Computer Networks COL 334/672

Network Security

Tarun Mangla

Slides adapted from KR

Sem 1, 2024-25

Network Security

- **What**: protecting network from an attack

Ransomware hits Telangana and Andhra Pradesh power department websites

Mahesh Buddi / TNN / Updated: May

The computer systems of Telangar
Ransomware attacked the systems
Officials in the Telangana power de

1.3 TB data encrypted and five servers affected in AIIMS ransomware attack: Centre

CERT-In and other stakeholder entities have advised necessary remedial measures, Minister tells Rajya Sabha

India Recorded 79 Million Cyber Attacks In 2023, Ranks 3rd Globally: Report
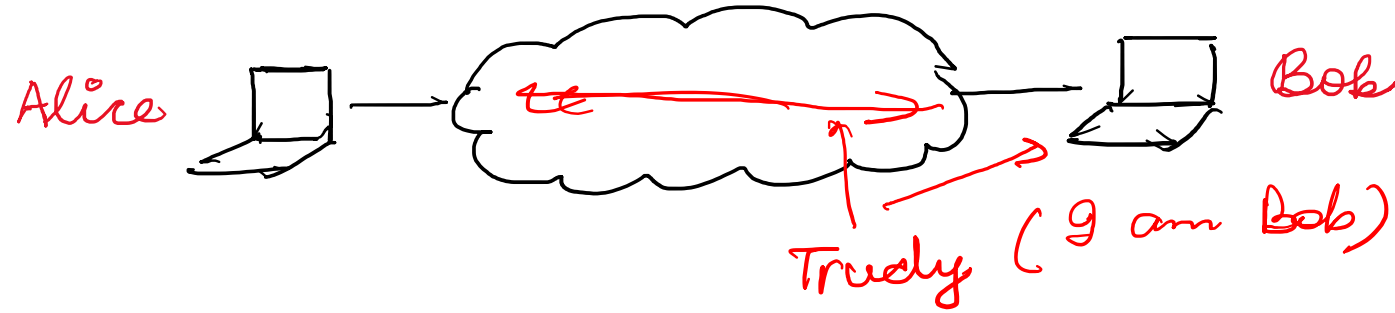
decentralization security

- **Historical perspective:** Internet was not designed with in mind (?)
  - Patches added to provide cybersecurity

What kinds of network attacks?

① Phishing

Alice

Trudy (I am Bob)

Bob

① Spoofing
② Eavesdropping
③ Denial of Service
   (Bring down of availability)

④ Modification of data

① Eavesdropping
   ↳ confidentiality

②. Modification of data
   (Message integrity)

③ Spoofing ; Authentication

④ _ Access & availability

What is network security?

Encryption → Cryptography

confidentiality: only sender, intended receiver should "understand" message contents
- sender encrypts message
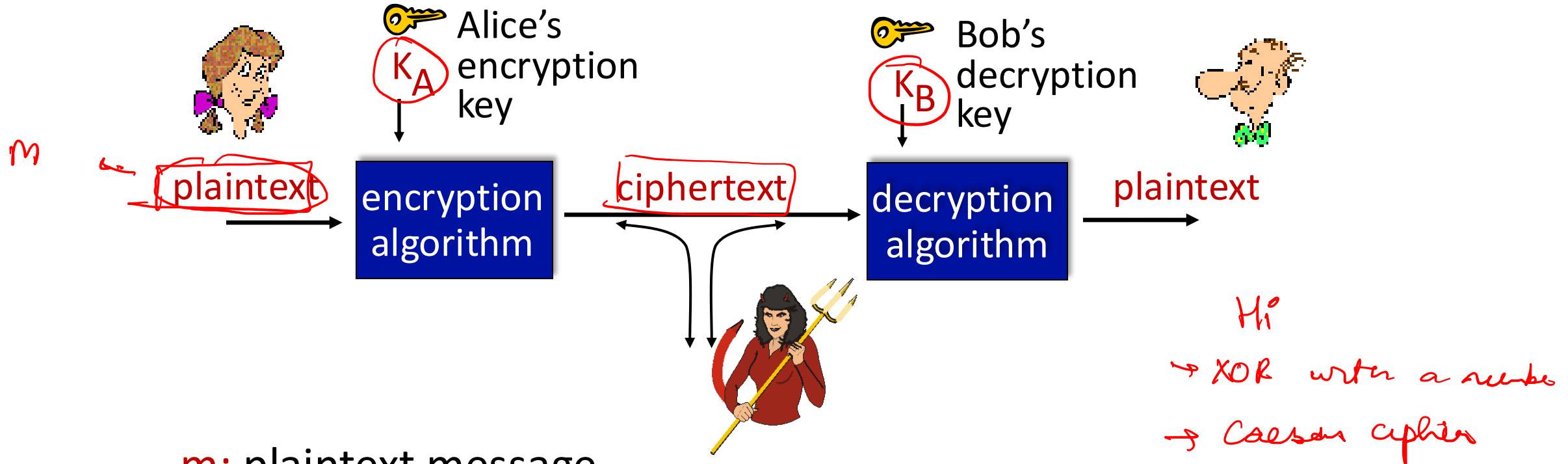- receiver decrypts message

authentication: sender, receiver want to confirm identity of each other

message integrity: sender, receiver want to ensure message not altered (in transit, or afterwards) without detection

access and availability: services must be accessible and available to users

Providing confidentiality

$K_A = K_B$: Symmetric encryption Algorithm

m

Alice's encryption key

K_A

plaintext → encryption algorithm → ciphertext → decryption algorithm → plaintext

Bob's decryption key

K_B

Hi
→ XOR with a number
→ Caesar cipher

m: plaintext message

$K_A(m)$: ciphertext, encrypted with key K_A

$m = K_B(K_A(m))$

Symmetric key cryptography

plaintext → encryption algorithm → ciphertext $K_S(m)$ → decryption algorithm → plaintext

Keys: K_S, K_S
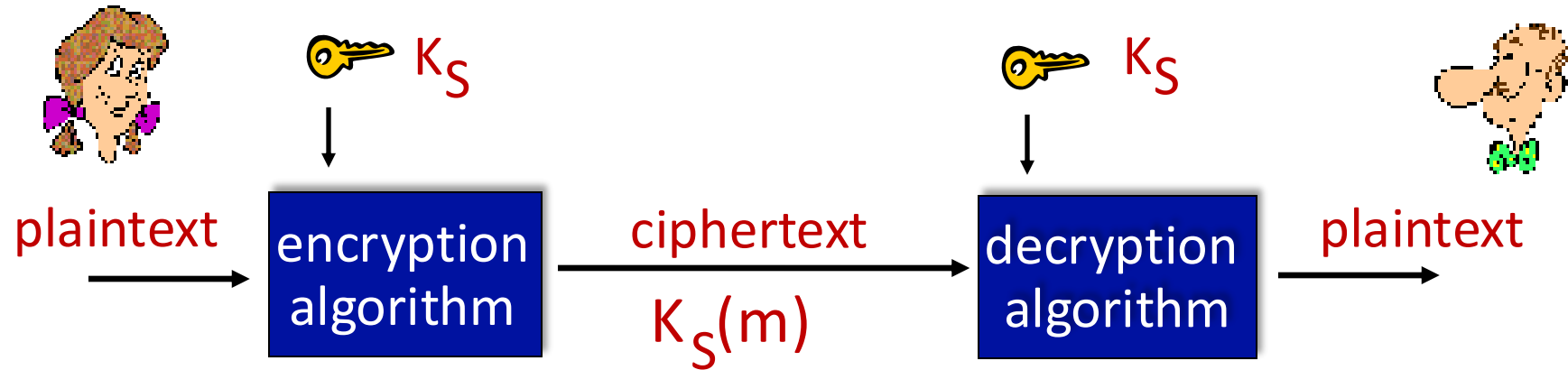
symmetric key crypto: Bob and Alice share same (symmetric) key: K

Symmetric key cryptography (example)

substitution cipher: substituting one thing for another

- monoalphabetic cipher: substitute one letter for another

```
plaintext:  abcdefghijklmnopqrstuvwxyz

ciphertext: mnbvcxzasdfghjklpoiuytrewq
```

Cipher text only attack

Brute force

↳ Statistical analysis

e.g.:
```
Plaintext: bob. i love you. alice
ciphertext: nkn. s gktc wky. mgsbc
```

→ Plain-text attack

🔑 *Encryption key:* mapping from set of 26 letters to set of 26 letters

How will you break such encryption?

Breaking an encryption scheme

good encryption scheme is hard to break w/ any of these attacks
computationally hard

- cipher-text only attack:
  Trudy has ciphertext she can analyze

- two approaches:
  - brute force: search through all keys
  - statistical analysis

- known-plaintext attack:
  Trudy has plaintext corresponding to ciphertext
  - *e.g.,* in monoalphabetic cipher, Trudy determines pairings for a,l,i,c,e,b,o,

- chosen-plaintext attack:
  Trudy can get ciphertext for chosen plaintext

Block Cipher

Substitution : $1 \longrightarrow 1$

- Cipher: n bits → n bits. Example: 3-bit block cipher:

Plain text
101 000

Cipher text
010 110

input	output	input	output
000	110	100	011
001	111	101	010
010	101	110	000
011	100	111	001

- How to do a brute-force attack on a 3-bit block cipher?

$2^{3}!$ mapping

Easy to break with

- What is the solution?
  - Use a large value of n. say 64-bit

    64-bit block cipher
    2^{64} bit table

  - The key becomes very large

64-bit Block Cipher Example

8 – different
cables

$T_1 \rightarrow T_8$

$$\frac{T_1 \rightarrow T_8}{n}$$

64-bit scrambler

64-bit input

| 8 bits | 8 bits | 8 bits | 8 bits | 8 bits | 8 bits | 8 bits | 8 bits |

| T_1 | T_2 | T_3 | T_4 | T_5 | T_6 | T_7 | T_8 |

| 8 bits | 8 bits | 8 bits | 8 bits | 8 bits | 8 bits | 8 bits | 8 bits |

Loop
for n
rounds

64-bit scrambler

64-bit output

64-bit output

Block Cipher

$K_s(m \oplus r)$

$(00000 \cdots)$
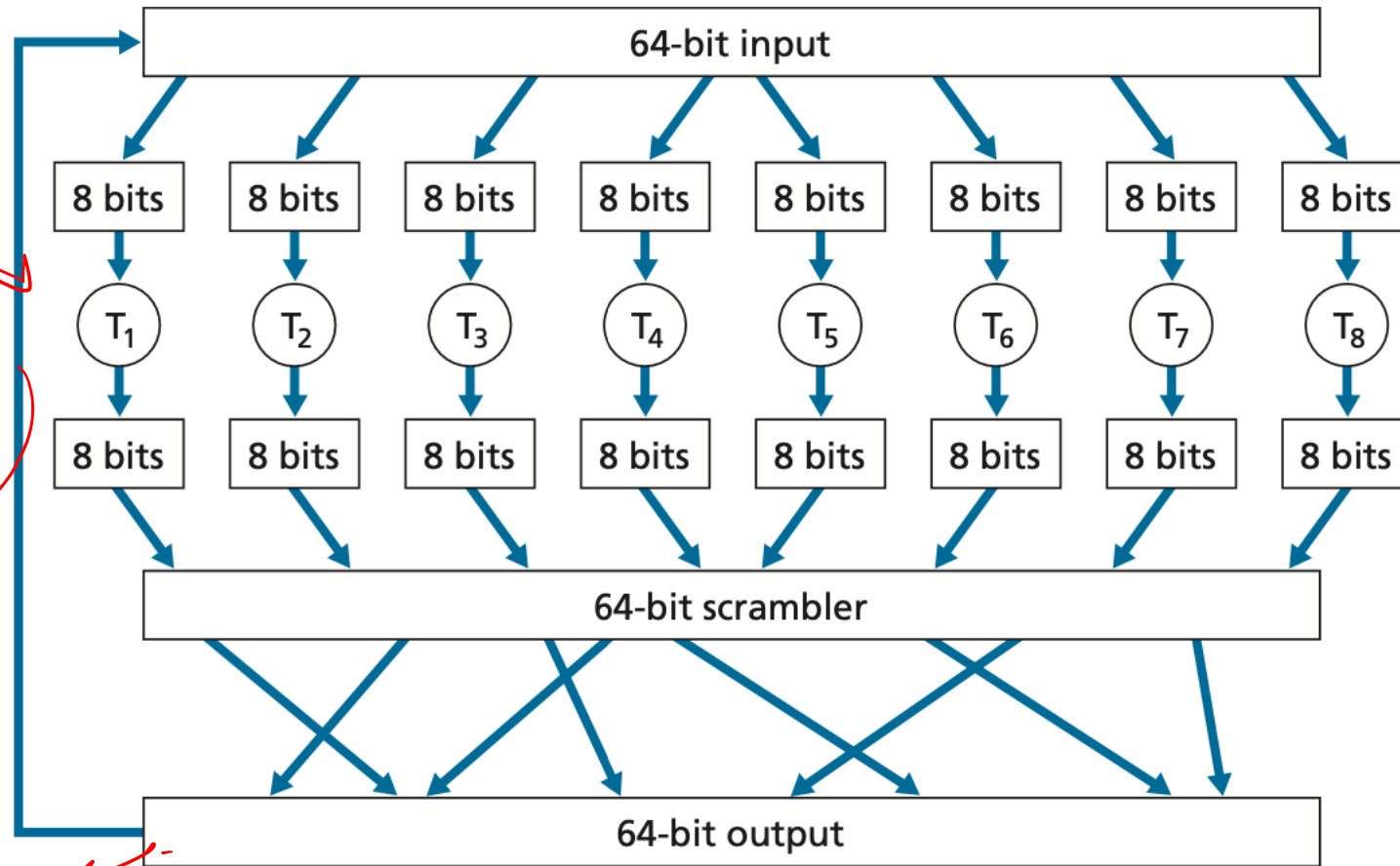
$(\text{const} \oplus xor)$

- Susceptible to known plaintext attack
  - For instance, two or more blocks could be "HTTP/1.1" which would lead to same ciphertext

- How to address this?

$c(i) = K_s(m(i) \oplus r(i))$

- Add some randomness into the ciphertext

Encryption

$c(1) \; r(1), \; c(2) \; r(2), \; c(3) \; r(3)$

n-bit message

↓
not efficient transmission $c(2)$

$m(i) = K_s^{-1}(c(i)) \oplus r(i)$

↓ de

$m(i) \oplus r(i) \oplus r(i)$

$= m(i) \; 000$

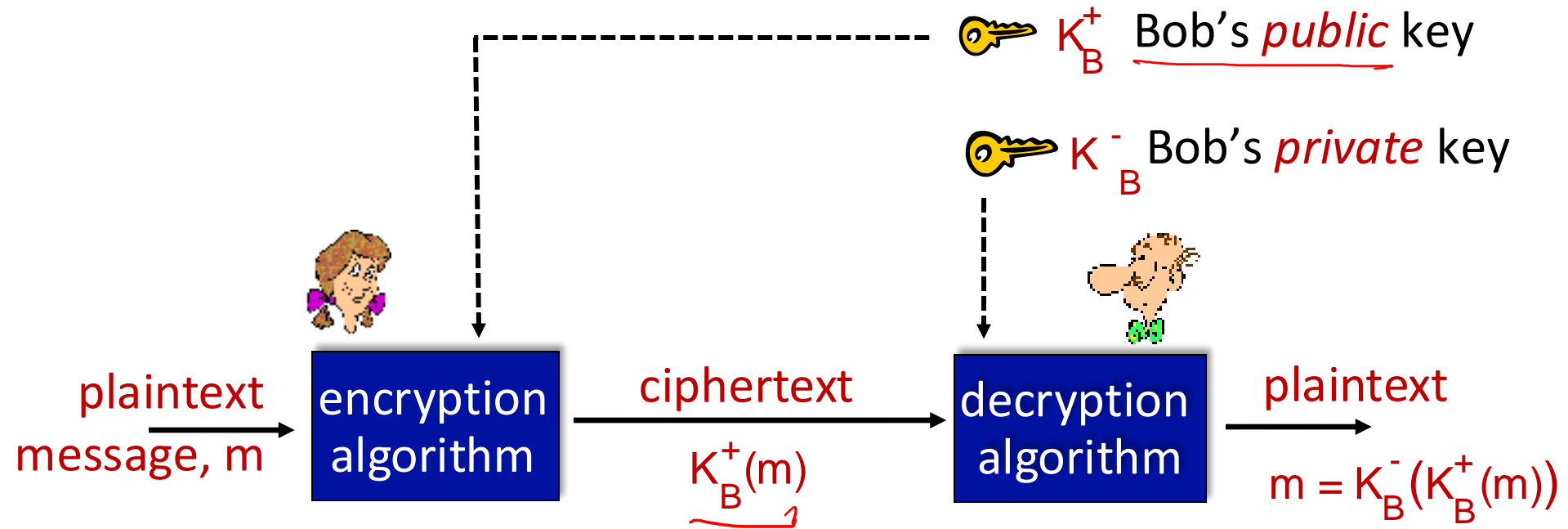$m(i) \oplus c(i-1) \quad \forall \; i > 1$

$m(1) \oplus IV$

Cipher Block Chaining
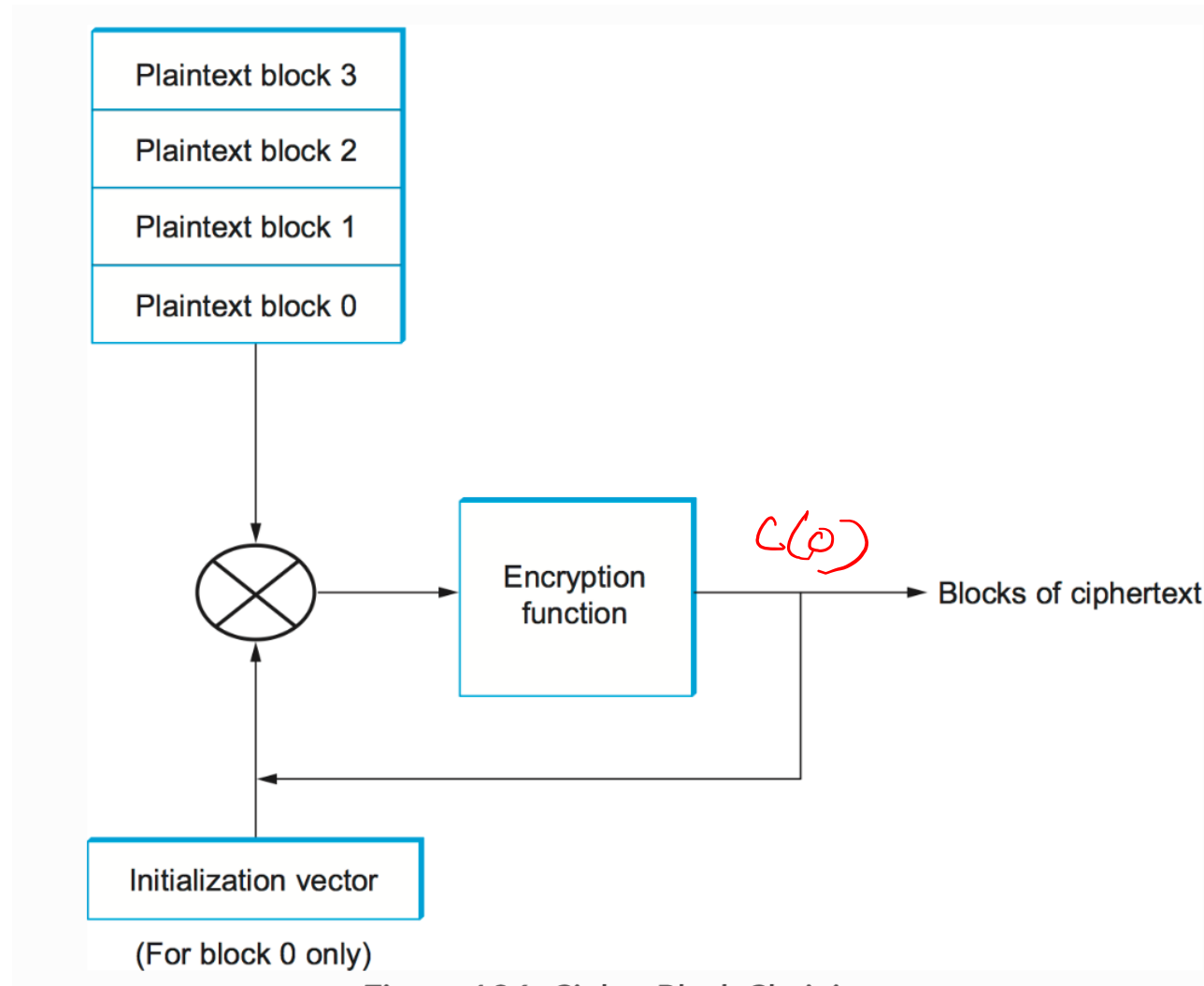
Symmetric key Cryptography

- Popular symmetric key algorithms: Data Encryption Standard (DES), Advanced Encryption Standard (AES)   *HTTPS / Wireless security*

  128 bit

- Symmetric key cryptography is generally faster

- Problem: how to share secret key

Public Key Cryptography

K_B^+ Bob's *public* key

K_B^- Bob's *private* key

plaintext message, m → encryption algorithm → ciphertext $K_B^+(m)$ → decryption algorithm → plaintext $m = K_B^-(K_B^+(m))$

Wow - public key cryptography revolutionized 2000-year-old (previously only symmetric key) cryptography!

- similar ideas emerged at roughly same time, independently in US and UK (classified)

Public key encryption algorithms

requirements:

① need $K_B^+(\cdot)$ and $K_B^-(\cdot)$ such that

$$K_B^-(K_B^+(m)) = m$$

Diffie-Hellman

② given public key K_B^+, it should be impossible to compute private key K_B^-

RSA: Rivest, Shamir, Adelson algorithm