des environnements cloud, assurant la sécurité des informations stratégiques

Fonctionnement de l'algorithme RSA



Fonctionnement de l'algorithme RSA

Algorithme de chiffrement RSA

- **Génération des clés publique et privée**
- **Chiffrement**
- **Déchiffrement**

Génération des clés publique et privée

- Le fonctionnement de RSA s'appuie sur des propriétés mathématiques des grands nombres premiers.

p, *q* : deux grands nombres premiers

d est calculé avec l'algorithme euclidien étendu

Key Generation

Select p, q	p and q both prime, $p \neq q$
Calculate $n = p \times q$	
Calcuate $\phi(n) = (p-1)(q-1)$	
Select integer e	$\gcd(\phi(n), e) = 1; 1 < e < \phi(n)$
Calculate d	$d \equiv e^{-1} \pmod{\phi(n)}$
Public key	$PU = \{e, n\}$
Private key	$PR = \{d, n\}$

d est l'inverse modulaire de e modulo $\varphi(n)$,c'est-à-dire d tel que $d \times e \equiv 1 \mod \varphi(n)$, souvent calculé avec l'algorithme d'Euclide étendu.

Chiffrement et déchiffrement

Encryption

Plaintext:	$M < n$
Ciphertext:	$C = M^e \bmod n$

Decryption

Ciphertext:	C
Plaintext:	$M = C^d \bmod n$

Astuce pour calculer d

- **Find a value for d such that**

$$d = \frac{1 + k\,\varphi(n)}{e}$$

- **Find the least value of 'k' which gives the integer value of 'd'**

substituting k=1, d = (1+160)/13

= 12.38 ×

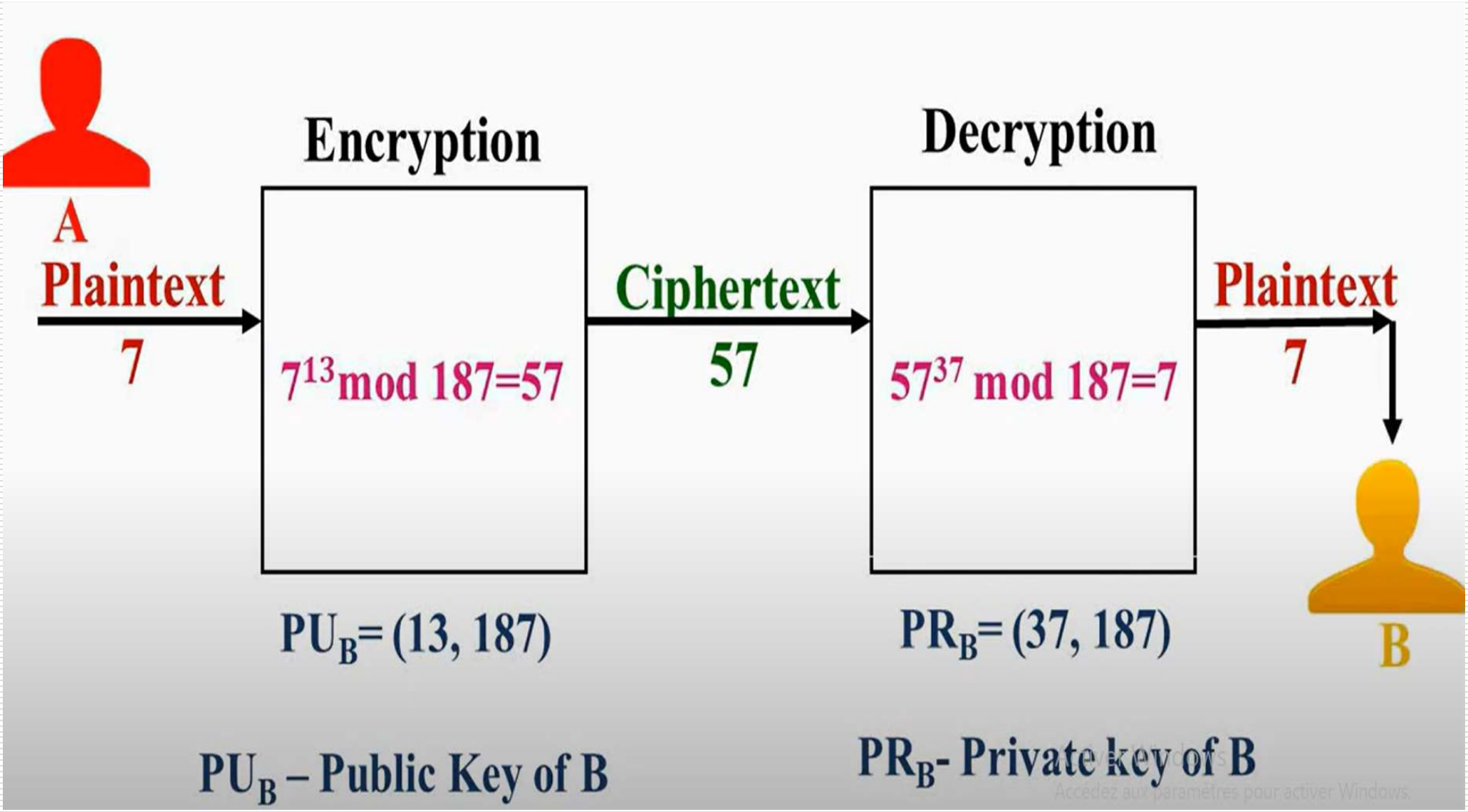
k=2, d = (1+320)/13

= 24.6 ×

k=3, d = (1+480)/13

= 37 √

Exemple


A
Plaintext
7
Encryption
$7^{13} \bmod 187 = 57$
Ciphertext
57
Decryption
$57^{37} \bmod 187 = 7$
Plaintext
7
B
$PU_B = (13, 187)$
$PR_B = (37, 187)$
PU_B – Public Key of B
PR_B- Private key of B

Exemple

- Encrypt the sentence “I love you” don’t consider upper/lower cases. Use RSA with public key (7, 33)
- **Solution:**
  - I love you has the following position sequence (09 12 15 22 05 25 15 21).
  - $09^7 \bmod 33 = 15$ | $12^7 \bmod 33 = 12$ | $15^7 \bmod 33 = 27$
  - $22^7 \bmod 33 = 22$ | $05^7 \bmod 33 = 14$ | $25^7 \bmod 33 = 31$
  - $15^7 \bmod 33 = 27$ | $21^7 \bmod 33 = 21$

- The resulting sequence is (15 12 27 22 14 31 27 21) which corresponds to **o l!vn %!u**

a b c d e f g h I j k l m n o p q r s t u v w x y z ! @ # $ % & *

Question: P and Q are two prime numbers. P=7, and Q=17. Take public key E=5. If plain text value is 6, then what will be cipher text value according to RSA algorithm? Again calculate plain text value from cipher text.

Solution:

1. Two prime numbers P=7, Q=17
2. $n = P * Q = 17 * 7 = 119$ **n = 119**
3. $\Phi(n) = (P-1) * (Q-1) = (17-1) * (7-1) = 16 * 6 = 96$ **Φ(n) = 96**
4. Public key E = 5. **E= 5**
5. Calculate d = 77. $d = ((\Phi(n) * i) + 1) / e$ **d= 77**

   $d = ((96*1)+1) / 5 = 19.4$

   $d = ((96*2)+1) / 5 = 38.6$

   $d = ((96*3)+1) / 5 = 57.8$

   $d = ((96*4)+1) / 5 = 77$ (Stop finding d because getting integer value)
6. Public key = {e, n} = {5, 119}, private key = {d, n} = {77, 119}.
7. Plain text PT = 6, $CT = PT^E \bmod n = 6^5 \bmod 119 = 41$. **Cipher Text = 41**
8. Cipher text CT = 41, $PT = CT^d \bmod n = 41^{77} \bmod 119 = 6$. **Plain Text = 6**

Question: In a public key cryptosystem using RSA algorithm, user uses two prime numbers 5 and 7. He chooses 11 as Encryption key, find out decryption key. What will be the cipher text, if the plaintext is 2? Decrypt the cipher text, what will be the value of plain text?

Solution:

1. Two prime numbers $p = 5$, $q = 7$
2. $n = p * q = 5 * 7 = 35$ **n = 35**
3. $\Phi(n) = (p-1) * (q-1) = (5-1) * (7-1) = 4 * 6 = 24$ **Φ(n) = 24**
4. Public key $e = 11$. **e= 11**
5. Calculate $d = 11$. $d = ((\Phi(n) * i) + 1) / e$ **d= 11**
6. Public key = {e, n} = {11, 35}, private key = {d, n} = {11, 35}.
7. Plain text $P = 2$, $C = P^e \bmod n = 2^{11} \bmod 35 = 18$. **Cipher Text = 18**
8. Cipher text $C = 18$, $P = C^d \bmod n = 18^{11} \bmod 35 = 2$. **Plain Text = 2**

Attaques de RSA

- Les attaques contre RSA sont diverses, voici les plus importantes :
  - **Attaque de factorisation :** L'attaque la plus directe consiste à factoriser le module $n = p \times q$. Si un adversaire réussit à retrouver p et q, il peut calculer la clé privée d et déchiffrer tous les messages. La sécurité repose donc sur la difficulté de cette factorisation pour de grands nombres.
  - **Attaque de Wiener :** Exploite des petites valeurs du dé d (clé privée) pour retrouver la clé via des développements en fractions continues, si d est trop petit par rapport à n
  - **Attaques par canaux auxiliaires (side-channel attacks) :** Exploitent des informations physiques comme le temps de calcul, la consommation électrique ou les émissions électromagnétiques pendant le chiffrement/déchiffrement pour déduire la clé privée.

Attaques de RSA

- **Attaques de chronométrage (timing attacks) :** Basées sur la mesure du temps que prend une opération cryptographique pour extraire des informations secrètes

- **Attaques au choix du texte clair (chosen-plaintext attacks)** : L'attaquant soumet des textes choisis et observe les sorties pour en déduire la clé.

- Attaques quantiques : Avec l'ordinateur quantique et notamment l'algorithme de Shor, RSA serait vulnérable car la factorisation des grands entiers deviendrait rapide.