Cryptology

Basic Terminology

- **plaintext** - original message
- **ciphertext** - coded message
- **cipher** - algorithm for transforming plaintext to ciphertext
- **key** - info used in cipher, known only to sender/receiver
- **encipher (encrypt)** - converting plaintext to ciphertext
- **decipher (decrypt)** - recovering ciphertext from plaintext
- **cryptography** - study of encryption and decryption principles/methods
- **cryptanalysis (codebreaking)** - study of principles/ methods of deciphering ciphertext *without* knowing key
- **cryptology** - field of both cryptography and cryptanalysis

Cryptography Ciphers

- Plaintext can be encrypted through stream cipher or block cipher.
- Stream cipher: each plaintext bit transformed into ciphertext bit, one bit at a time
- Block cipher: message divided into blocks (e.g., sets of 8- or 16-bit blocks) and each is transformed into encrypted block.

Cryptography Techniques

- Symmetric Cryptography:

If

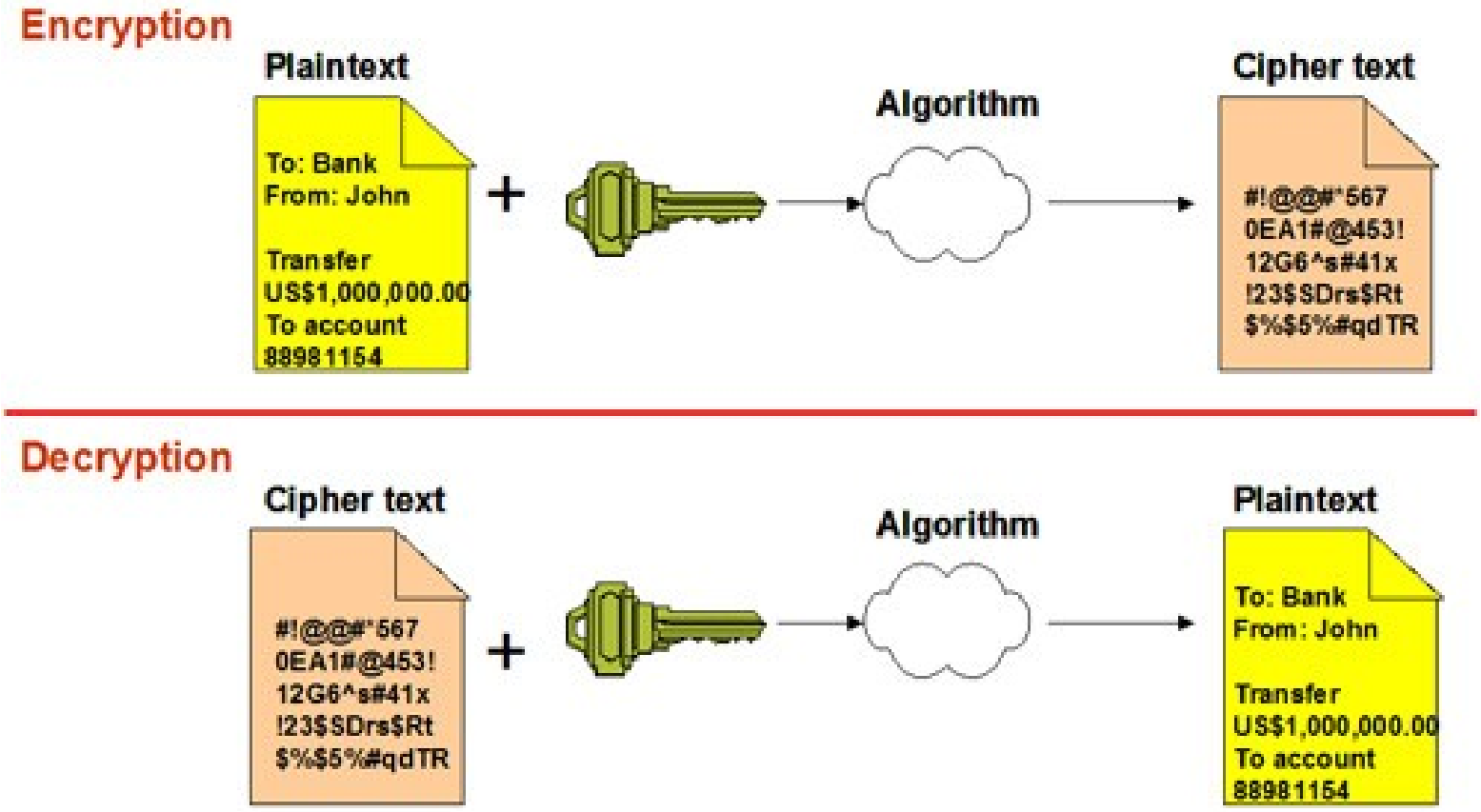
Encryption key = Decryption Key (same)

- Asymmetric Cryptography:

If

Encryption key ≠ Decryption Key (different)

Cryptography Techniques



Cipher Types

1. **Block Cipher:**

   Message will be divided into blocks, for example 64 bits and the encryption process will take place on each block.

2. **Stream Cipher:**

   Encryption process will take place on each bit with the key bit

Block Cipher

1. **Substitution Cipher:**

- A technique in which the letters of plaintext are replaced by other letters or symbols.
- Position of a letter is fixed but its value will be changed.

2. **Transposition Cipher:**

- Value of a letter is fixed but its position is changed.

3. **Product Cipher:**

- Value and position of a letter are changed.

Substitution Cipher

- **Mono-alphabetic cipher**

A cipher that uses fixed substitution over the entire message.

- **Poly-alphabetic cipher**

A cipher that uses a number of substitutions at different positions in the message.

Cryptography Key Size

- When using ciphers, size of the cryptography key very important
- Strength of many encryption applications and cryptosystems measured by the key size
- For cryptosystems, security of encrypted data is not dependent on keeping cryptography algorithm secret
- Cryptosystem security depends on keeping some or all of elements of key(s) secret