Al-Mustaqbal University
College of Sciences
Intelligent Medical System Department

جامعة المستقبل
AL MUSTAQBAL UNIVERSITY

كلية العلوم

قسم الانظمة الطبية الذكية

Lecture: (7)

Information Security in Healthcare

Subject: Diffie Hellman and RSA

Level: Fourth

Lecturer: Prof. Dr. Mehdi Ebady Manaa

Study Year: 2025-2026

Public Key Cryptography

1. Diffie–Hellman

Diffie–Hellman is a cryptographic method that lets two parties securely agree on a shared secret over an insecure channel (like the internet), without ever sending the secret itself.

Two people can create the same secret number **independently**, even if an eavesdropper sees everything they exchange.

Diffie–Hellman is a method that allows **two parties** (Alice and Bob) to create the **same shared secret key** over a public channel, **without sending the secret key directly**.

What it's used for

- HTTPS (TLS)
- VPNs
- Secure messaging (e.g., Signal, WhatsApp)
- SSH

How it works (simplified)

1. **Public agreement**
   Both parties agree on two public numbers:
   - A large prime number **p**
   - A base **g**

   These are not secret.

2. **Private choices**
   - **Alice** picks a secret number **a**
   - **Bob** picks a secret number **b**
3. **Exchange values**
   - Alice sends: **$A = g^a \bmod p$**
   - Bob sends: **$B = g^b \bmod p$**
4. **Compute shared secret**
   - Alice computes: $S = B^a \bmod p$
   - Bob computes: $S = A^b \bmod p$

Both end up with the same secret**:**

$$S = g^{ab} \bmod p$$

1) Public parameters (known to everyone)

Both Alice and Bob agree on:

- $p = 23$ (a prime number)
- $g = 5$ (a generator)

These values are **public**.

2) Private keys (kept secret)

- Alice chooses a private key: $a = 6$
- Bob chooses a private key: $b = 15$

These values are **secret** and are never shared.

3) Compute public keys

Alice computes her public key

$$A = g^a \bmod p = 5^6 \bmod 23$$

Calculation:

- $5^2 = 25 \equiv 2 \pmod{23}$
- $5^4 \equiv 2^2 = 4 \pmod{23}$
- $5^6 = 5^4 \cdot 5^2 \equiv 4 \cdot 2 = 8 \pmod{23}$

So Alice sends:

$$A = 8$$

Bob computes his public key

$$B = g^b \bmod p = 5^{15} \bmod 23$$

So Bob sends:

$$B = 19$$

4) Exchange public keys

- Alice sends $A = 8$ to Bob
- Bob sends $B = 19$ to Alice

An attacker can see:

- $p = 23$
- $g = 5$
- $A = 8$
- $B = 19$

But the attacker does **not** know:

- $a = 6$
- $b = 15$

5) Compute the shared secret

Alice computes

$$K = B^a \bmod p = 19^6 \bmod 23$$

$$K = 2$$

Bob computes

$$K = A^b \bmod p = 8^{15} \bmod 23$$

$$K = 2$$

Because:

$$B^a \bmod p = (g^b)^a \bmod p = g^{ab} \bmod p$$

and

$$A^b \bmod p = (g^a)^b \bmod p = g^{ab} \bmod p$$

So both sides compute the same value.

السؤال : كيف نحسب ال g المولد ؟؟؟

2. The RSA Algorithm:

It is a public key cryptography algorithm, which was proposed by Created by Ron Rivest, Adi Shamir and Len Adleman in 1978. 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 (message integrity) 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 $d\,e \equiv 1 \pmod{\phi(n)}$.

- 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 $n = p \times q = 17 \times 11 = 187$.
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 $e = 7$. from GCD ($\phi(n)$, e)=1
5. **Determine** d such that $de \equiv 1 \pmod{160}$ and $d < 160$.The correct value is $d = 23$, **because** $23 \times 7 = 161 = (1 \times 160) + 1$.

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.

$88^7 \bmod 187 = [(88^4 \bmod 187) * (88^2 \bmod 187) * (88^1 \bmod 187)] \bmod 187$
$= 894{,}432 \bmod 187 = 11$

RSA Public-Key Cryptography

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

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

$79{,}720{,}245 \bmod 187 = 88$

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.

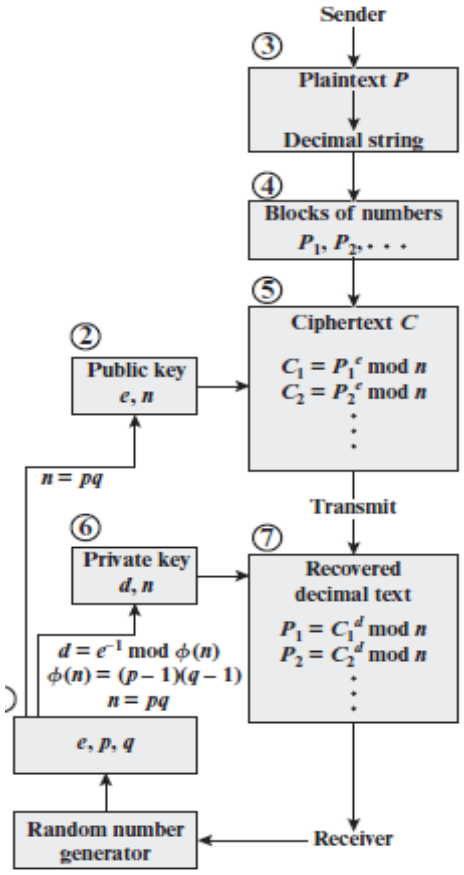
■ Mathematical attacks: There are several approaches, all equivalent in effort to factoring the product of two primes.

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

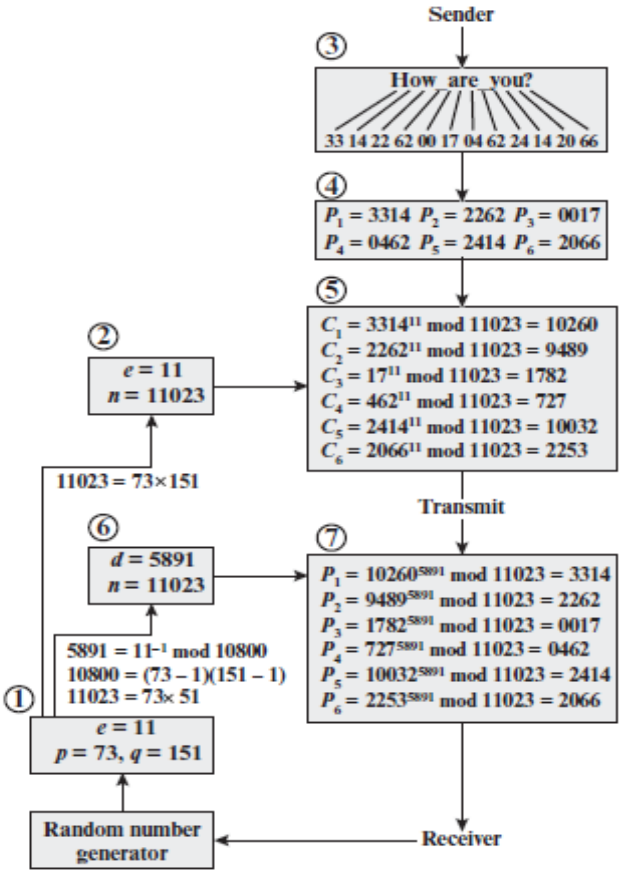
■ Hardware fault-based attack: This involves inducing hardware faults in the processor that is generating digital signatures.

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

RSA processing of multiple blocks



(a) General approach



(b) Example