Mustansiriyah University	Public-Key Cryptography	Class: Third Year
Engineering College	Asymmetric Cipher	Course name: Data Encryption
Computer Engineering Dep.	RSA Algorithm	Lecturer: Fatimah Al-Ubaidy

RSA Public-Key Cryptography

The RSA Algorithm: It is a public key cryptography algorithm, which was proposed by Diffie and Hellman. RSA can be used for key exchange, digital signatures and the encryption of small blocks of data.

- RSA is primarily used to encrypt the session key used for secret key encryption or the message's hash value (digital signature).
- RSA's mathematical hardness comes from the ease in calculating large numbers and the difficulty in finding the prime factors of those large numbers.
- To create an RSA public/private key pair, here are the basic steps:

1- Choose two prime numbers, p and q such that $p \neq q$.

2- Calculate the modulus, $n = p \times q$.

3- Calcuate $\phi(n) = (p - 1) \times (q - 1)$.

4- Select integer e such that gcd $(\phi(n), e) = 1$ and $1 < e < \phi(n)$. (* gcd is greater common divisor)

5- Calculate an integer d from the quotient $de \equiv 1 \pmod{\phi(n)} \Rightarrow de = 1 + k\,\phi(n) \Rightarrow$

$d = (1 + k\,\phi(n)) / e$

- To encrypt a message, M, with the public key (e, n), create the ciphertext, C, using the equation:

$C = M^e \bmod n$

- The receiver then decrypts the ciphertext with the private key (d, n) using the equation:

$M = C^d \bmod n$

RSA Public-Key Cryptography

The RSA Example

1. Select two prime numbers, p = 17 and q = 11.
2. Calculate n = p× q = 17 × 11 = 187.
3. Calculate $\phi(n) = (p - 1)(q - 1) = 16 \times 10 = 160$.
4. Select e such that e is relatively prime to $\phi(n) = 160$ and less than $\phi(n)$; we choose e = 7.
5. Determine d such that $de \equiv 1 \pmod{160}$ and $d < 160$. $de = 1 + k\,\phi(n)$

The correct value is d = 23, because 23 × 7 = 161 = 1 + (1 × 160).
The resulting keys are public key PU = {7, 187} and private key PR = {23, 187}.

Given a plaintext input of M = 88. For encryption, we need to calculate $C = 88^7 \bmod 187$.
we can do this as follows.

$88^7 \bmod 187 = [(88^4 \bmod 187) * (88^2 \bmod 187) * (88^1 \bmod 187)] \bmod 187$
$88^1 \bmod 187 = 88$
$88^2 \bmod 187 = 7744 \bmod 187 = 77$
$88^4 \bmod 187 = 59{,}969{,}536 \bmod 187 = 132$
$88^7 \bmod 187 = (88 * 77 * 132) \bmod 187 = 894{,}432 \bmod 187 = 11$

RSA Public-Key Cryptography

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

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

$11^1 \bmod 187 = 11$

$11^2 \bmod 187 = 121$

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

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

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

In the preceding example shows, we can make use of a property of modular arithmetic:

$[(a \bmod n) * (b \bmod n)] \bmod n = (a * b) \bmod n$

As another example, suppose we wish to calculate $x^{11} \bmod n$ for some integers x and n. Observe that $x^{11} = x^{1+2+8} = (x)(x^2)(x^8)$.

Public-Key Cryptography

Applications for Public-Key Cryptosystems:

■ **Encryption/decryption:** The sender encrypts a message with the recipient's public key, and the recipient decrypts the message with the recipient's private key.

■ **Digital signature:** The sender "signs" a message with its private key.

■ **Key exchange:** Two sides cooperate to exchange a session key.

The security of RSA:

Five possible approaches to attacking the RSA algorithm are

■ **Brute force:** This involves trying all possible private keys.

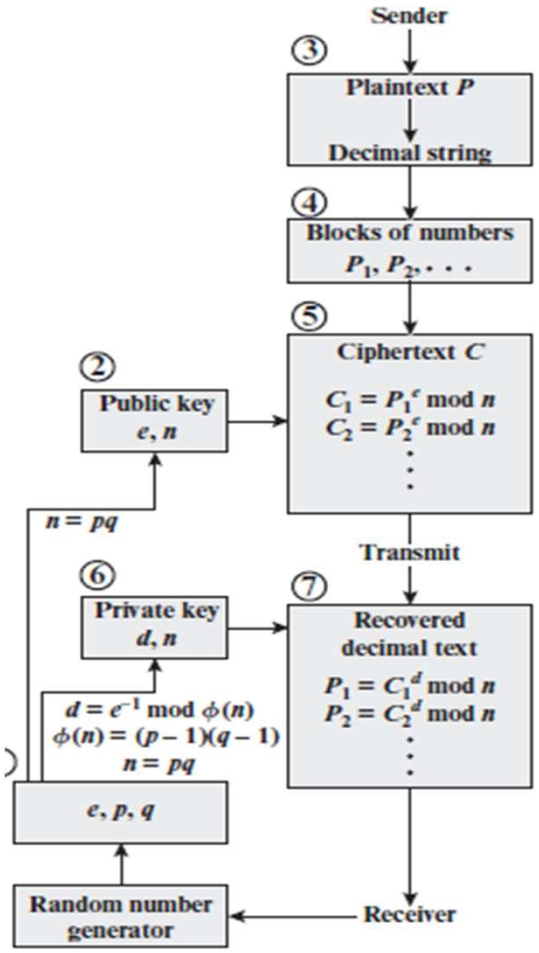
■ **Mathematical attacks:** There are several approaches, all equivalent in effort to factoring the product of two primes.

■ **Timing attacks:** These depend on the running time of the decryption algorithm.

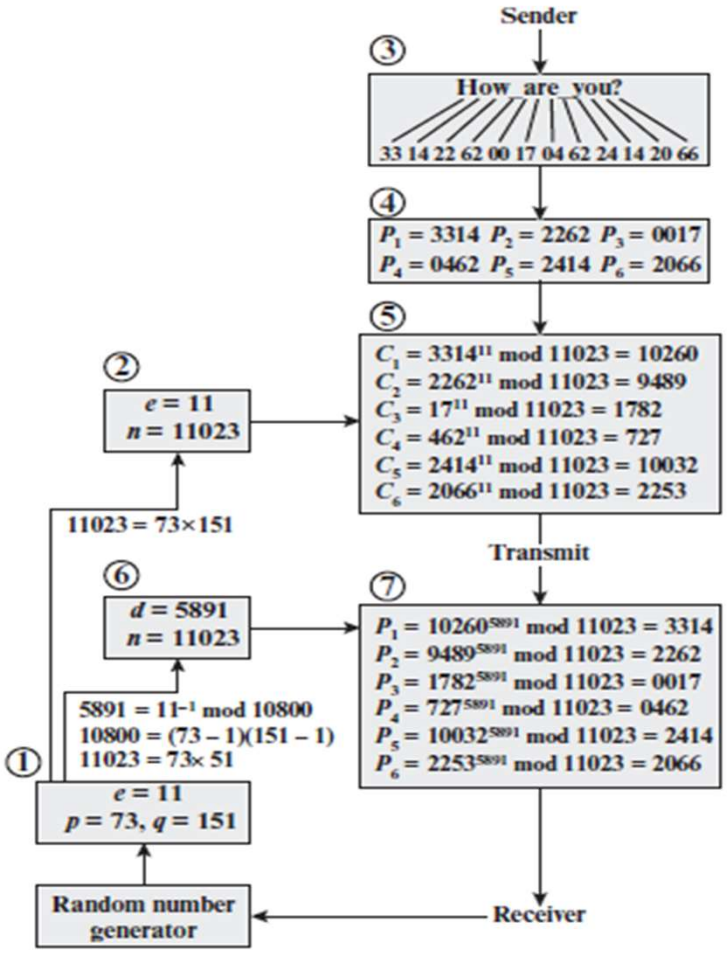
■ **Hardware fault-based attack:** This involves inducing hardware faults in the processor that is generating digital signatures.

■ **Chosen ciphertext attacks:** This type of attack exploits properties of the RSA algorithm.

RSA processing of multiple blocks



(a) General approach



(b) Example