The RSA algorithm:

The RSA (The Rivest-Shamir-Adleman) scheme is a block cipher in which the plaintext and ciphertext are integers between 0 and n - 1 for some n. A typical size for n is 1024 bits, or 309 decimal digits. That is, n is less than 2^{1024}.

Description of the Algorithm

The scheme developed by Rivest, Shamir, and Adleman makes use of an expression with exponentials.

Plaintext is encrypted in blocks, with each block having a binary value less than some number n. That is, the block size must be less than or equal to $\log_2(n)$; in practice, the block size is i bits, where $2^i < n \leq 2^i+1$. Encryption and decryption are of the following form, for some plaintext block M and ciphertext block C:

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

$$M = C^d \bmod n = (M^e)^d \bmod n = M^{ed} \bmod n$$

Both sender and receiver must know the value of n. The sender knows the value of e, and only the receiver knows the value of d. Thus, this is a public-key encryption algorithm with a public key of ***PU* = {*e, n*}** and a private key of ***PU* = {*d, n*}.** For this algorithm to be satisfactory for public-key encryption, the following requirements must be met:

1- It is possible to find values of e, d, n such that $M^{ed} \bmod n = M$ for all $M < n$.

2- It is relatively easy to calculate mod M^e mod n and Cd for all values of $M < n$.

3- It is infeasible to determine d given e and n.

We are now ready to state the RSA scheme. The ingredients are the following:

p,q, two prime numbers	(private, chosen)
$n = pq$	(public, calculated)
e, with gcd(f(n),e) = 1;1 < e < f(n)	(public, chosen)
$d \equiv e^{1}$ (mod f(n))	(private, calculated)

Figure 11.1 illustrates The RSA Algorithm.

Key Generation

Select p, q	p and q both prime, $p \neq q$
Calculate $n = p \times q$	
Calculate $\phi(n) = (p-1)(q-1)$	
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	$PR = \{d, n\}$

Encryption

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

Decryption

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

Figure 11.1. The RSA Algorithm

Ex:

- Choose **p = 3** and **q = 11**
- Compute **n = p * q = 3 * 11 = 33**
- Compute **φ(n) = (p - 1) * (q - 1) = 2 * 10 = 20**
- Choose **e** such that **1 < e < φ(n)** and e and n are prime.

  Let **e = 7**
- Compute a value for **d** such that **(d * e) mod φ(n) = 1**. One solution is

  d = 3 because [(3 * 7) mod20 = 1]
- Public key is **{e, n} = {7, 33}**
- Private key is **{d, n)}= {3, 33}**

For encryption :

The plain text(Message) =2

The cipher text $= 2^7 \ mod\ 33$

C $= 29$

For decryption :

C=29

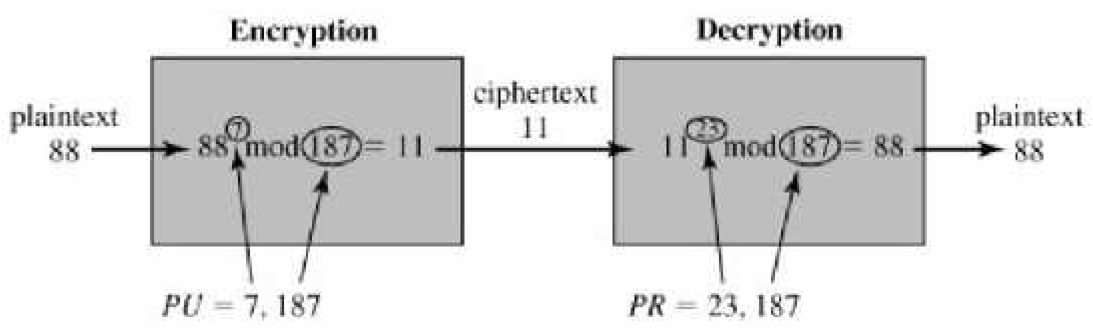
The plain text$=29^3 \ mod\ 33$

$P = 2$

Ex:

- Select two prime numbers, $p = 17$ and $q = 11$.
- Calculate $n = pq = 17 \times 11 = 187$.
- Calculate $\varphi(n) = (p-1)(q-1) = 16 \times 10 = 160$.
- Select e such that e is relatively prime to $\varphi(n) = 160$ and less than $\varphi(n)$ we choose $e = 7$.
- Determine d such that $de \equiv 1 \pmod{160}$ and $d < 160$. The correct value is $d = 23$, because $23 \times 7 = 161 = 10 \times 160 + 1$.

The resulting keys are public key $PU = \{7,187\}$ and private key $PR = \{23,187\}$.



The example shows the use of these keys for a plaintext input of $M = 88$.
For encryption, we need to calculate $C = 88^7 \bmod 187$.
Exploiting the properties of modular arithmetic, we can do this as follows:

$$88^7 \bmod 187 = [(88^4 \bmod 187) \times (88^2 \bmod 187) \times (88^1 \bmod 187)] \bmod 187$$

$$88^1 \bmod 187 = 88$$

$$88^2 \bmod 187 = 7744 \bmod 187 = 77$$

$$88^4 \bmod 187 = 59{,}969{,}536 \bmod 187 = 132$$

$$88^7 \bmod 187 = (88 \times 77 \times 132) \bmod 187 = 894{,}432 \bmod 187 = 11$$

For decryption, we calculate $M = 11^{23} \bmod 187$:

$11^{23} \bmod 187 = [(11^1 \bmod 187) \times (11^2 \bmod 187) \times (11^4 \bmod 187) \times (11^8 \bmod 187) \times (11^8 \bmod 187)] \bmod 187$

$11^1 \bmod 187 = 11$

$11^2 \bmod 187 = 121$

$11^4 \bmod 187 = 14{,}641 \bmod 187 = 55$

$11^8 \bmod 187 = 214{,}358{,}881 \bmod 187 = 33$

$11^{23} \bmod 187 = (11 \times 121 \times 55 \times 33 \times 33) \bmod 187 = 79{,}720{,}245 \bmod 187 = 88$