School of

Engineering and Computer Science

Te Kura Mātai Pūkaha, Pūrorohiko

CYBR 171 T1 2023

Ngā whakapūtanga o Te Haumaru rorohiko
Cybersecurity Fundamentals

Modern Cryptography I

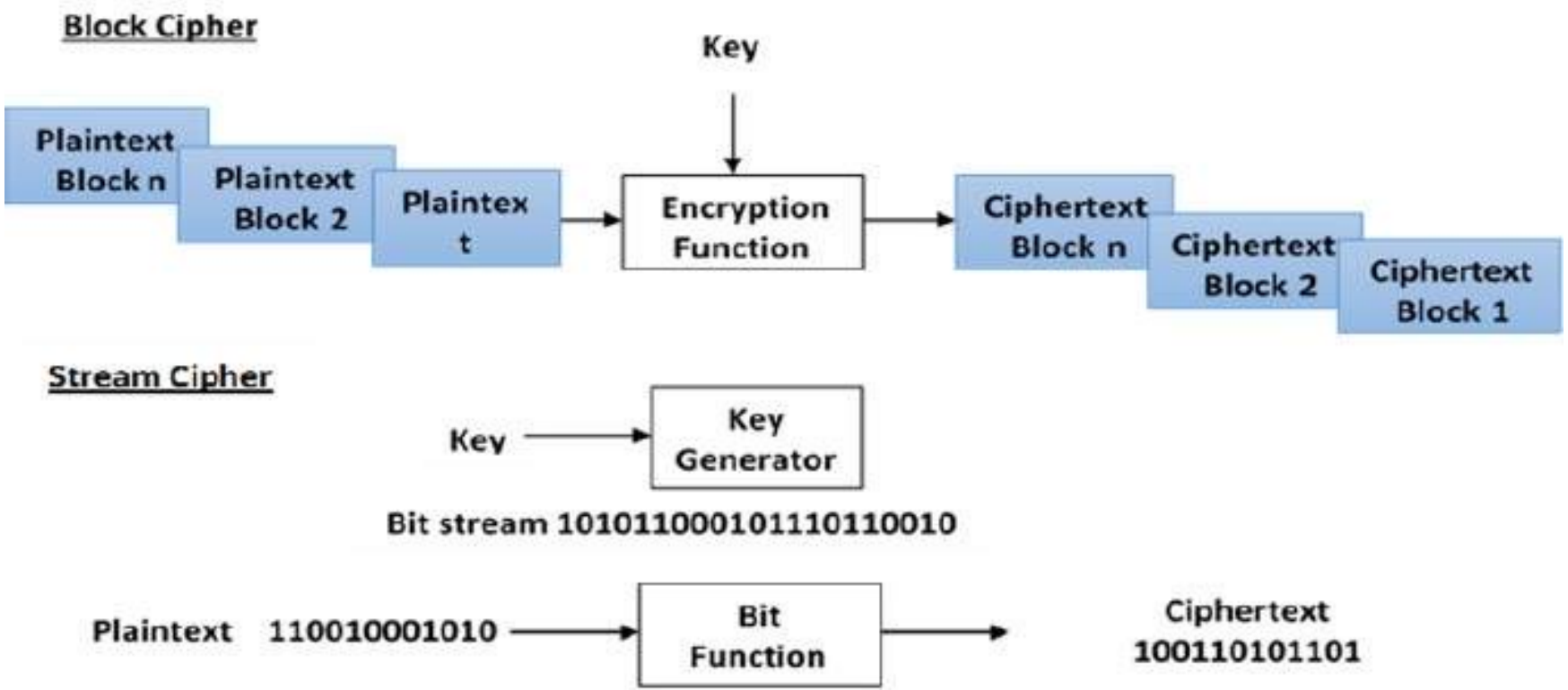
Learning objectives

- Role of **block size** in modern symmetric key ciphers.
- Relationship between key size and resistance to key exhaustion attacks.
- Difference between electronic code book (**ECB**) and cipher block chaining (**CBC**) modes in terms of security.

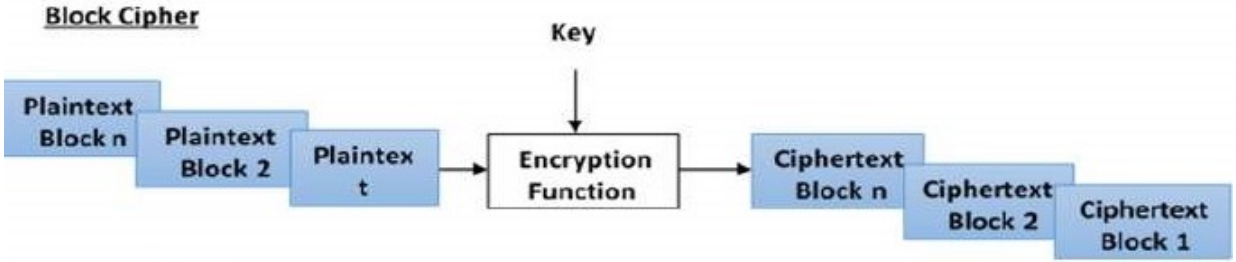
PART I:

Importance of *block* and *key* sizes

Block and stream ciphers



Modern Symmetric block ciphers



- DES, 3DES, AES and Blowfish examples of modern symmetric block ciphers.
- Takes a fixed-size block of plaintext bits and generates a block of ciphertext bits, generally of the same size.
- The size of a block is **fixed** for a given scheme.
- The choice of block size does not ***directly*** affect the strength of the encryption scheme, but smaller sizes can lead to the success of known plaintext attacks.

Padding in Block Cipher

- Block cipher length usually a multiple of 8 bits
  - Most processors handle data in bytes
  - Bytes are a multiple of 8 bits
  - UTF-8 characters are expressed as 8-bit values
- Most plaintexts are a multiple of 8 bits, for example:
  - DES uses blocks of size 64 bits.
  - Imagine a 150-bit plaintext.
  - Two 64-bit blocks plus one block of 22 bits.
  - Final block needs 42 redundant bits to make a complete block.
- Process of adding redundant bits called “padding”, too much padding is inefficient.

Key *size*, key *length* and key *space*

- Key size and key length refer to the **number of bits in a key**.
- Key space is the **set of all possible keys** that can be used.
- Although the cipher algorithms should be assumed to be known, the security of the system depends on the **secrecy of the key**.
- Must resistant to a type of brute force attack called an ***exhaustive key search*** where the attackers try all possible combinations of a key until they find the correct one.
- Dependent upon the **speed** of decryption and the **number** of keys that must be tried.
- The number of possible keys in the key space = $\mathbf{2^m}$ where **m** is the number of bits in the key.

Resistance to Key Exhaustion Attacks

Key size (bits)	Cipher	Number of Alternative Keys	Time Required at 10^9 decryptions/s	Time Required at 10^{13} decryptions/s
56	DES	$2^{56} \approx 7.2 \quad 10^{16}$	2^{55} ns = 1.125 years	1 hour
128	AES	$2^{128} \approx 3.4 \quad 10^{38}$	2^{127} ns = 5.3 10^{21} years	5.3 10^{17} years
168	Triple DES	$2^{168} \approx 3.7 \quad 10^{50}$	2^{167} ns = 5.8 10^{33} years	5.8 10^{29} years
192	AES	$2^{192} \approx 6.3 \quad 10^{57}$	2^{191} ns = 9.8 10^{40} years	9.8 10^{36} years
256	AES	$2^{256} \approx 1.2 \quad 10^{77}$	2^{255} ns = 1.8 10^{60} years	1.8 10^{56} years

Average Time Required for Key Exhaustion Attacks

PART II:

Electronic Code Book Mode of operation

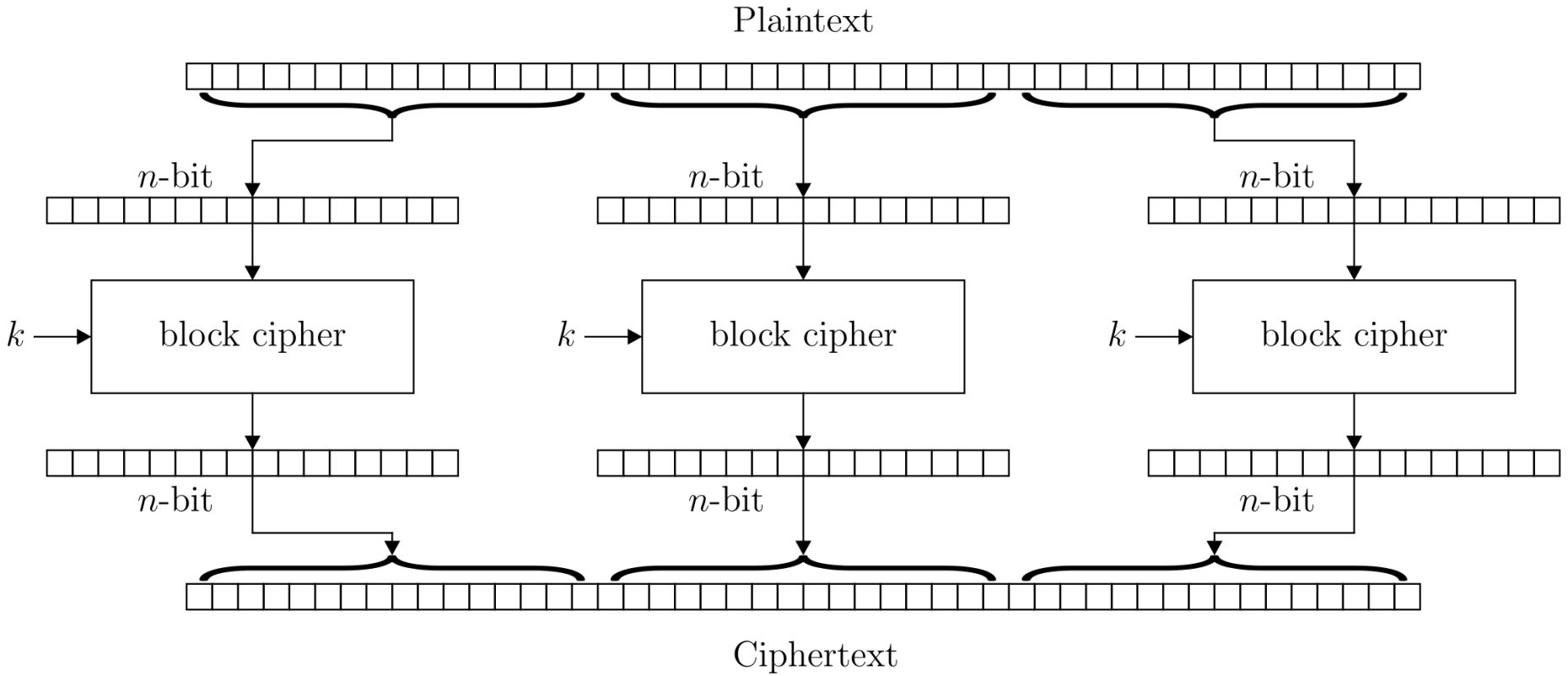
Modes of Operation

- Block ciphers have different **modes** of operation for different types of tasks.
- Several basic types – focus here on electronic code book (**ECB**) and cipher block chaining (**CBC**).
- ECB is *obsolete* but occasionally still used.
- When it is, it leads to problems ….
  - Adobe data breach in 2013
  - 38,000,000 passwords exposed
    https://nakedsecurity.sophos.com/2013/11/04/anatomy-of-a-password-disaster-adobes-giant-sized-cryptographic-blunder/

Electronic Code Book (ECB)

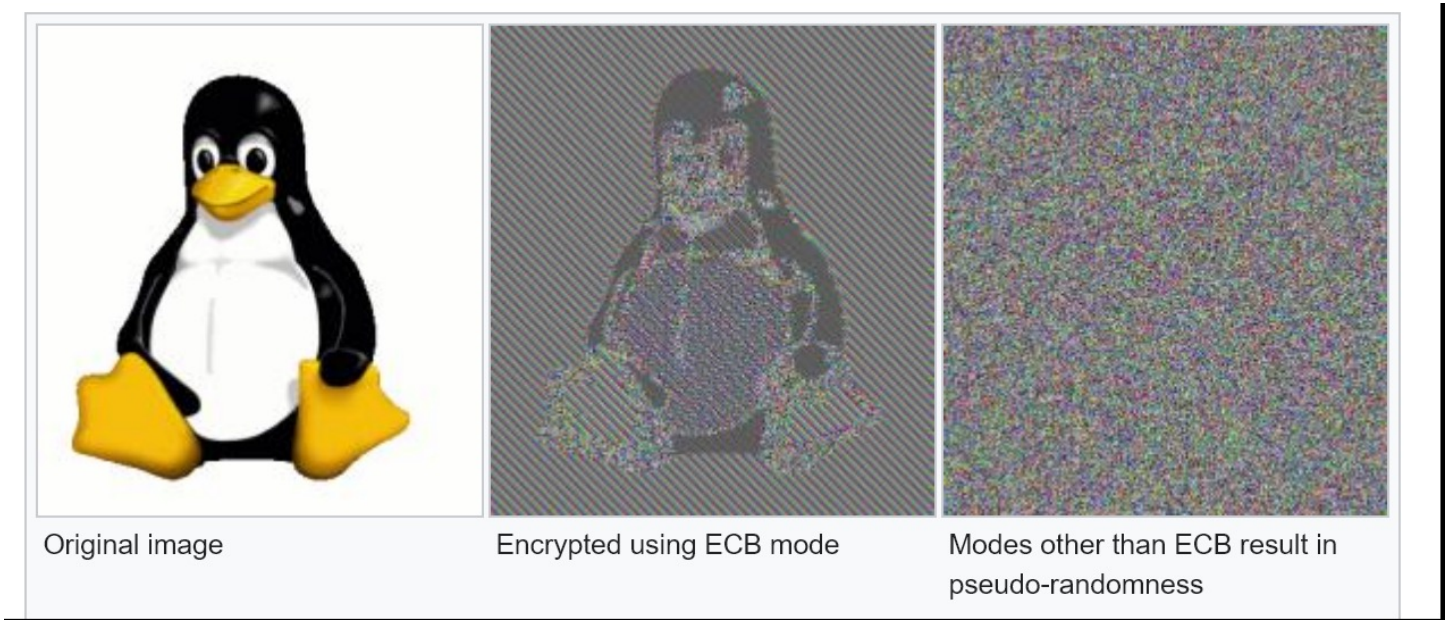
- Electronic code book has each block of plaintext encrypted **separately** using the key.
- Problem with this is that **identical plaintext** blocks result in **identical ciphertexts**.
- Lacks the property of **diffusion**, too easy to see the relationship between plaintext and ciphertext.
- What we want is a small change in the plaintext to cause a big change in the ciphertext.
- ECB does not hide data patterns very well and not recommended.

Electronic Code Book (cont.)



Electronic Code Book (cont.)

- This is a classic visualization showing how data patterns are revealed unless randomness added.



Code Book Attack

- Example of known **plaintext attack**
  - Attacker knows at least one sample both the plaintext and ciphertext
  - Builds a "**code book**" table
  - Ciphertext block corresponds to which plaintext block
  - Information can help with guessing whole plaintext
- Consider an 8-bit sized block i.e. one UTF-8 character.
- Assume attacker can able to get or guess some of the plaintext matching the ciphertext and builds a code book.

Example: Code Book Attack

- Code book:

Plaintext	Ciphertext
A	E
C	K
D	L
W	O

- Attacker sees message
  - ERREKCERLEOI
- Attacker applies partial code book
  - A??ACKA?DAW?
- Attacker makes an educated guess to decode the rest

PART III:

Cipher Block Chain Mode of operation

Defending Against Code Book Attack

- Attacker needs to observe $2^{blocksize/2}$ ciphertexts before entries are repeated.
  - Choose **larger block sizes**, this is why we have a 64-bit minimum.
  - **Change the key** on a regular basis and choose a different one every time.

- Use a **different mode** of operation that incorporates some randomness – enter the Cipher Block Chaining (**CBC**) mode.

Exclusive OR (XOR)

- Before we look at CBC, need to introduce one of the building blocks – exclusive OR (XOR).
- Operator on binary data, takes two bits (A and B) and returns **true** (1) if both bits are opposites and otherwise returns **false**.
- XOR can be used to implement a one time pad using a stream of bits as the key.

Input		Output
A	B	A xor B
0	0	0
0	1	1
1	0	1
1	1	0

Exclusive OR (XOR) - 1

- Example: encrypt “hi”.
- Setup our XOR crypto cipher
  - Convert each character from UTF-8 to binary bits (https://onlineutf8tools.com/convert-utf8-to-binary)
    - Two characters ***h*** and ***I***
    - **01101000 01101001**
  - Create a random key of the same length
    - 01010010 01000101

Exclusive OR (XOR) - 2

- Example: **encrypt** “hi”.
- Encryption
  - XOR every bit of the plaintext with key
    01101000 01101001 ("**hi**")
    XOR
    01010010 01000101 (**secret key**)
    =
    00111010 00101100 (encrypted message “**:,**”)

Exclusive OR (XOR) - 3

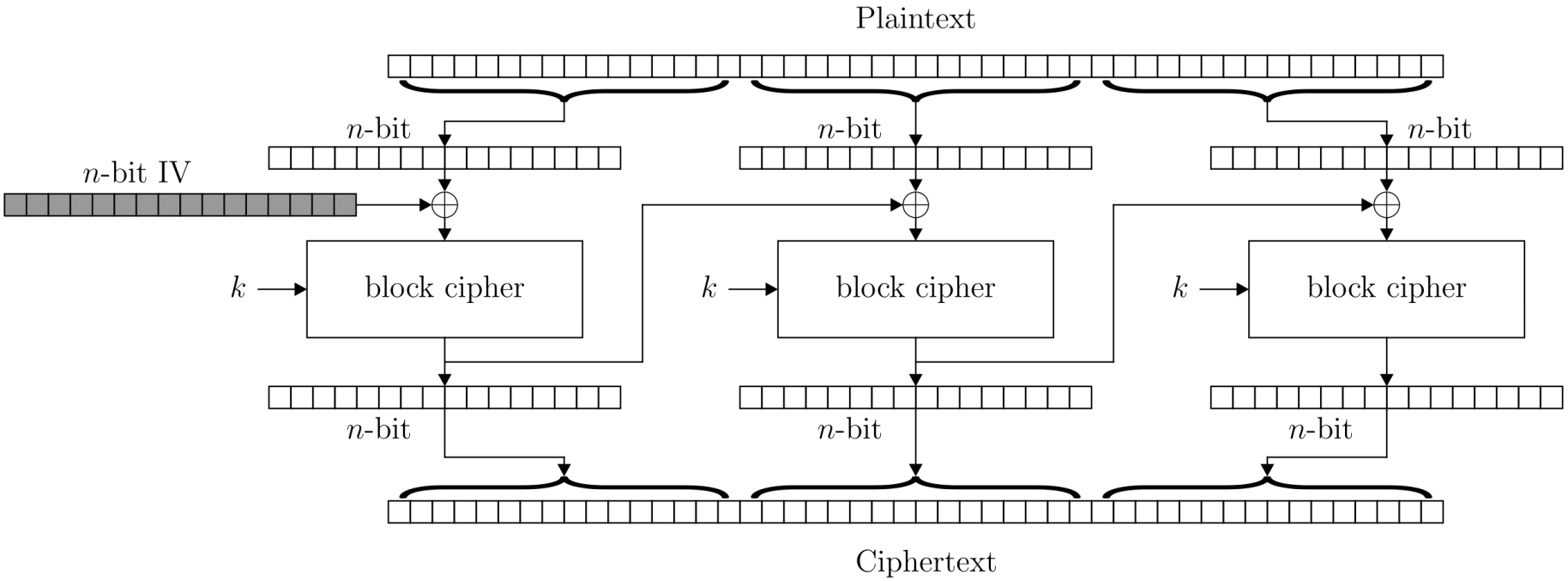
- Example: decrypt “:,”.
- **Decryption**
  - XOR every bit of the ciphertext with key

00111010 00101100 (encrypted message “**:,**”)
XOR
01010010 01000101 (**secret key**)
=
01101000 01101001 ("hi")

Cipher Block Chaining (CBC)

- We want to add apparent **randomness** to hide the patterns in the data.
- Cipher block chaining (CBC) makes each ciphertext block depend upon the value of the **previous ciphertext block**.
- Achieved in two ways:
  - Use of XOR function
  - Use of initialization vector (IV)

Cipher Block Chaining (cont.)



IV Must be *Random*

- The initialization vector (IV) is combined with the plaintext adds randomness.
- Chaining between the blocks causes the randomness to diffuse through all of the ciphertext.
- Use a different IV each time and making it as random as possible is very important for good randomness.
- **You don't have to keep the IV secret** as long as **the key is kept secret**.

What's up next

- Labs ... You still have 10 days to complete Lab 1.

- Next week we will look at
  - the key distribution problem,
  - asymmetric cryptosystems, and
  - authentication