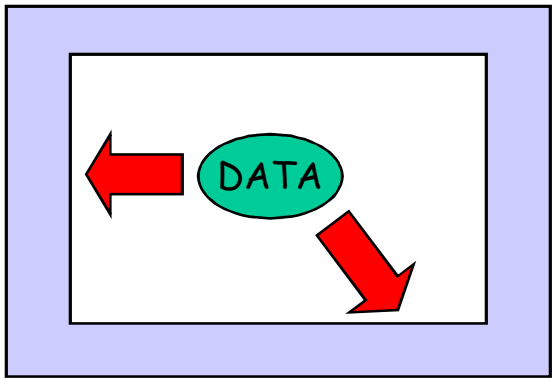
E-commerce Systems security

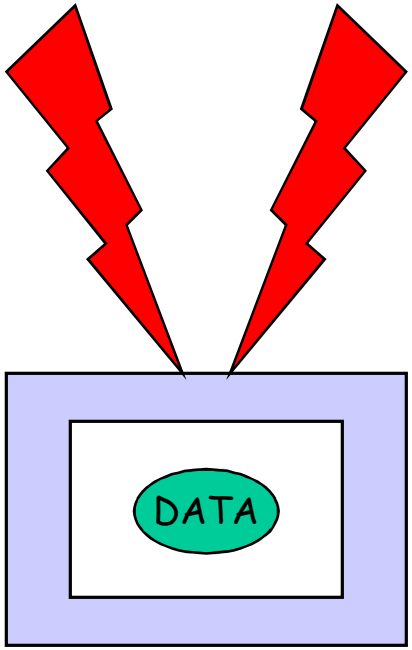
Security Function of Network

- **Availability** -- System resources are safeguarded from tampering and are available for authorized users at the time and in the format needed
- **Confidentiality** -- Information is not accessed or disclosed to unauthorized individuals, entities, or processes
- **Identification and Authentication** -- Verification that the originator of a transaction is the originator
- **Integrity** -- Information is not altered by an unauthorized person or process
- **Non-repudiation** -- Undeniable proof of participation by the sender and/or receiver in a transaction

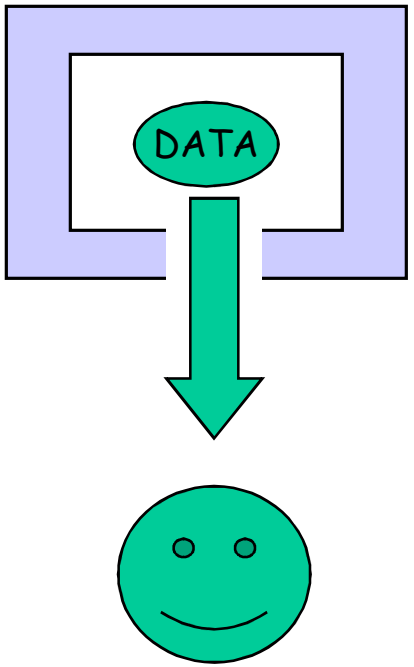
Goals of Security



Confidentiality



Integrity



Availability

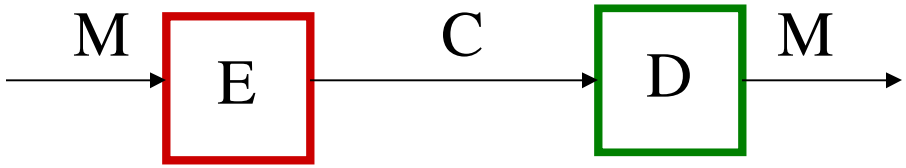
Cryptography Algorithms

- **Symmetric Algorithm (Secret Key Algorithm)**
- **Public Key Algorithm**
- **Message Digest**

Cryptography: Basic Terminology

- Plaintext (or cleartext)
  - The message.
  - Denoted by M or P.
- Encryption (encipher)
  - Encoding of message.
  - Denoted by E.
- Ciphertext
  - Encrypted message.
  - Denoted by C.
- Decryption (decipher)
  - decoding of ciphertext
  - denoted by D.

Encryption and Decryption



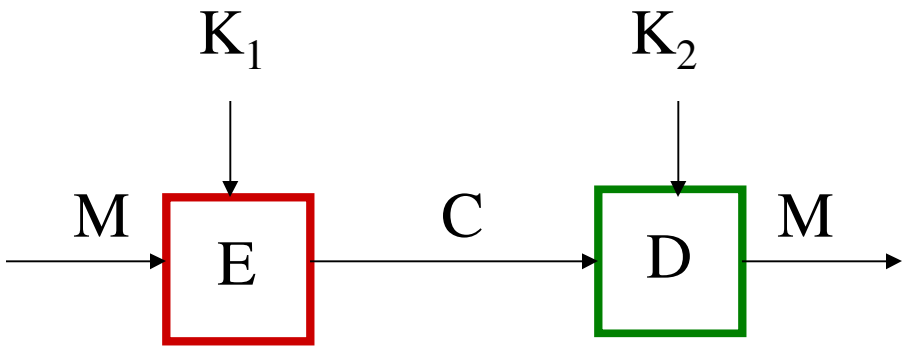
The following identity must hold true:

$D(C) = M$, where $C = E(M)$

Cryptography: Algorithms and Keys

- A method of encryption and decryption is called a **cipher**.
- Generally there are two related functions: one for encryption and other for decryption.
- Some cryptographic methods rely on the secrecy of the algorithms.
- Such methods are mostly of historical interest.
- All modern algorithms use a **key** to control encryption and decryption.
- Encryption key may be different from decryption key.

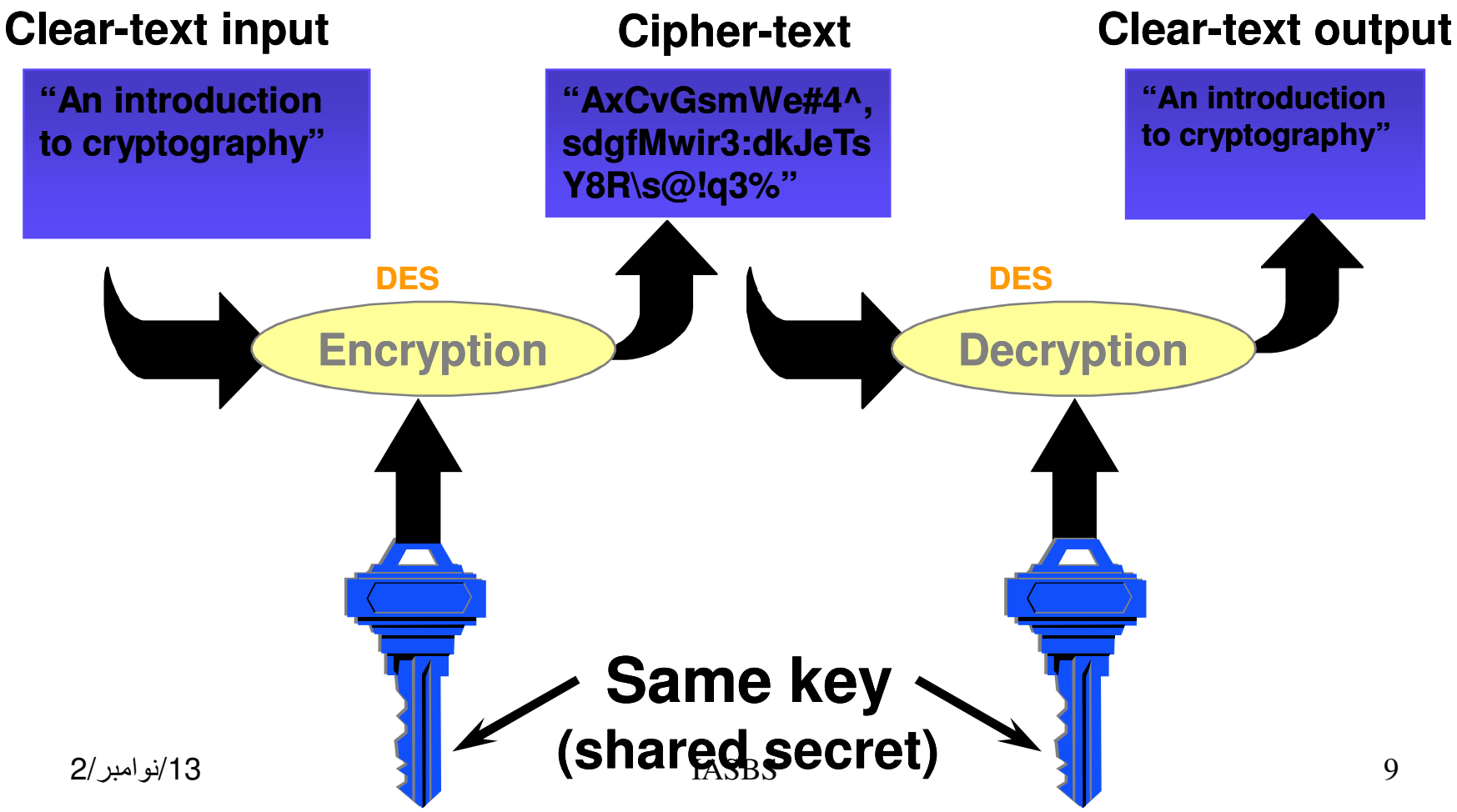
Key Based Encryption/Decryption



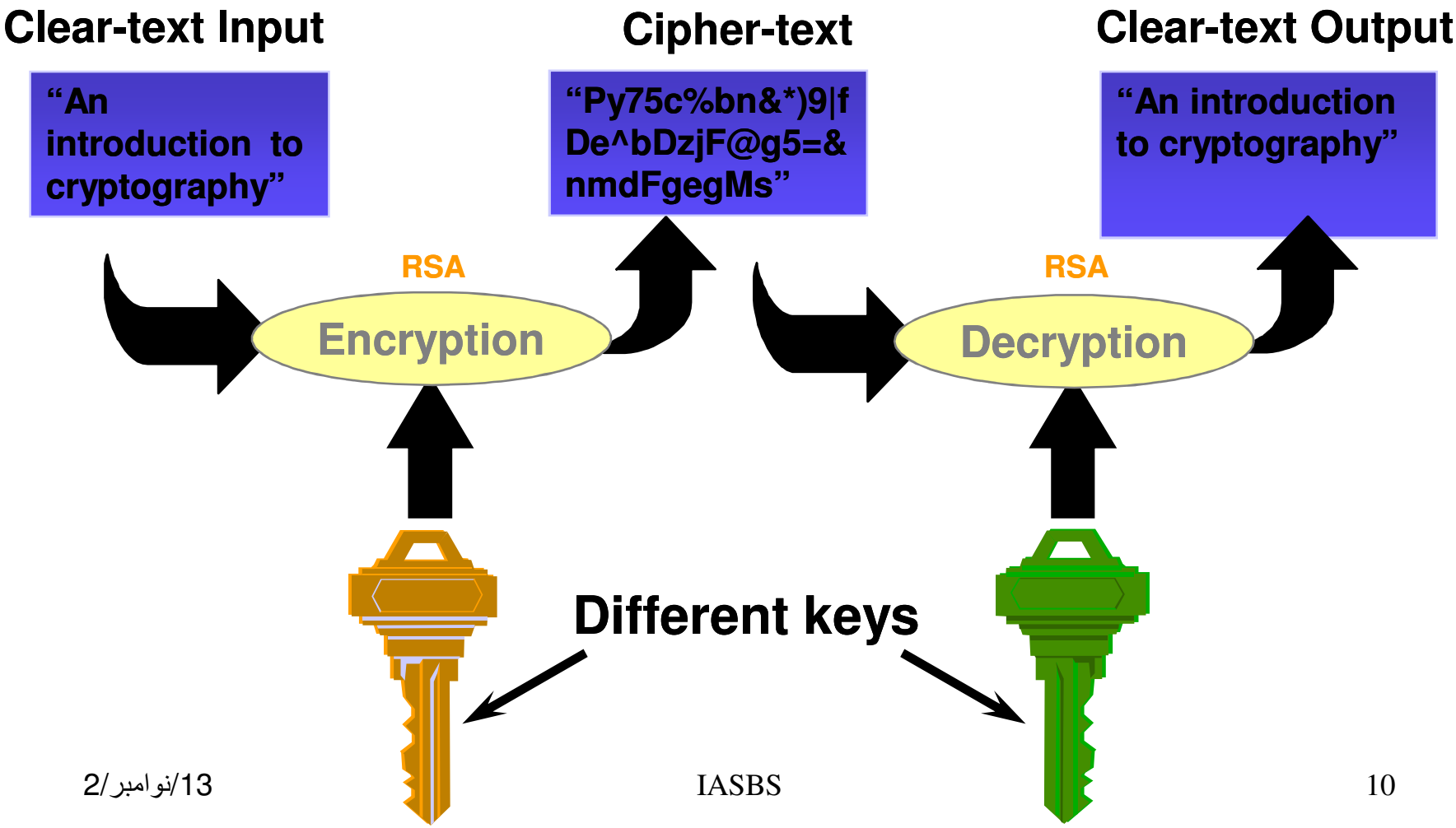
Symmetric Case: both keys are the same or derivable from each other.

Asymmetric Case: keys are different and not derivable from each other.

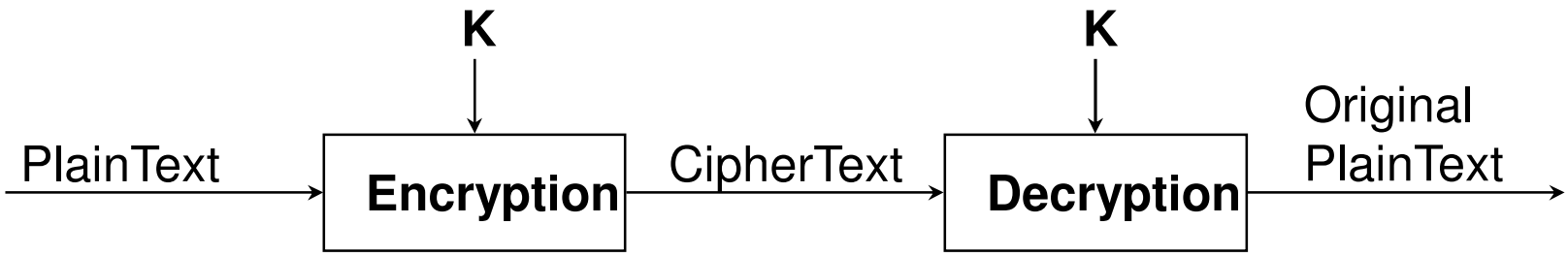
Symmetric Encryption



Asymmetric Encryption

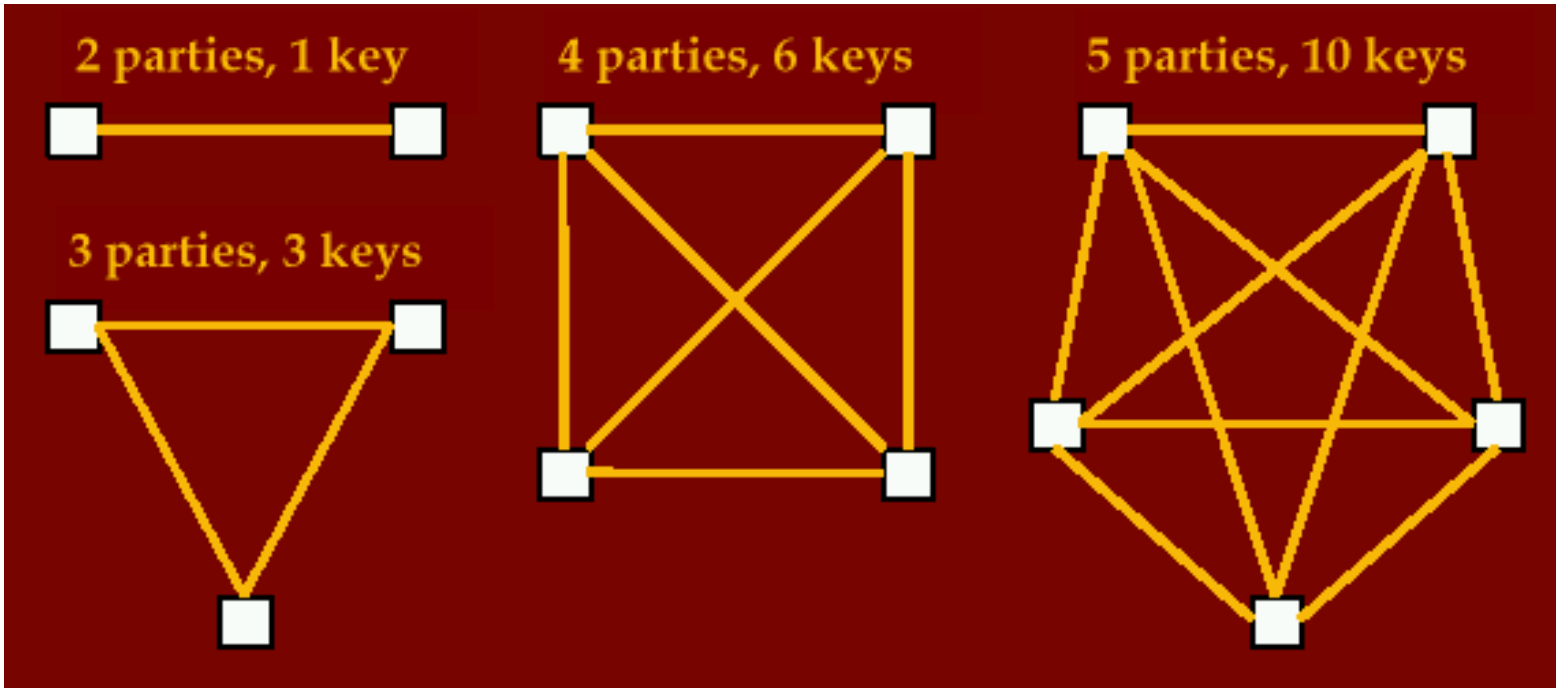


Symmetric Algorithm



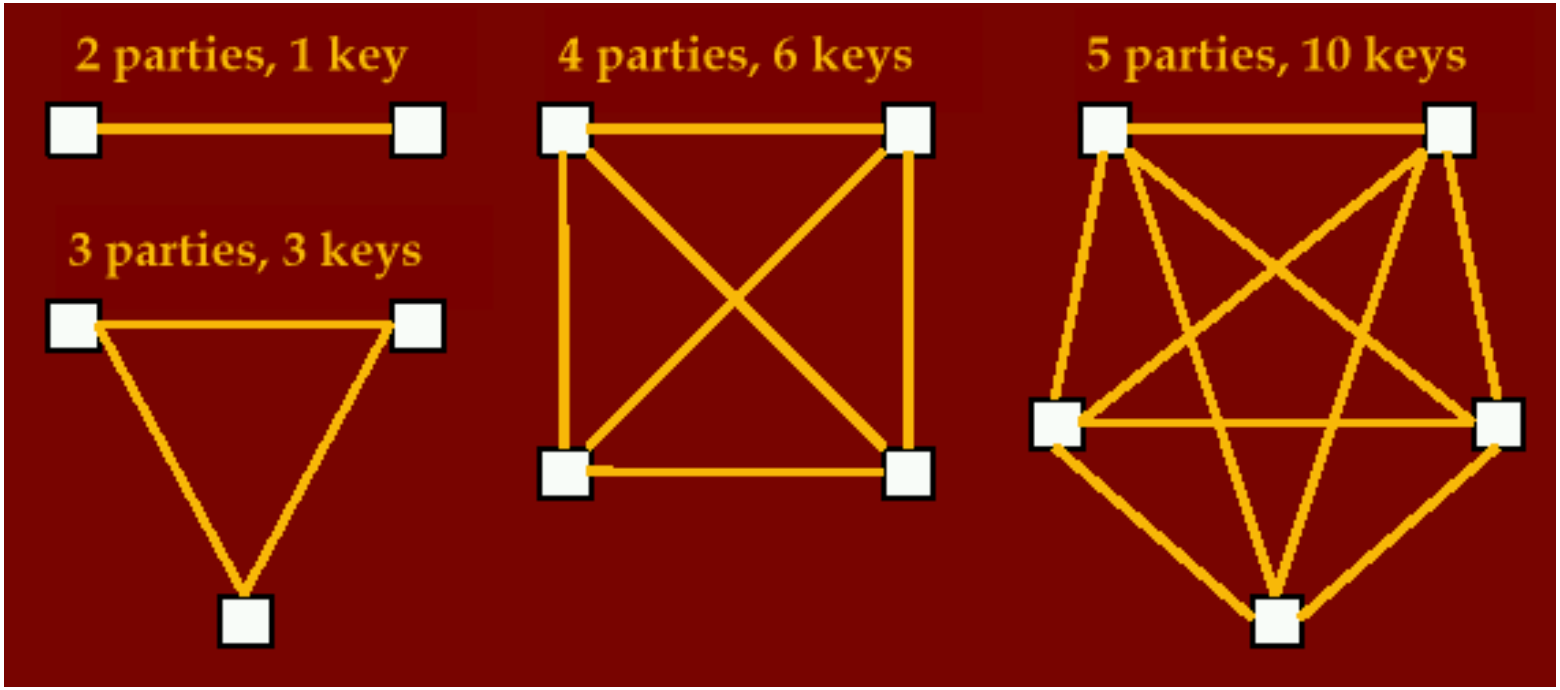
- Also called symmetric or single-key algorithms.
  - Stream ciphers: operate on single bit or byte.
  - Block ciphers: operate on blocks (typically 64 bits)
- Sender and Receiver Use Same Secret Key
- Advantage :simple, Fast Encryption and Decryption
- Disadvantage: key exchange, key management
- Algorithms : RC4, DES, IDEA, etc

Symmetric Key - Issues



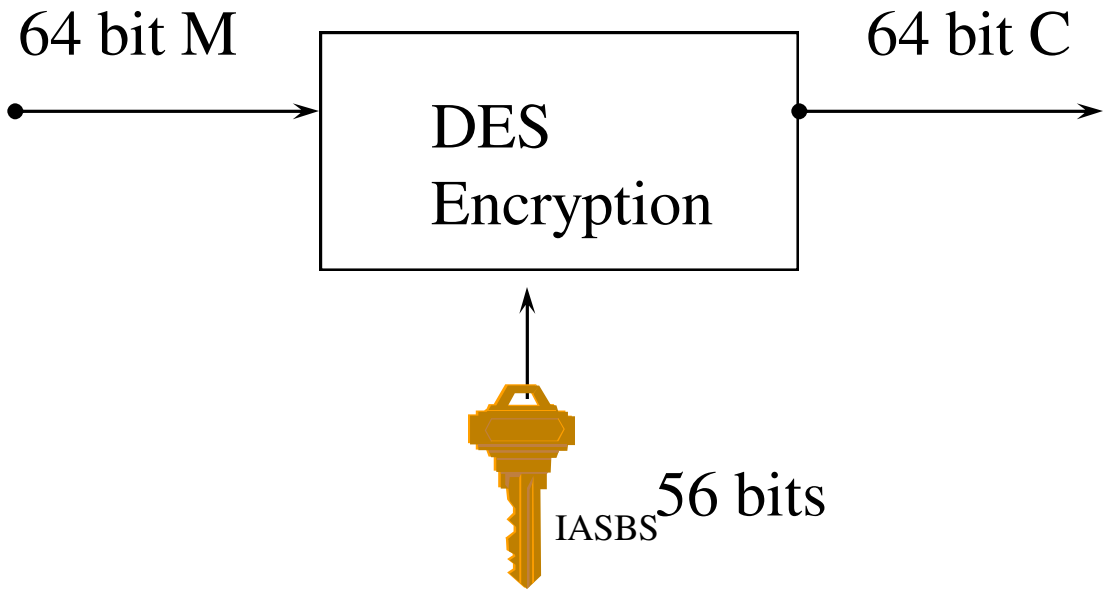
Symmetric Key - Issues

Key management, keys required = (p*(p-1))/2 or:

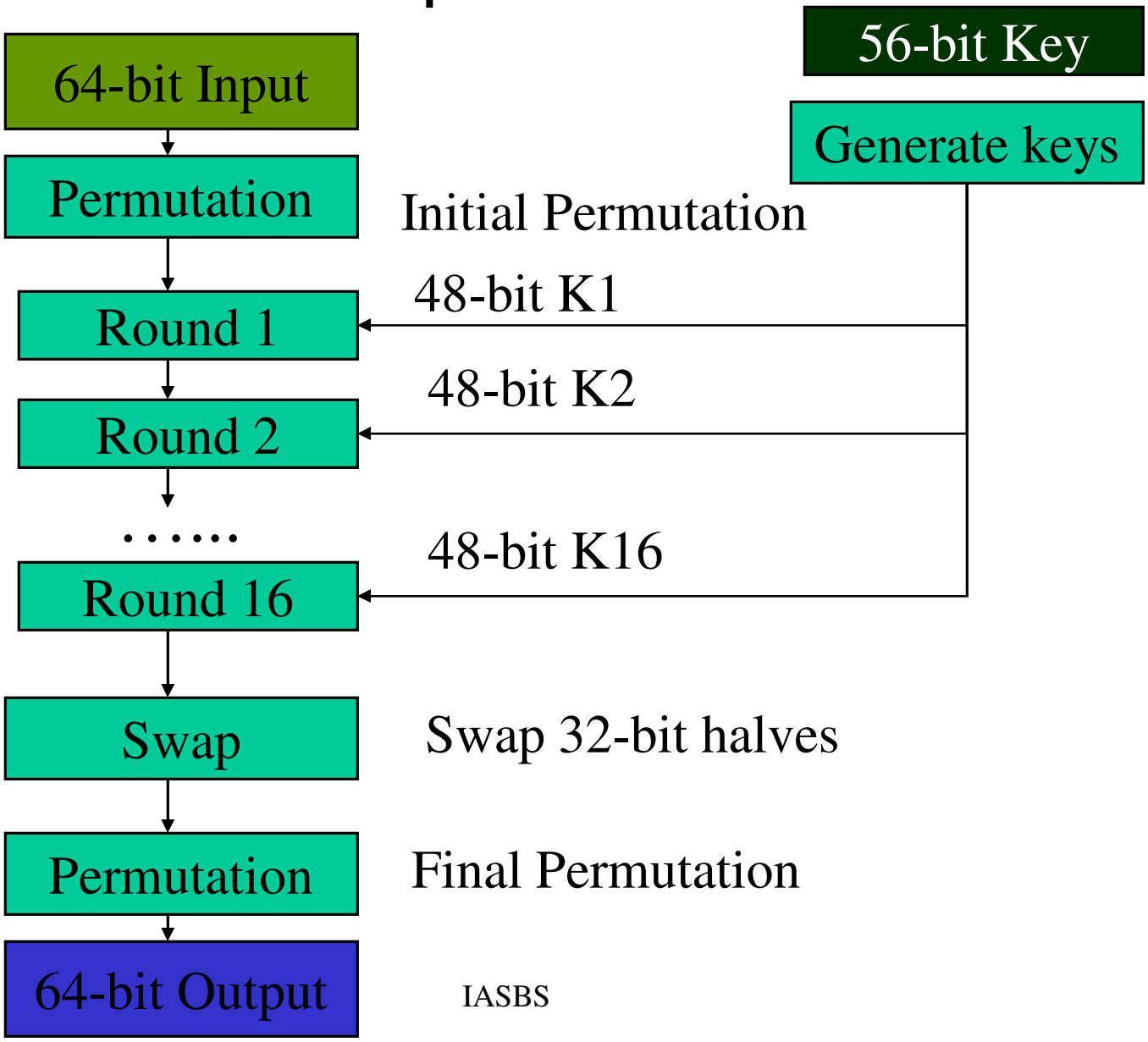


DES (Data Encryption Standard)

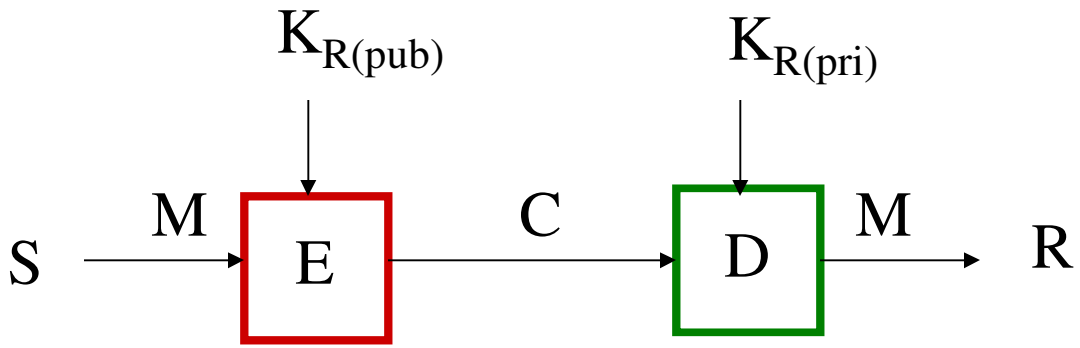
- Published in 1977, standardized in 1979.
- Key: 64 bit quantity=8-bit parity + 56-bit key
  - Every 8th bit is a parity bit.
- 64 bit input, 64 bit output.
- Encrypts 64-bit data using 56-bit key



DES: Top-Down View

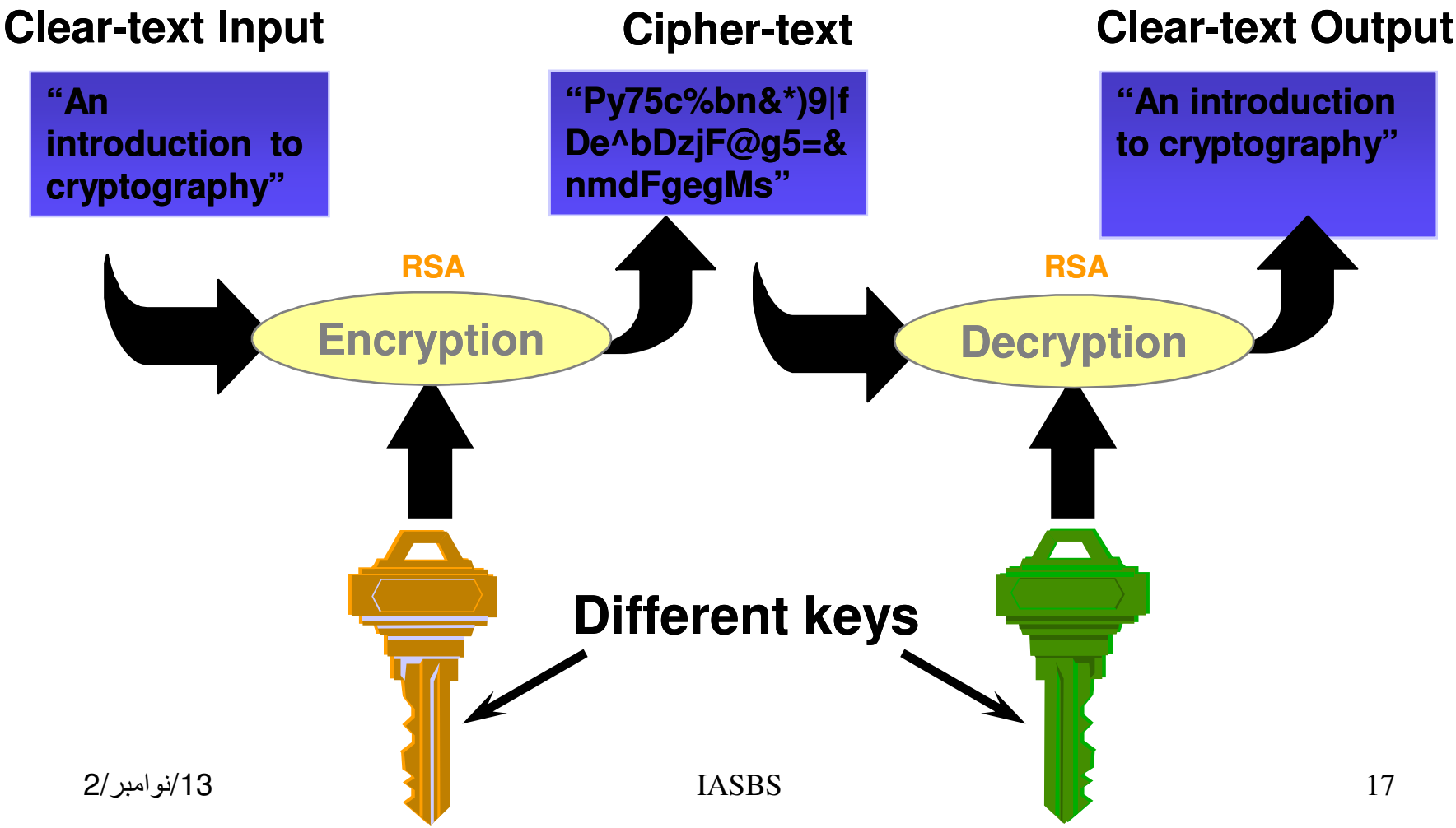


2. Public Key Cryptography

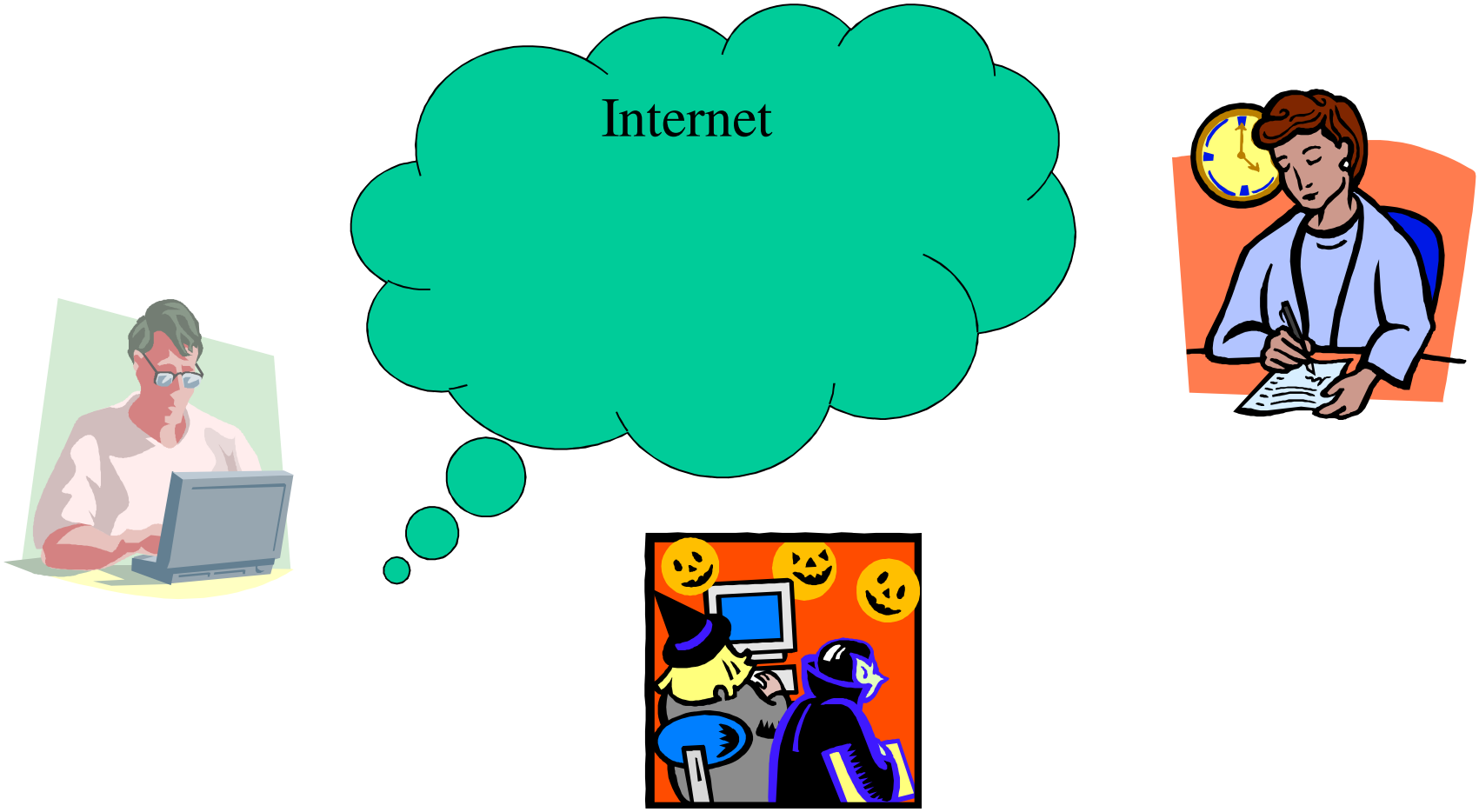


$K_{R(pub)}$ is Receiver's public key and $K_{R(pri)}$ is Receiver's private key.

Asymmetric Encryption



Establishing Shared Secrete



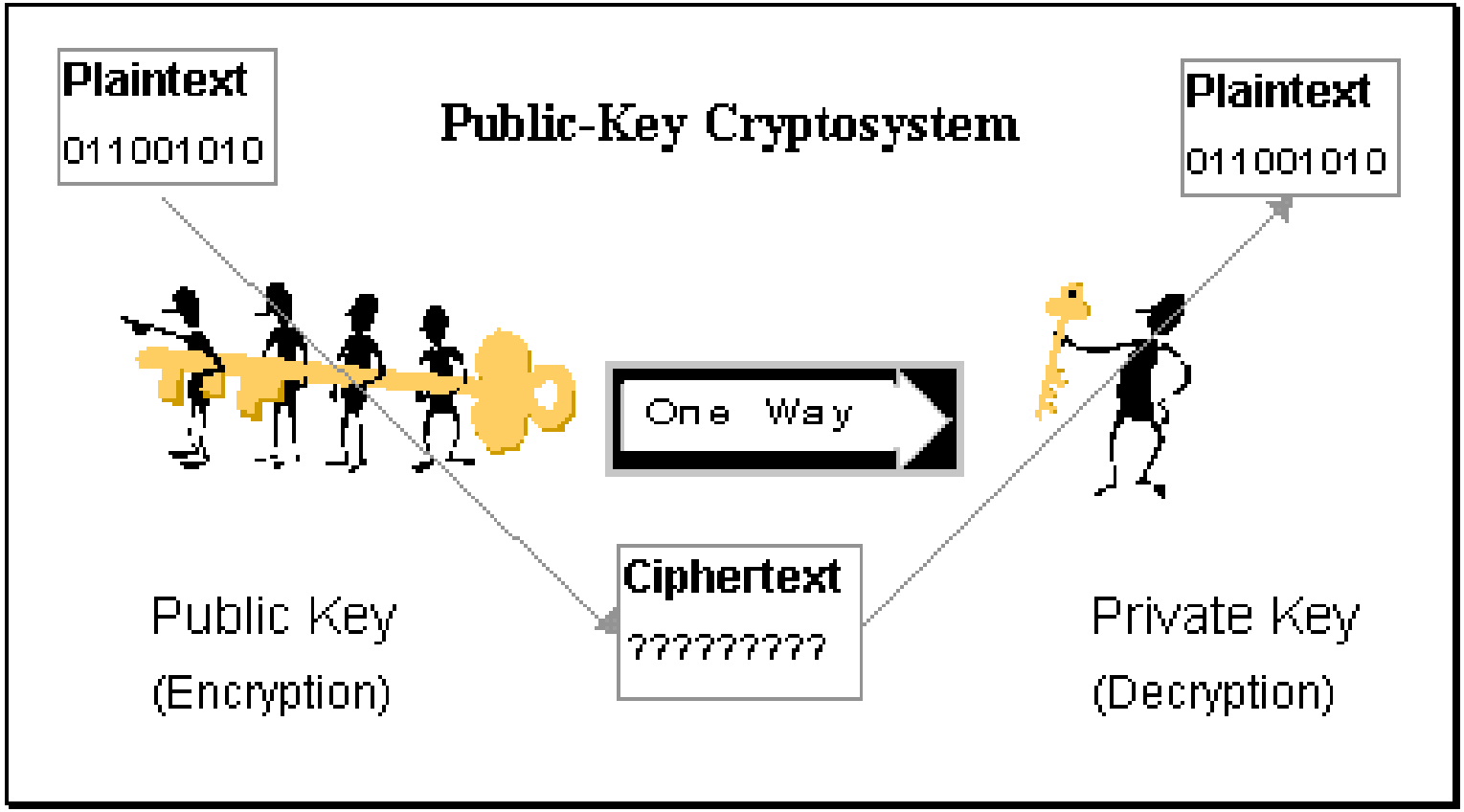
Simplified Math Tricks

- Public key cryptography is based on the mathematical concept of multiplicative inverse.
- Multiplicative inverses are two numbers that when multiplied equals one (e.g., 7 x 1/7 = 1)
- In modular mathematics, two whole numbers are inverses if they multiplies to 1 (e.g., 3 x 7 mod 10 = 1)
- Use modular inverse pairs to create public and private keys.
- Example
  - Message is 4
  - To scramble it, use 4 X 3 mod 10 = 2
  - To recover it, use 2 x 7 mod 10 = 4

Asymmetric Algorithms

- Also called public-key algorithms.
- Encryption key is different from decryption key.
- Furthermore, one cannot be calculated from other.
- Encryption key is often called the **public key** and decryption key is often called the **private key**.
- Advantages: better key management.
- Disadvantages: slower, more complex.
- Examples: RSA, Diffie-Hellman, El Gamal, etc.

Public Key Cryptosystem



RSA Public Keys

- Named for Ron Rivest, Adi Shamir, and Len Adleman, published in 1978.
- Most widely known and used public key system.

RSA Key Generation

- Pick large random primes p,q.
- Let p*q = n and β=(p-1)(q-1).
- Choose a random number e such that: 1<e<β and gcd(e, β)=1. (relative primes)
- Calculate the unique number d such that 1<d<β and $d*e \equiv 1 \pmod{\beta}$. (d is inverse of e)
- The public key is {e,n} and the private key is {d,n}.
- The factors p and q may be kept private .

Encryption and Decryption

- Suppose Alice wants to send a message m to Bob.
- Alice computes $c = m^e \bmod n$, where {e,n} is Bob's public key.
- She sends c to Bob.
- To decrypt, Bob computes $m = c^d \bmod n$, where {d,n} is Bob's private key.
- The mathematical relationship between e and d ensures that Bob correctly recovers m.
- Since only Bob knows d, only he can decrypt.

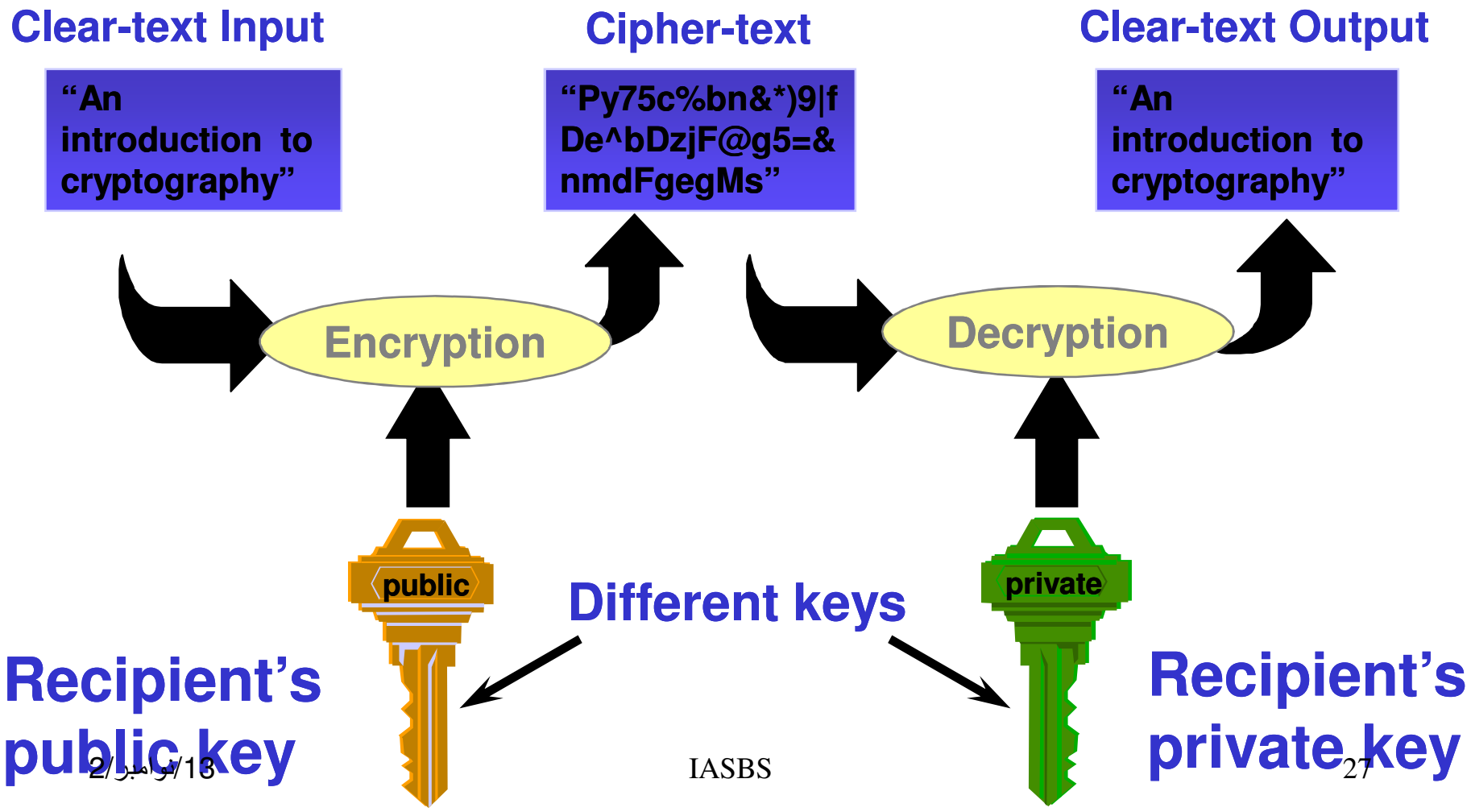
RSA - Authentication

- Suppose Alice wants to send a message m to Bob and ensure him that the message is indeed from her.
- Alice computes signature $s = m^d \bmod n$, where (n,d) is Alice's private key.
- She sends m and s to Bob.
- To verify the signature, Bob computes using (n,e) $m = s^e \bmod n$ and checks that it is recovered.
- In practice, RSA is combined with a symmetric key cryptosystem (e.g., DES) to encrypt.
- RSA is usually combined with a hash function to sign a message.

RSA Example - Key Setup

1. Select primes: $p=17$ & $q=11$
2. Compute $n = pq = 17 \times 11 = 187$
3. Compute $\phi(n)=(p-1)(q-1)=16 \times 10=160$
4. Select e: $\gcd(e,160)=1$; choose $e=7$
5. Determine d: $de=1 \bmod 160$ and $d < 160$ Value is $d=23$ since $23 \times 7=161= 1 \times 160+1$
6. Publish public key $PU=\{7,187\}$
7. Keep secret private key $PR=\{23,187\}$

Example: Confidentiality



Diffie-Hellman Key Exchange

- Only for Key Exchange
- Does NOT Encrypt or Decrypt
- by Diffie & Hellman in 1976
- is a practical method for public exchange of a secret key
- Widely used in Security Protocols and Commercial Products

Global Public Elements

- q Prime number
- α $\alpha < q$

User A Key Generation

- Select private X_A $\quad X_A < q$
- Calculate public Y_A $\quad Y_A = \alpha^{X_A} \bmod q$

User B Key Generation

- Select private X_B — $X_B < q$
- Calculate public Y_B — $Y_B = \alpha^{X_B} \bmod q$

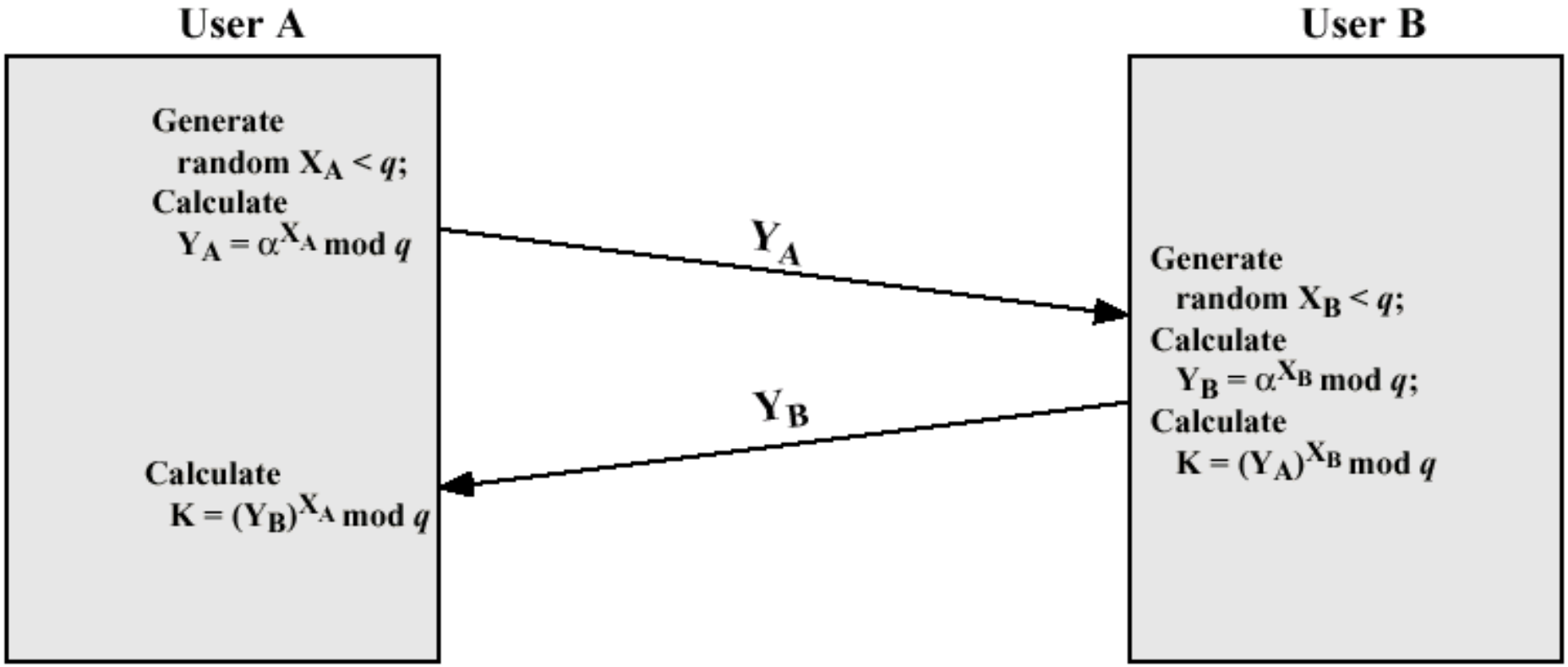
Generation of Secret Key by User A

- $K = (Y_B)^{X_A} \bmod q$

Generation of Secret Key by User B

- $K = (Y_A)^{X_B} \bmod q$

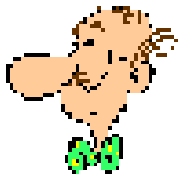
Diffie-Hellman Key Exchange



Diffie-Hellman Key Exchange

Alice
A

Public Parameters:
large prime **q**
primitive root **a**



Bob
B

Choose a secret X_A

Compute $Y_A = a^{X_A} \bmod q$

Send Y_A →

Shared Key
$K_{AB} = Y_B^{X_A}$
$= a^{X_B X_A} \bmod q$

Choose a secret X_B

Compute $Y_B = a^{X_B} \bmod q$

← **Send** Y_B

Shared Key
$K_{AB} = Y_A^{X_B}$
$= a^{X_A X_B} \bmod q$

Diffie-Hellman Example

- users Alice & Bob who wish to swap keys:
- agree on prime $q=353$ and $\alpha=3$
- select random secret keys:
  - A chooses $x_A=97$, B chooses $x_B=233$
- compute public keys:
  - $y_A=3^{97} \bmod 353 = 40$ (Alice)
  - $y_B=3^{233} \bmod 353 = 248$ (Bob)
- compute shared session key as:

$K_{AB}= y_B^{x_A} \bmod 353 = 248^{97} = 160$ (Alice)

$K_{AB}= y_A^{x_B} \bmod 353 = 40^{233} = 160$ (Bob)

ELGAMAL CRYPTOGRAPHIC

Global Public Elements	
q	prime number
α	$\alpha < q$ and α a primitive root of q

Key Generation by Alice	
Select private X_A	$X_A < q - 1$
Calculate Y_A	$Y_A = \alpha^{XA} \bmod q$
Public key	$PU = \{q, \alpha, Y_A\}$
Private key	X_A

ELGAMAL CRYPTOGRAPHIC

Encryption by Bob with Alice's Public Key	
Plaintext:	$M < q$
Select random integer k	$k < q$
Calculate K	$K = (Y_A)^k \bmod q$
Calculate C_1	$C_1 = \alpha^k \bmod q$
Calculate C_2	$C_2 = KM \bmod q$
Ciphertext:	(C_1, C_2)

ELGAMAL CRYPTOGRAPHIC

Decryption by Alice with Alice's Private Key	
Ciphertext:	(C_1, C_2)
Calculate K	$K = (C_1)^{XA} \bmod q$
Plaintext:	$M = (C_2 K^{-1}) \bmod q$

Alice generates a key pair as follows:

1. Alice chooses $X_A = 5$.
2. Then $Y_A = \alpha^{X_A} \bmod q = \alpha^5 \bmod 19 = 3$ (see Table 8.3).
3. Alice's private key is 5; Alice's pubic key is $\{q, \alpha, Y_A\} = \{19, 10, 3\}$.

ELGAMAL CRYPTOGRAPHIC

Suppose Bob wants to send the message with the value $M = 17$

1. Bob chooses $k = 6$.
2. Then $K = (Y_A)^k \bmod q = 3^6 \bmod 19 = 729 \bmod 19 = 7$.
3. So
   $C_1 = \alpha^k \bmod q = \alpha^6 \bmod 19 = 11$
   $C_2 = KM \bmod q = 7 \times 17 \bmod 19 = 119 \bmod 19 = 5$
4. Bob sends the ciphertext $(11, 5)$.

ELGAMAL CRYPTOGRAPHIC

For decryption:

1. Alice calculates $K = (C_1)^{X_A} \bmod q = 11^5 \bmod 19 = 161051 \bmod 19 = 7$.
2. Then K^{-1} in GF(19) is $7^{-1} \bmod 19 = 11$.
3. Finally, $M = (C_2 K^{-1}) \bmod q = 5 \times 11 \bmod 19 = 55 \bmod 19 = 17$.

تمرین

- روشهای ممکن برای شکستن الگوریتم RSA چیست؟ توضیح دهید؟
- چه روشی برای شکستن پروتکل مبادله کلید عمومی Diffie-Hellman وجود دارد توضیح دهید؟
- الگورتم 3DES راتوضیح دهید ؟ چرا از 2DES استفاده نمیشود؟
- رمزگذاری منحنی بیضوی ECC را به طور کامل شرح دهید؟

Q&A