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

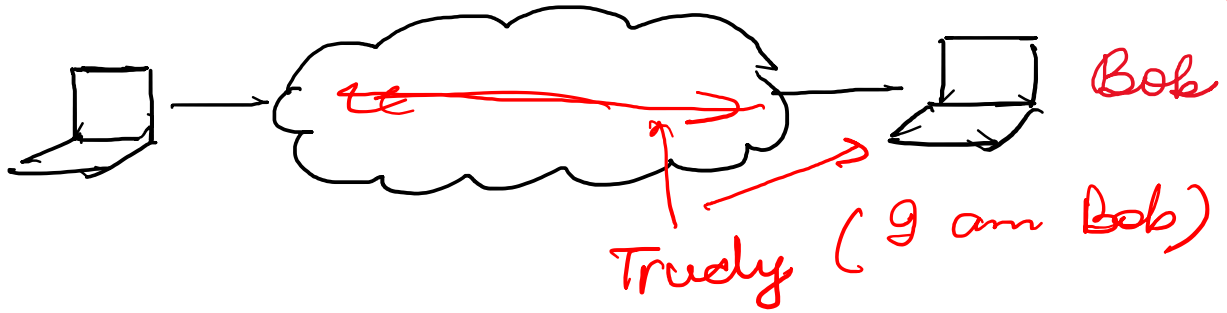
decentralization → security

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

Computer security is Network security

What kinds of network attacks?

① Phishing



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

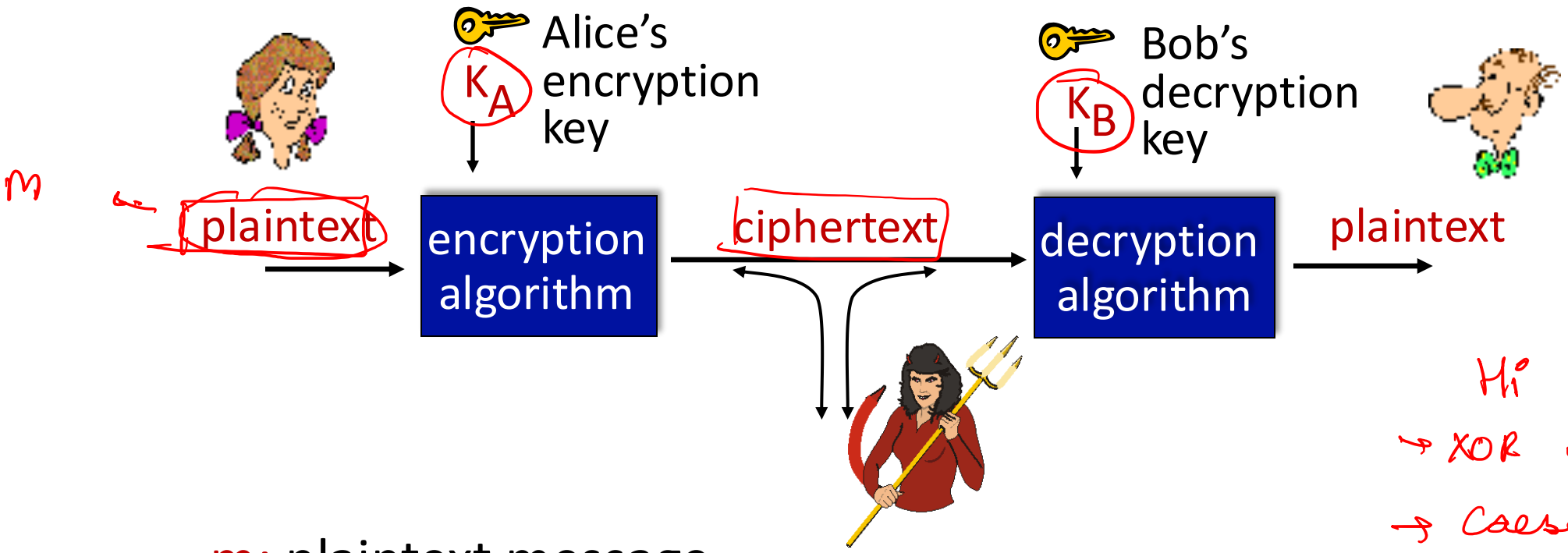
authentication: sender, receiver want to confirm identity of each other

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



Hi

→ XOR with a number

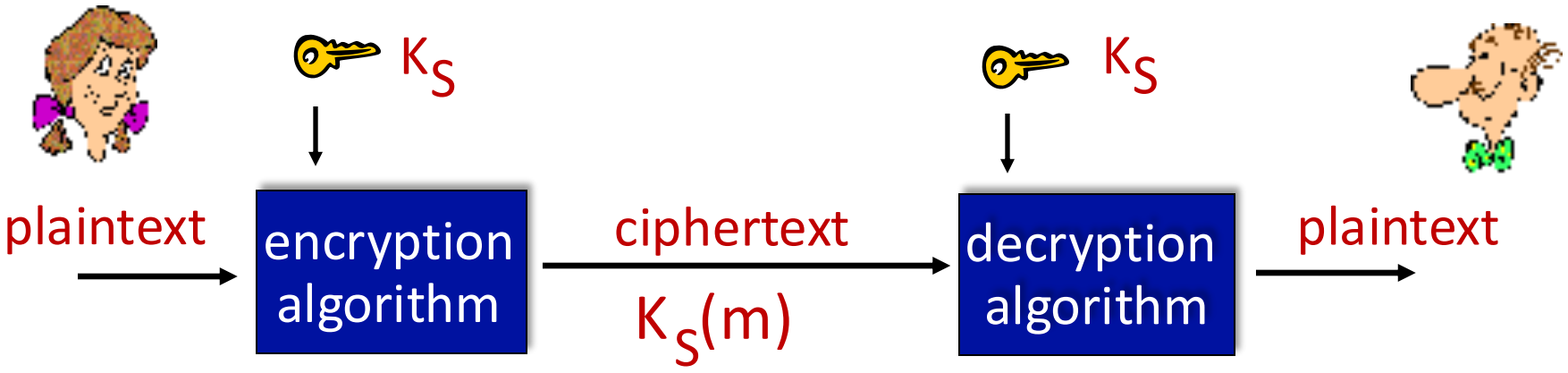
→ Caesar cipher

m: plaintext message

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

$m = K_B(K_A(m))$

Symmetric key cryptography



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
```

Ciphertext 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

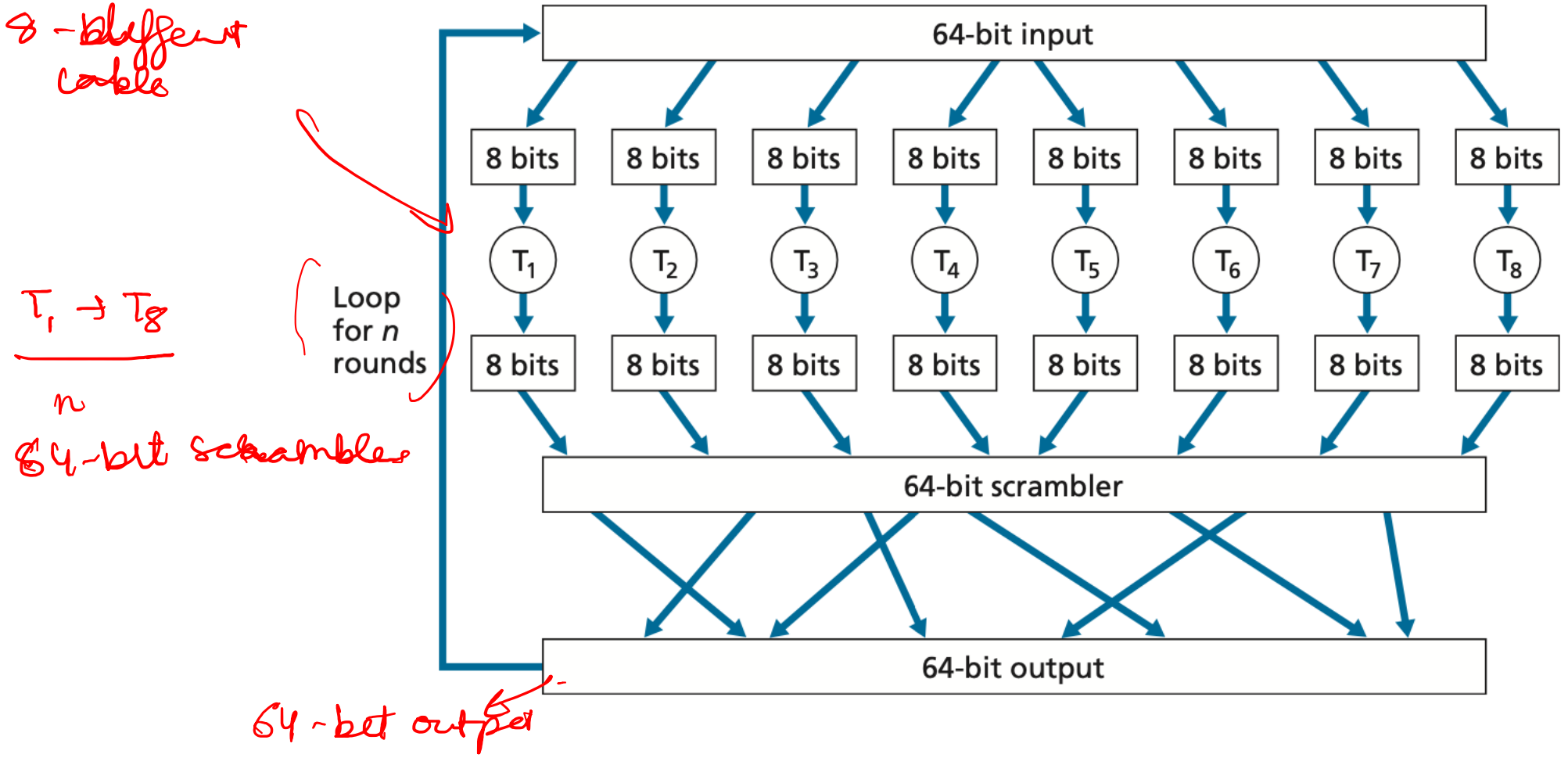
Block Cipher

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

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

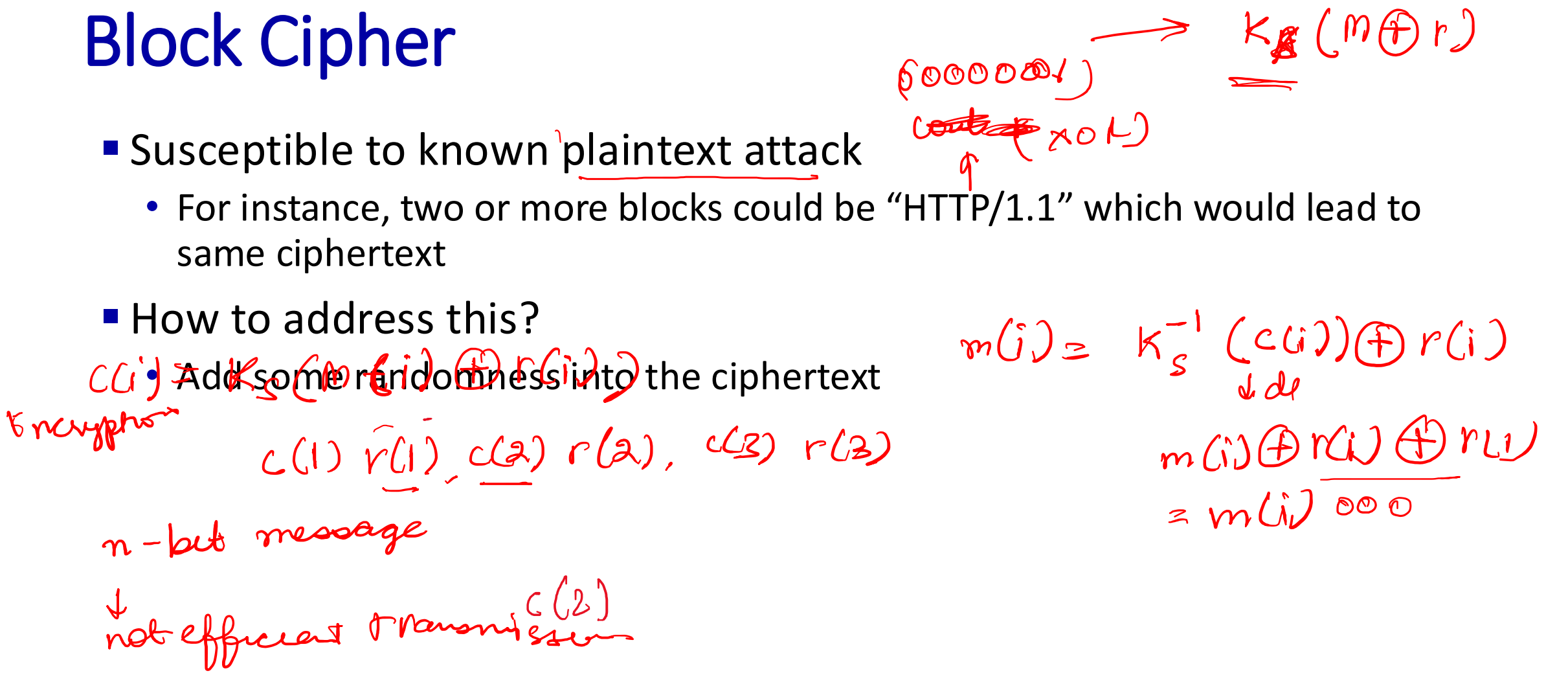
- How to do a brute-force attack on a 3-bit block cipher?
- What is the solution?
  - Use a large value of n, say 64-bit
  - The key becomes very large

64-bit Block Cipher Example

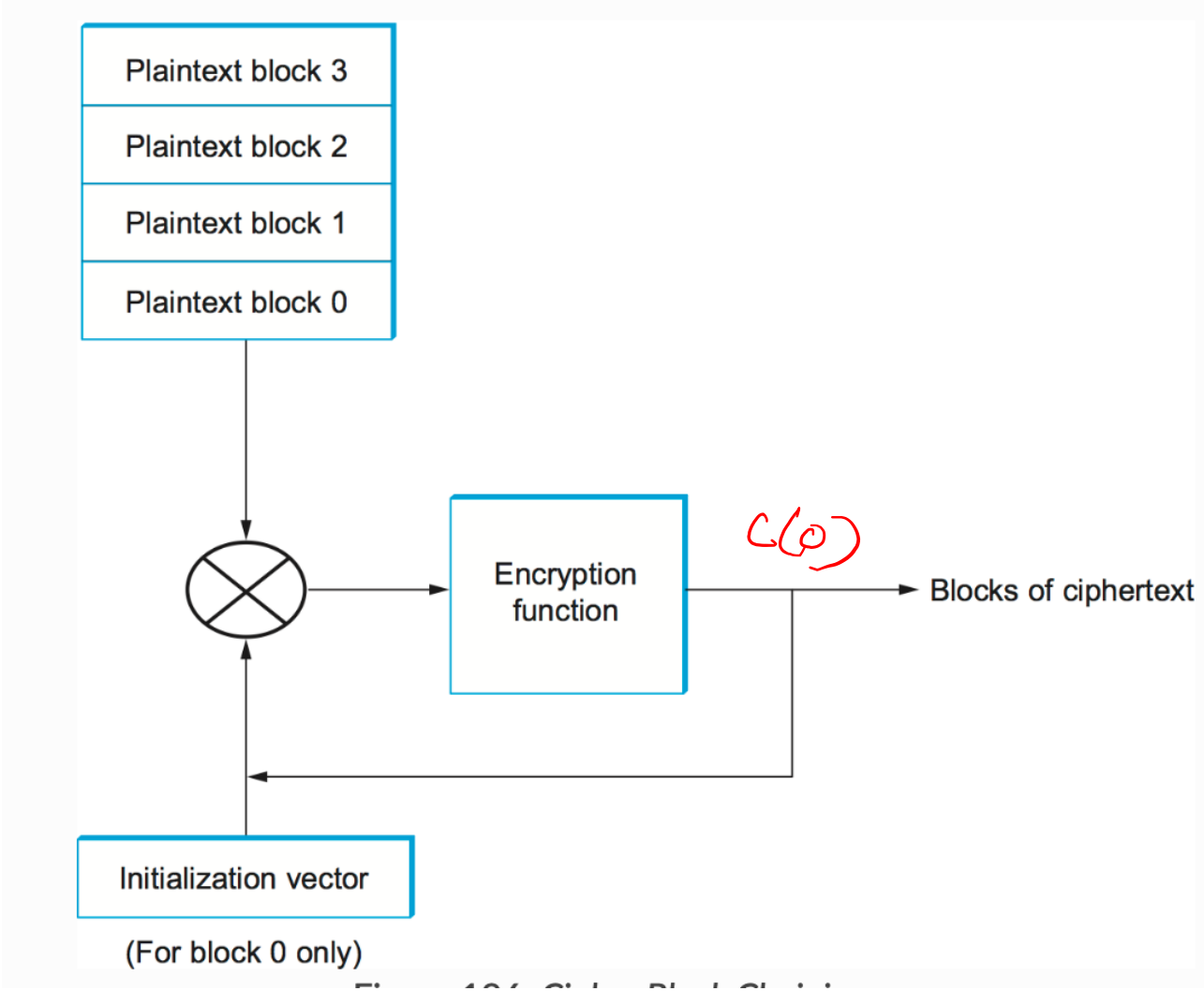


Block Cipher

- 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?
  - Add some randomness into the ciphertext



Cipher Block Chaining



Symmetric key Cryptography

- Popular symmetric key algorithms: Data Encryption Standard (DES), Advanced Encryption Standard (AES)

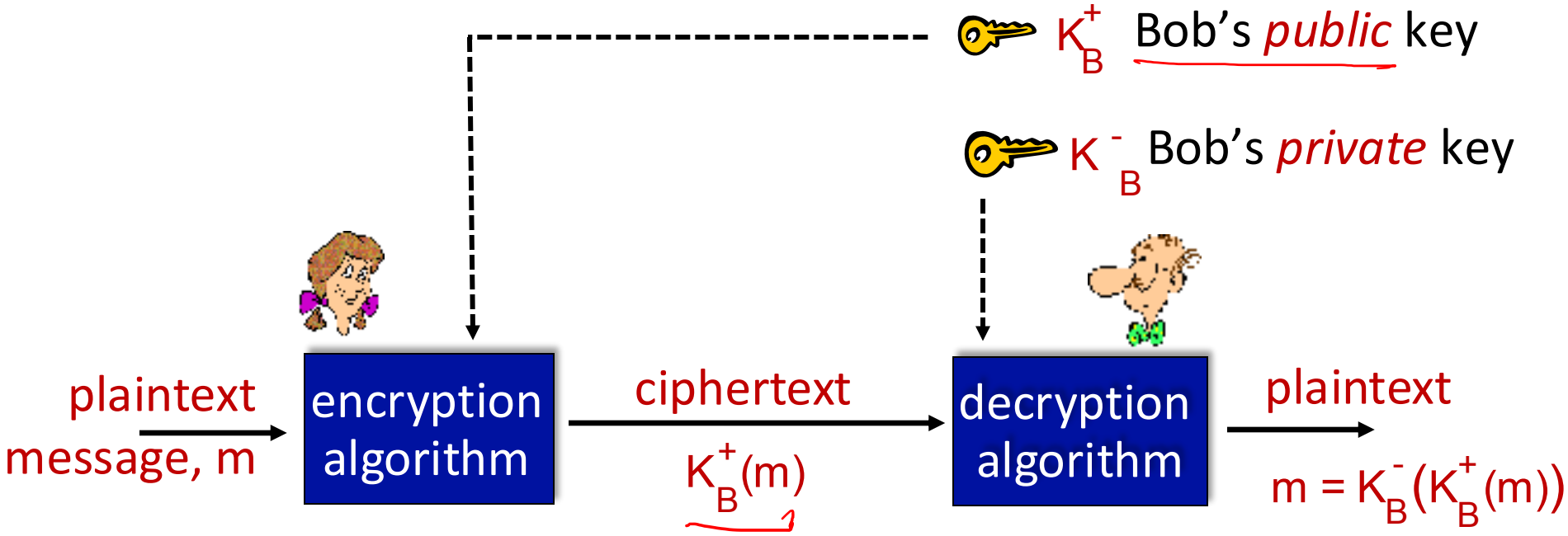
128 bit

HTTPS / Wireless security

- Symmetric key cryptography is generally faster

- Problem: how to share secret key

Public Key Cryptography



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