02 – BASIC SECURITY MECHANICS AND MECHANISMS

WIRELESS LAN SECURITY

Integrity Mechanisms

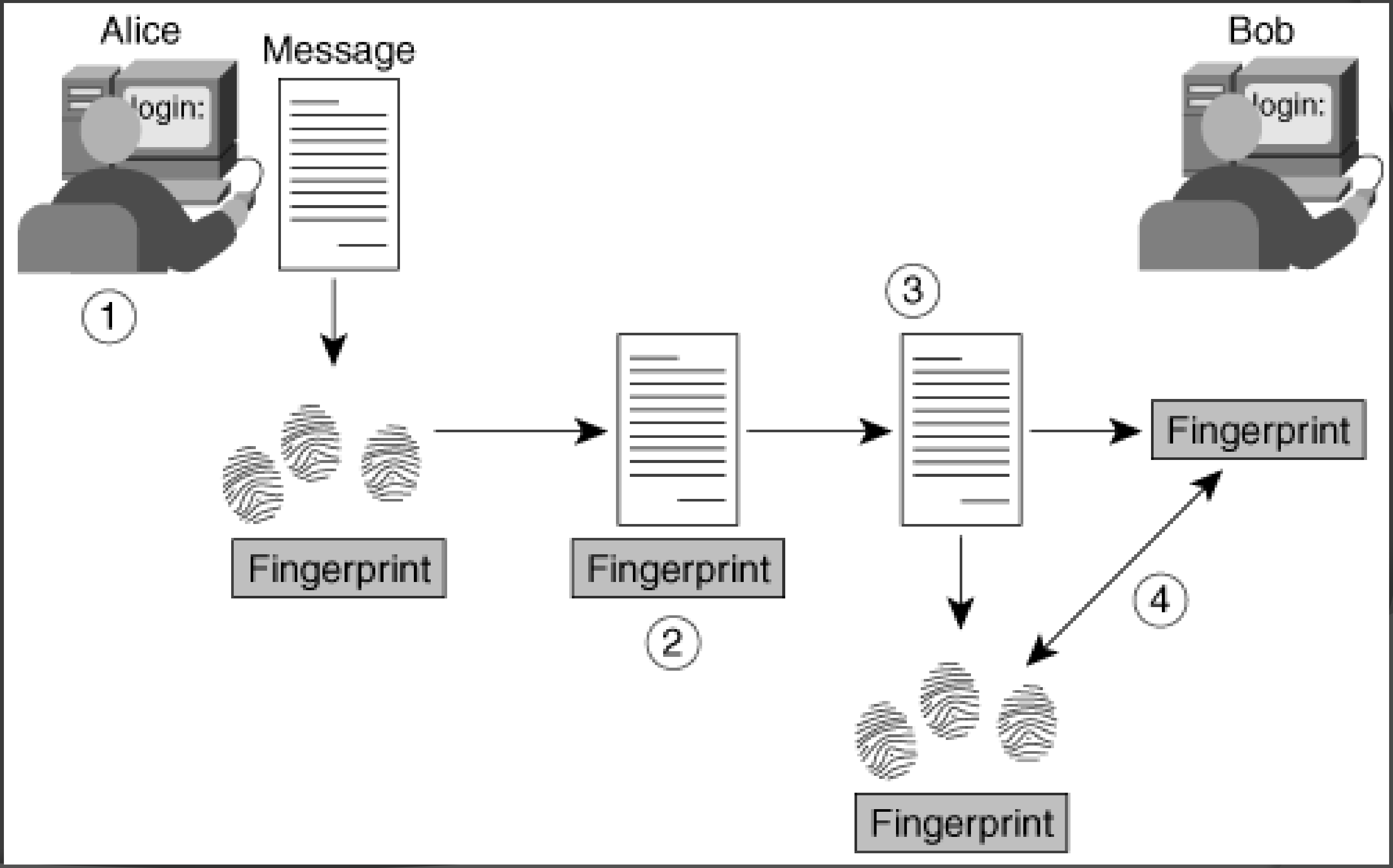
- Integrity mechanisms are aimed at detecting any changes to a set of bytes.
- Achieved by using hash functions and digital signatures.
- Digital signatures use the hash function mechanism and encrypt the resultant hash.

Hash Functions

- A hash function takes an input message of arbitrary length and outputs fixed-length code - the hash, or the message digest.

- A hash function must exhibit the following properties:
  - consistent
  - random
  - unique
  - one way

Using a One-Way Hash Function for Data Integrity



Man-in-the-Middle (MitM) attacks

- An MitM attack refers to an entity listening to a believed-to-be-secure communication and impersonating either the sender or receiver.

- This entity intercepts the message from the sender, adds its own content, and finally substitutes the correct hash for the altered message.

- The receiver verifies the hash and comes to the conclusion that the altered message was sent by the sender. This deception works because the hash itself is not protected.

Common hash functions

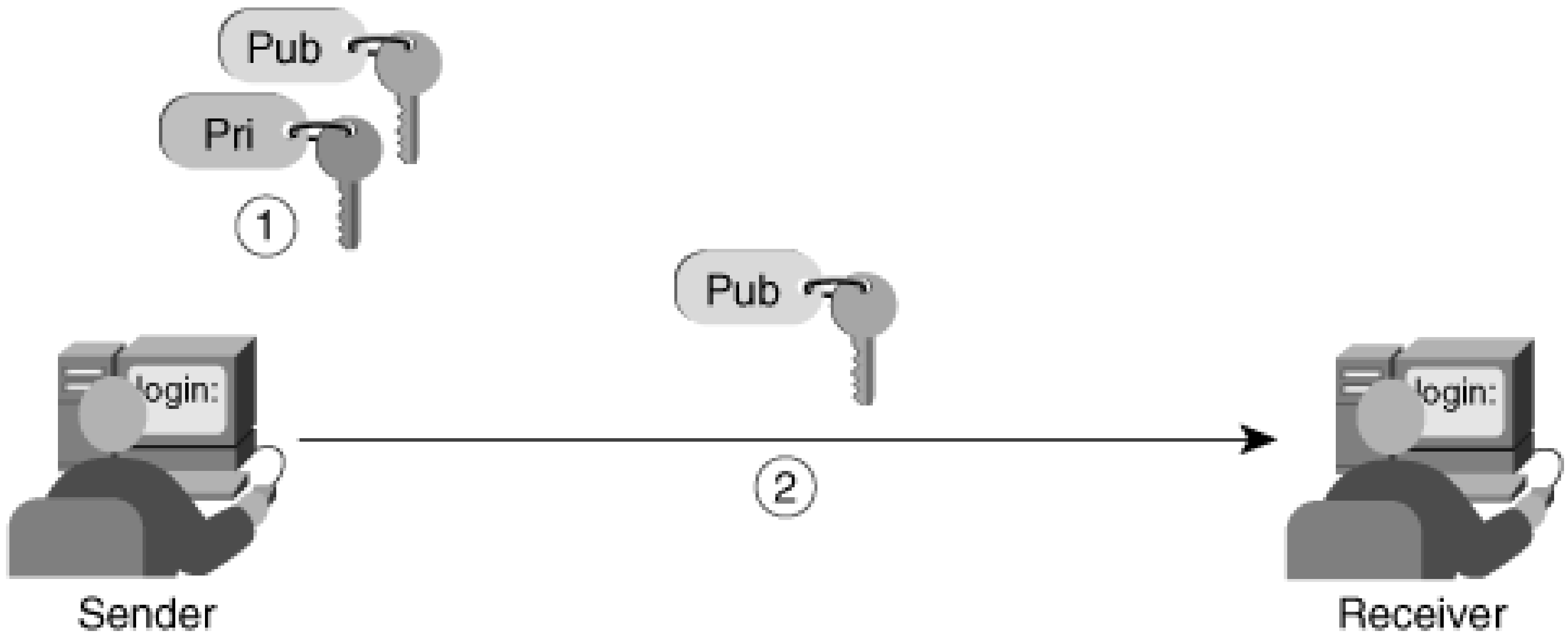
- Message Digest 4 (MD4) algorithm
- Message Digest 5 (MD5) algorithm
- Secure Hash Algorithm (SHA)

- MD5 and SHA are used most often in current security product implementations; both are based on MD4.
- MD5 processes its input in 512-bit blocks and produces a 128-bit message digest.
- SHA also processes its input in 512-bit blocks but produces a 160-bit message digest

Digital Signatures

- an encrypted message digest appended to a document.
- can be used to confirm the identity of the sender and the integrity of the document.
- based on a combination of public key encryption and one-way secure hash function algorithms.

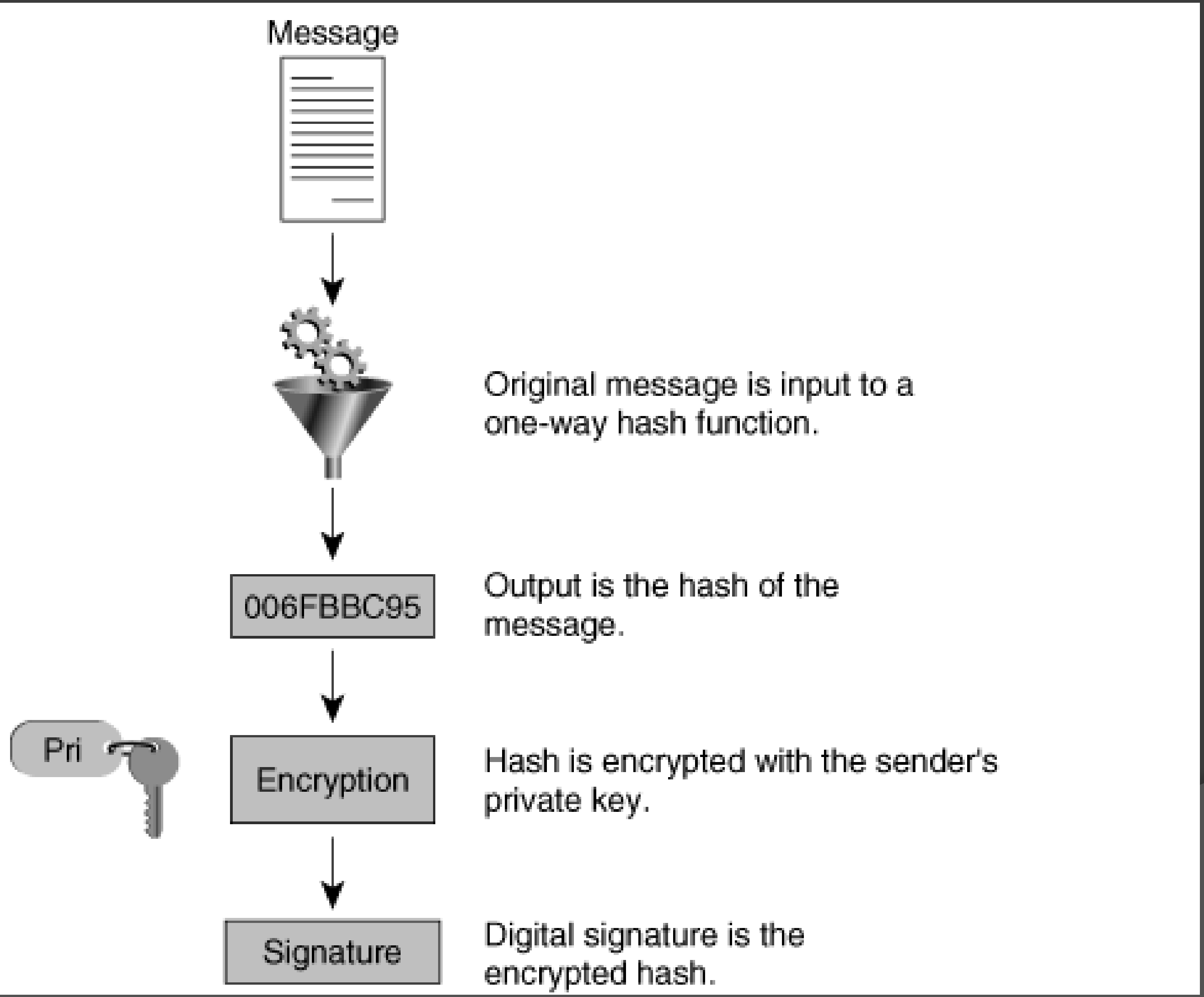
Creating a Digital Signature



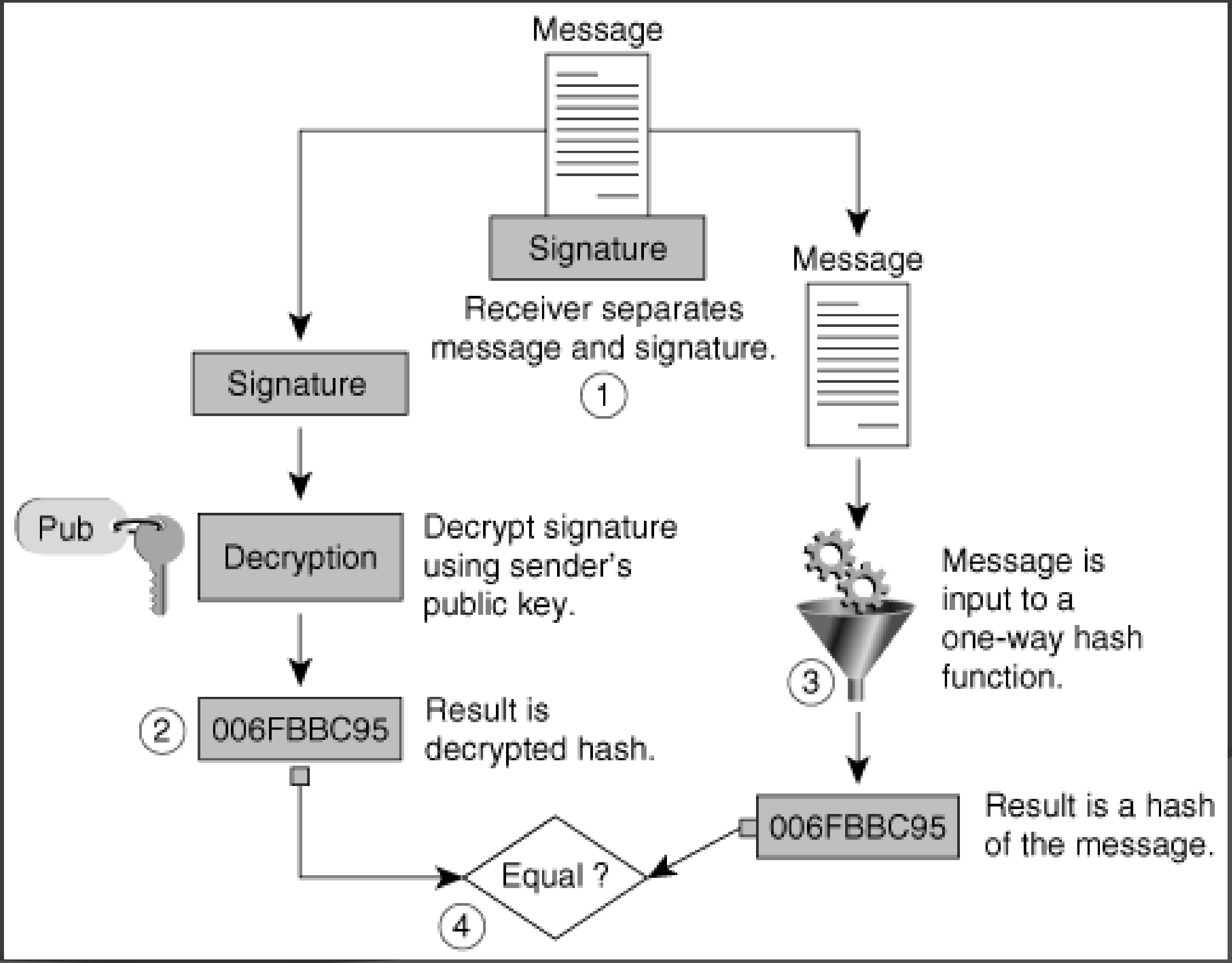
1 Sender creates a public/private key pair.

2 Sender sends his public key to the receiver.

Creating a Digital Signature



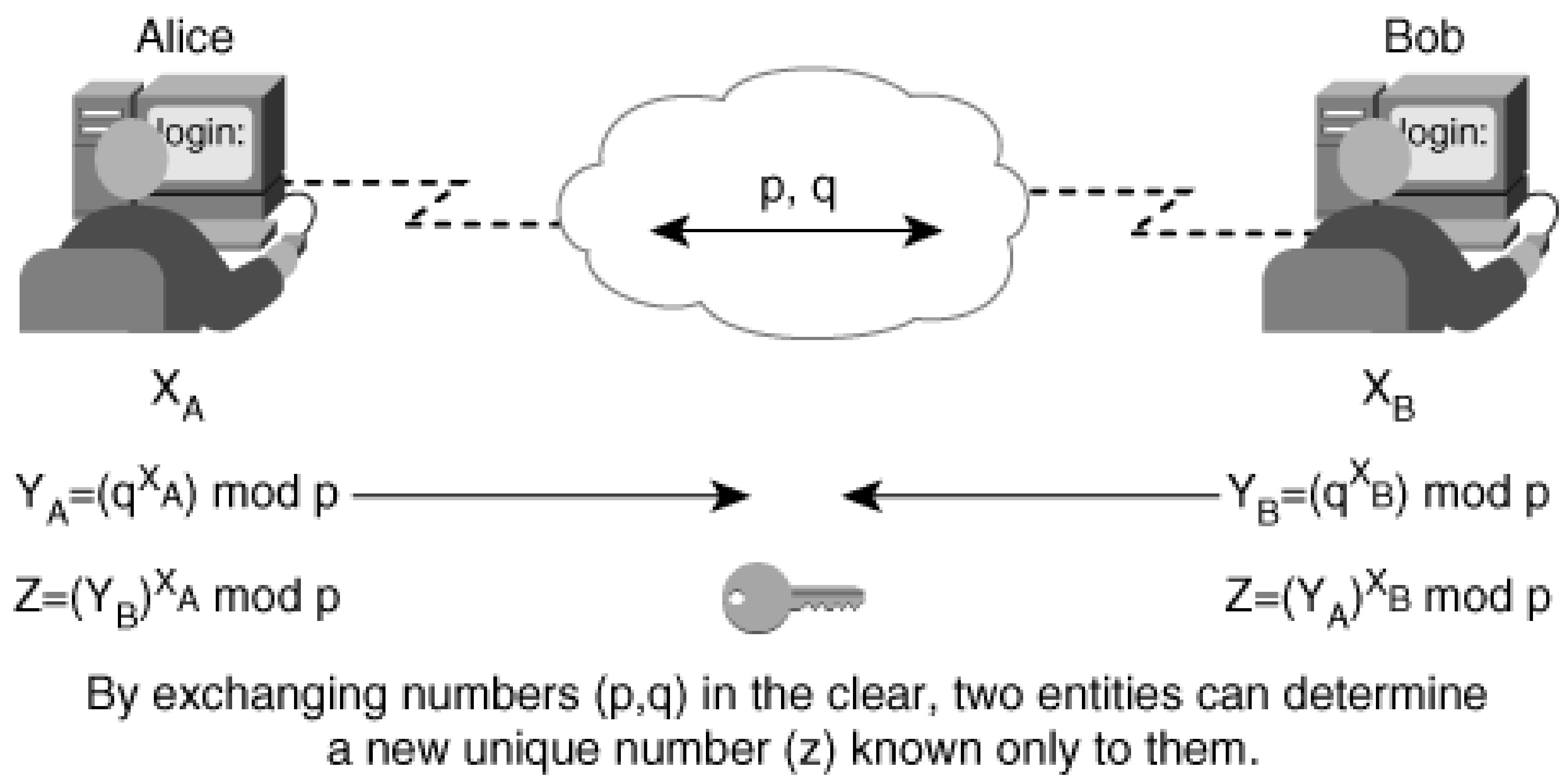
Verifying a Digital Signature



Key Management

- a difficult problem in secure communications, largely due to social rather than technical factors
- Scalability and manageability are two important factors
- Current wireless technologies use symmetric key encryption
- For a small number of access points (APs) and clients, it is reasonable to create a key and manually enter it. However, in most wide-scale corporations, this mechanism is awkward and outdated.

Establishing Secret Keys Using the Diffie-Hellman Algorithm



Creating and Distributing Public Keys

- ensure the uniqueness of each public/private key pair
- the creation of sets of parameters that meet the needs of the algorithm (for example, prime numbers for RSA)
- The problem is how you can distribute the public keys in a secure manner and how you can trust the entity that gives you the key.

RSA Public-key algorithm

- RSA is a **block cipher. The ingredients of RSA scheme are:**
  - **p, q, two prime numbers (private, chosen)**
  - **$n = pq$, $\Phi(n)=(p-1)(q-1)$ (public, calculated)**
  - **e, with $\gcd(\Phi(n),e)=1$; $1<e< \Phi(n)$ (public, chosen)**
  - **$d = e^{-1} \bmod \Phi(n)$ (private, calculated)**
  - **Private key = {d, n}**
  - **Public key = {e, n}**
- Suppose that B has published its public key and that A wishes to send the message M to B. Then A calculates
  - **$C = M^e \pmod n$**

  and transmits C.
- On receipt of this cipher text, B decrypts by calculating
  - **$M= C^d \pmod n$.**

RSA Example

- Select two prime numbers **p=7 and q=17.**
- Calculate **n=pq=7*17=119.**
- Calculate **Φ(n)=(p-1)(q-1) = 6*16 = 96.**
- Select e such that e is relatively prime to **Φ(n)=96** and less than **Φ(n)**; in this case, **e=5.**
- Determine **d** such that **de=1 mod 96** and **d<96**. The correct value is **d=77** because **77*5=385=4*96+1.**
- The resulting keys are public key **KU={5,119} and private key KR={77,119}.**

- The following example shows the use of these keys for a plaintext input of **M=19**.
- For encryption, **19** is raised to the fifth power, yielding **2476099**. Upon division by **119**, the remainder is determined to be **66**.
  - Hence, $\mathbf{19^5=66 \bmod 119}$**,** and the ciphertext is **66.**
- For decryption, it is determined that $\mathbf{66^{77}=19 \bmod 119}$**.**

Digital Certificates

- to distribute public keys.
- require the use of a trusted third party: the certificate authority.
- a digitally signed message that typically is used to attest to the validity of a public key of an entity.

The general format of a certificate

- Version number
- Serial number of the certificate
- Issuer algorithm information
- Issuer of certificate
- Valid to/from date
- Subject's public key
- Public key algorithm information of the subject of the certificate
- Digital signature of the issuing authority
- Optional extensions

Certificate Authorities (CA)

- The trusted third party that vouches for the validity of the certificate.

- It is up to the CA to enroll certificates, distribute certificates, and remove (revoke) certificates when the information they contain becomes invalid.

Obtaining a Public Key in a Trusted Manner Using a CA