SMU
SINGAPORE MANAGEMENT UNIVERSITY

School of
Computing and
Information Systems

CS440
Foundations of Cybersecurity

Symmetric Key Encryption

Overview

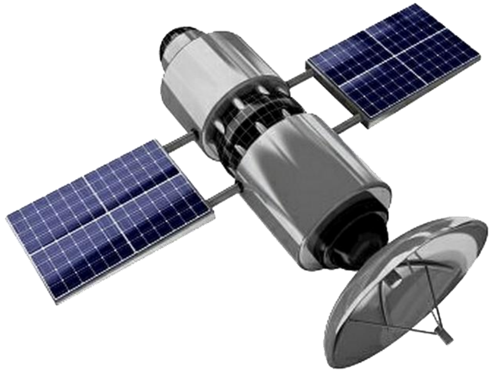
Content

- Why do we need encryption?
- Rationale behind encryption ciphers
- One-time pad
- Block cipher
  - AES algorithm
  - Encryption modes: ECB, CBC, CTR
- Cryptanalysis

After this module, you should be able to

- explain the rationale behind encryption and various types of encryption methods
- explain what is cryptanalysis
- use symmetric key ciphers

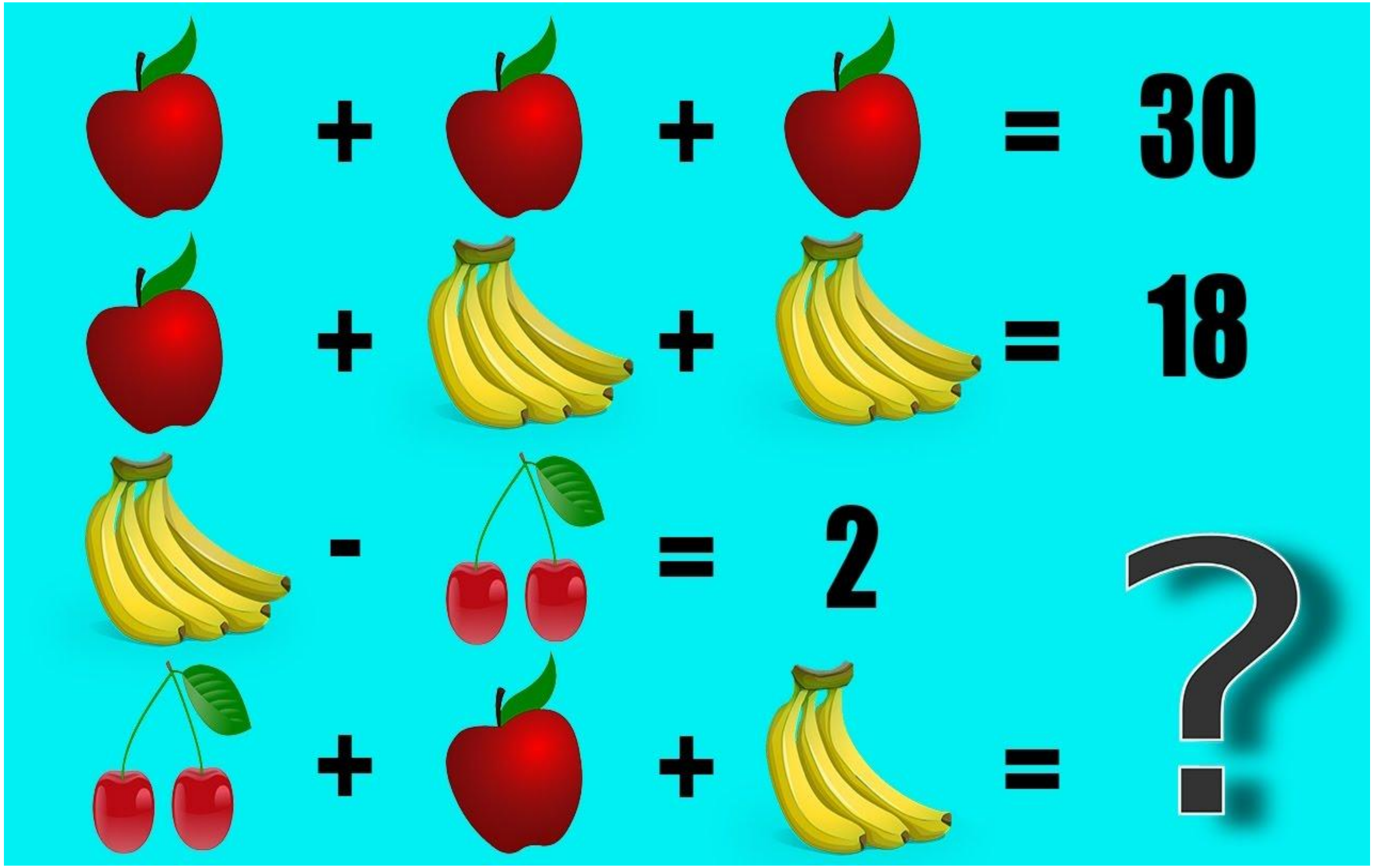
Motivation: Confidentiality is crucial



Motivation

- The sender has no (physical) control of communication data once they leave the platform.
  - No exclusive communication channel

Cannot prevent the adversary from accessing the data


+
+
= 30
+
+
= 18
-
= 2
+
+
=
?

Rationale of Encryption

- Information semantics and representation are different.
  - We recognize semantics from representations by using patterns.
  - Different ways of representations have different patterns.
- IF the adversary cannot find patterns, it gets a hard time to extract semantics from a given representation.

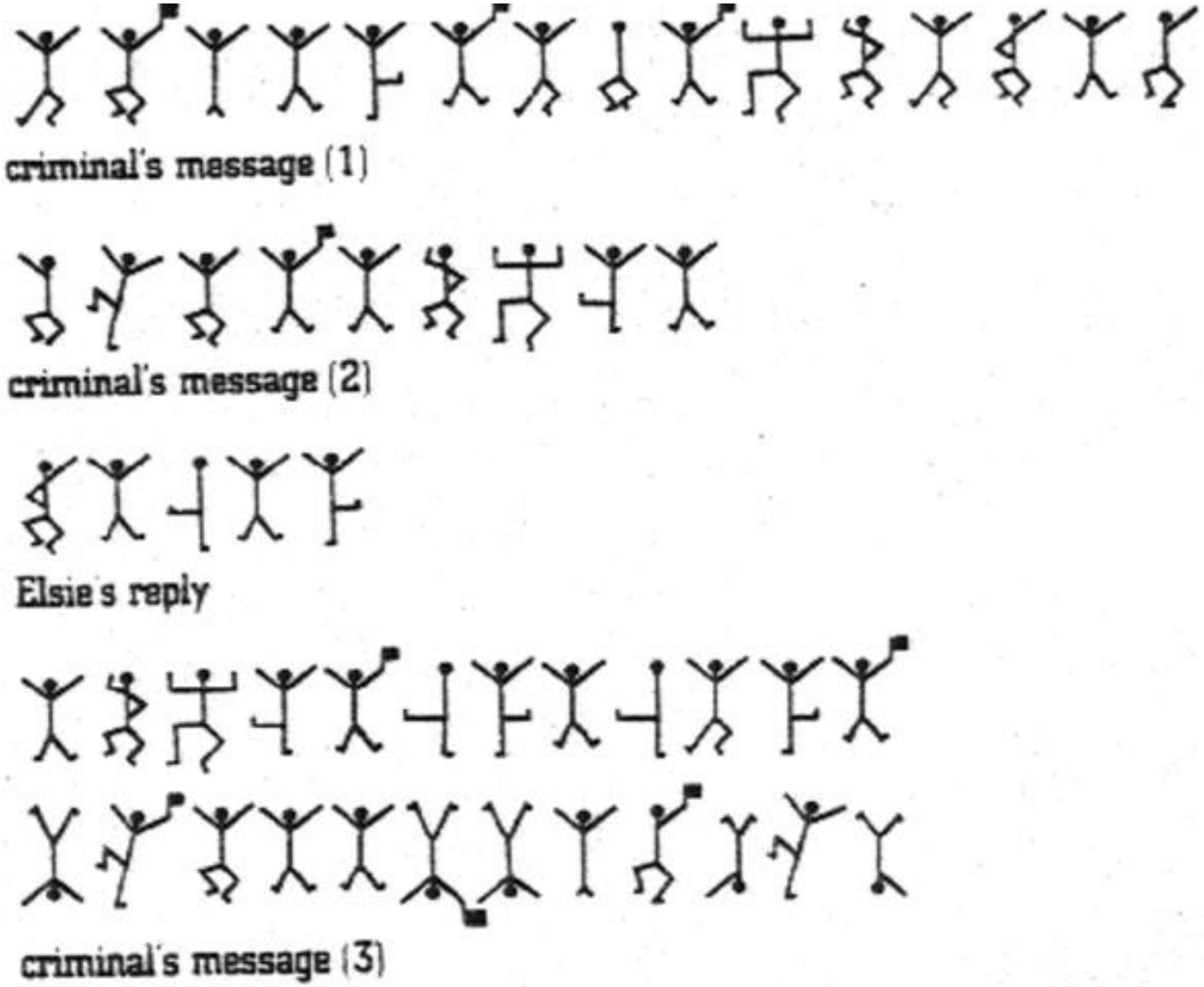
“Two“, “2“, “贰“ , “два“, “dos“, “dua“, “ezimbil”

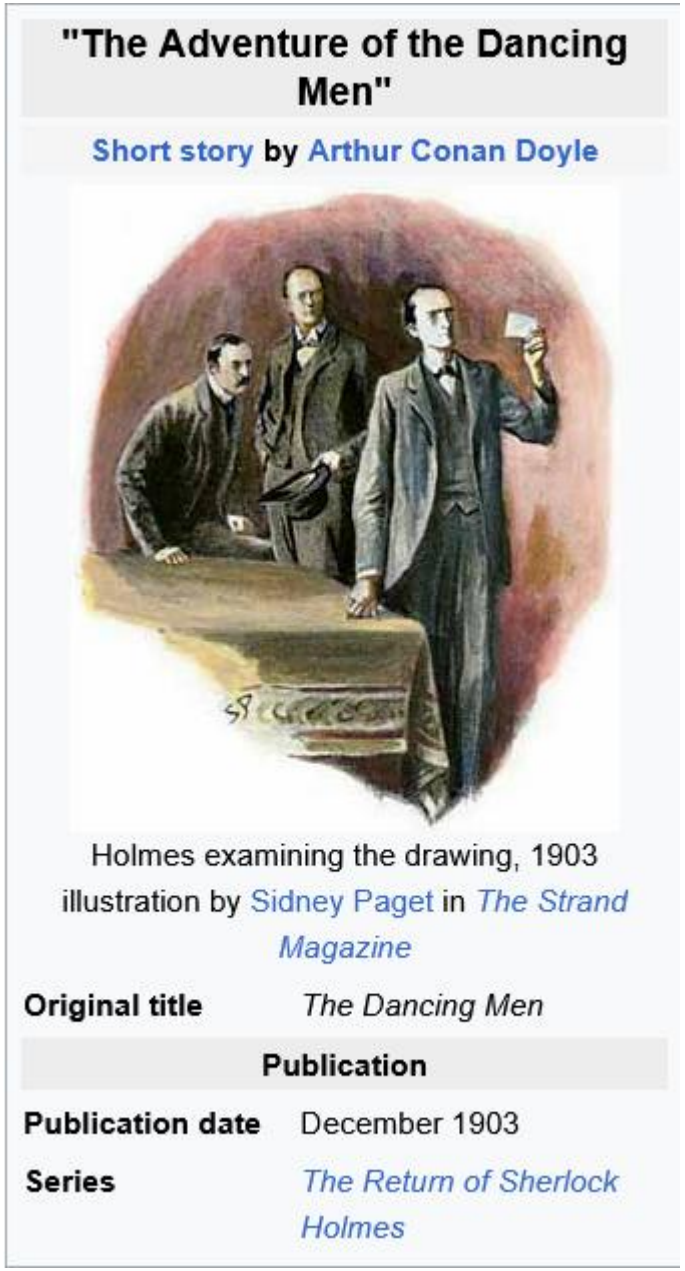
Rationale of Encryption

- GOAL: to make the ciphertext without patterns recognizable to the adversary.
  - Ideally, the ciphertext is random, i.e., no pattern!
- Approach 1: substitution
  - Substitution can be made on the symbol set or on a fixed sized group of symbols.
  - E.g., “A” → “132”, “B”→ “888 ”, ...
- Approach 2: shuffle or permutation
  - Rearrange the symbols to different positions in the ciphertext.

But, we need a way to get back the original data!!

Substitution – an example




"The Adventure of the Dancing Men"

Short story by Arthur Conan Doyle

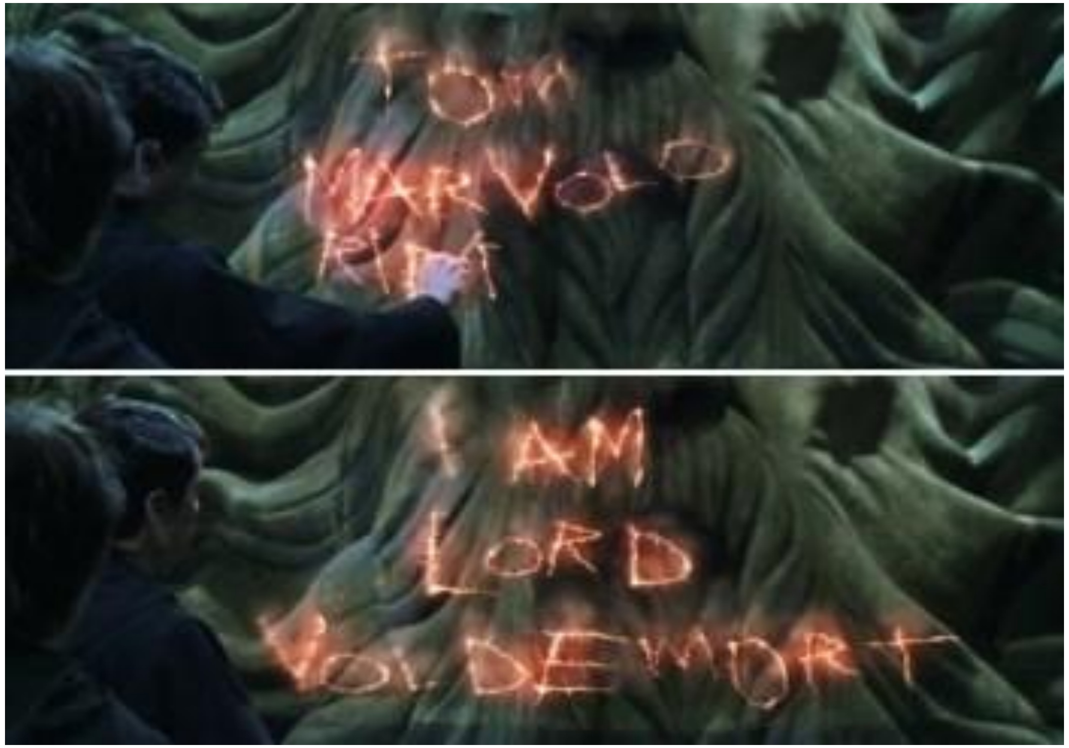
Holmes examining the drawing, 1903 illustration by Sidney Paget in *The Strand Magazine*

Original title	*The Dancing Men*
Publication	
Publication date	December 1903
Series	*The Return of Sherlock Holmes*

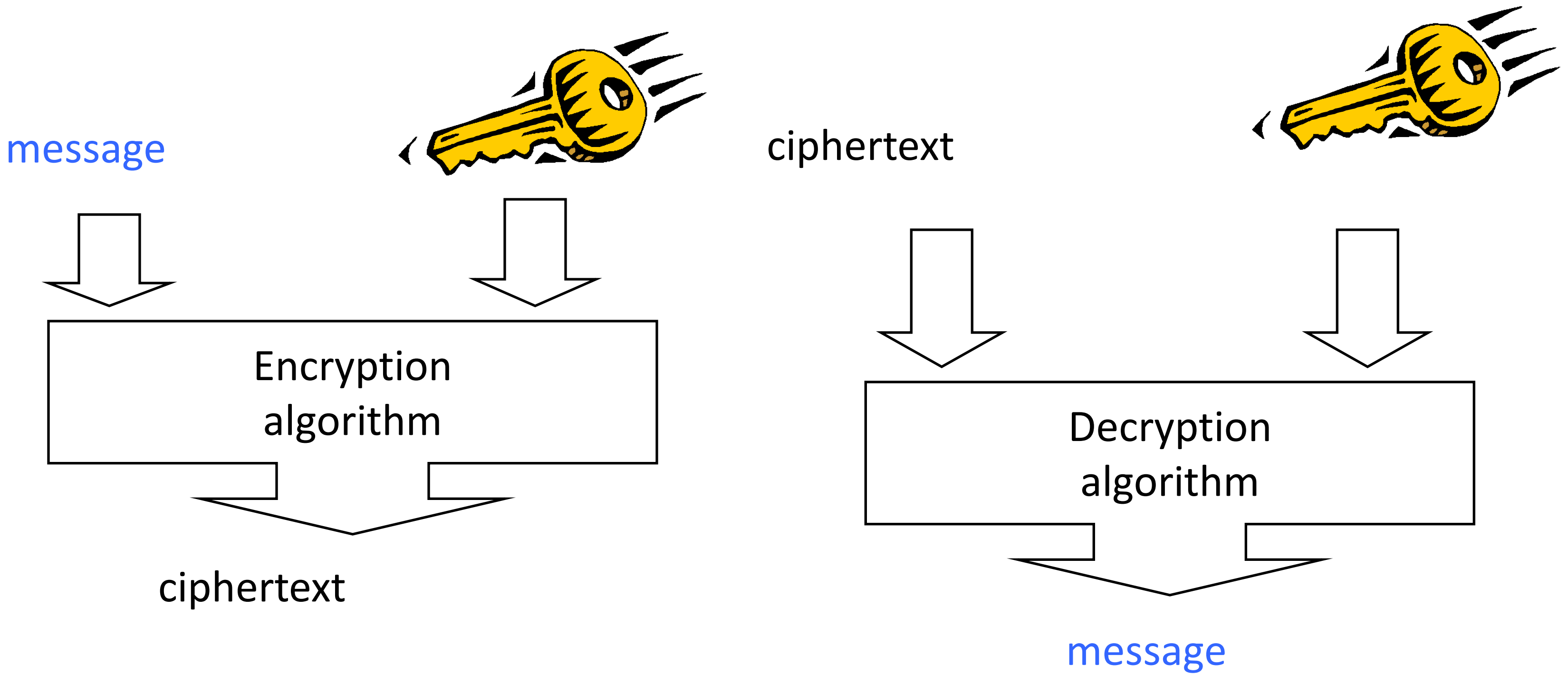
Permutation – an example

Harry Potter and the Chamber of Secrets (2002)

TOM MARVOLO RIDDLE

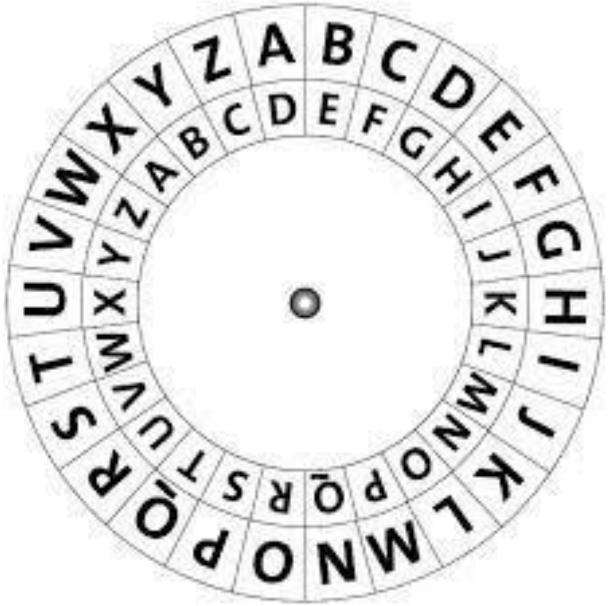


Encryption/Decryption



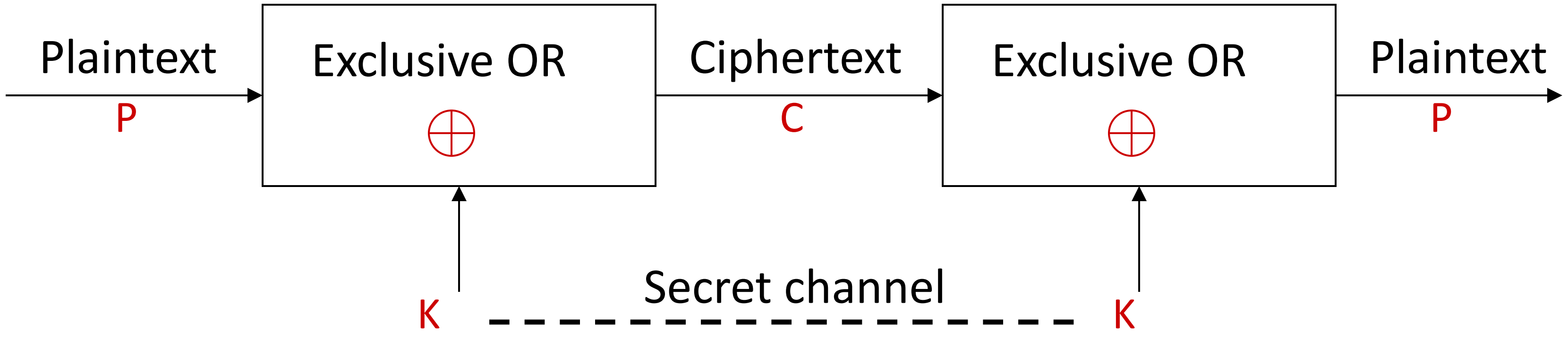
Caesar Cipher

- Julius Caesar 2000 years ago
- Substitution: a letter is replaced by another letter (the original Caesar cipher is a shift cipher)


A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

- Demo in CrypTool Online

One-Time Pad (a.k.a. Vernam Cipher)



- P: a bitstring (aka binary string) representation of the plaintext (i.e. message)
- K: a random bitstring with the same length as the plaintext
- Every encryption uses a new freshly chosen key.

One-time pad

- An example of Vernam Cipher
  - Alice:

    P: 100 010 111 011 110 001…

    K: 010 011 101 101 010 111…

    C: 110 001 010 110 100 110…
  - Bob:

    C: 110 001 010 110 100 110…

    K: 010 011 101 101 010 111…

    P: 100 010 111 011 110 001…

Exclusive OR operations

$1 \oplus 0 = 1;\ \ 0 \oplus 1=1$

$0 \oplus 0 =0;\ \ 1 \oplus 1=0$

Perfectly/Unconditionally secure: unbreakable even with infinite amount of computational power, assuming the attacker has no knowledge about the key

Impractical: The need for synchronization & the need for an unlimited number of keys

Message in Binary

Dec	Hex	Binary	Symbol
65	41	01000001	A
66	42	01000010	B
67	43	01000011	C
68	44	01000100	D
69	45	01000101	E
70	46	01000110	F
71	47	01000111	G
72	?	?	H
73	?	?	I
74	?	?	J

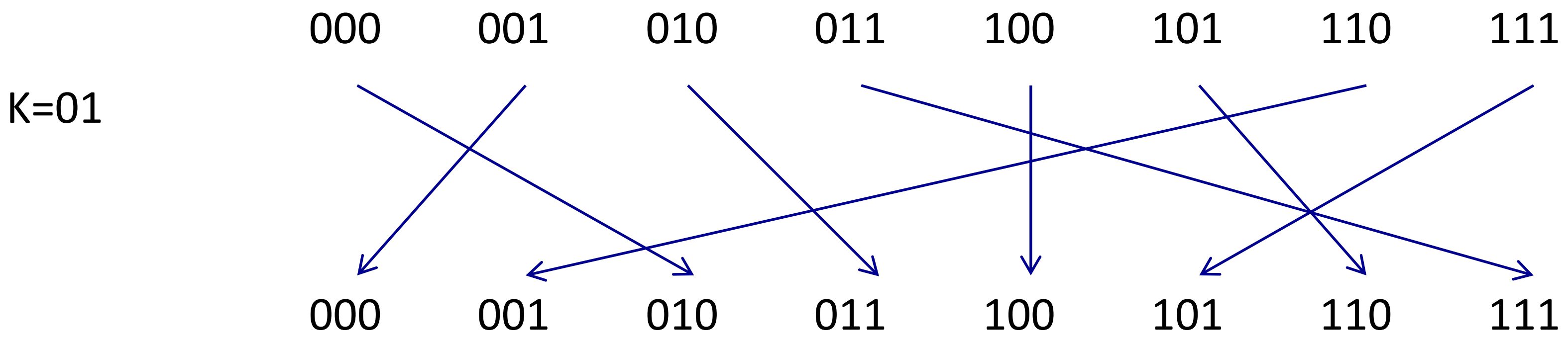
ASCII Character to Binary Conversion

- https://www.youtube.com/watch?v=5aJKKgSEUnY

Block Ciphers

- Block Ciphers are for binary messages.
  - Text messages are also binaries when they are processed by computers.
- A **block** is a fixed number of consecutive bits in the message as
  - Intuitively, blocks are like words in our dictionary, except that blocks are of the same length.
- To encrypt a message, make substitutions upon each block in the message with another block chosen from the block domain (i.e., the set of all possible blocks.)
- The cipher algorithm and the key jointly define the mapping between plaintext blocks and ciphertext blocks.

A Toy Example (my invention!)



Block size: 3 bits

Key size: 2 bits

K=

Key Challenge: How can software derive the mapping according to a given key?

plaintext

000110110011010001

K=01

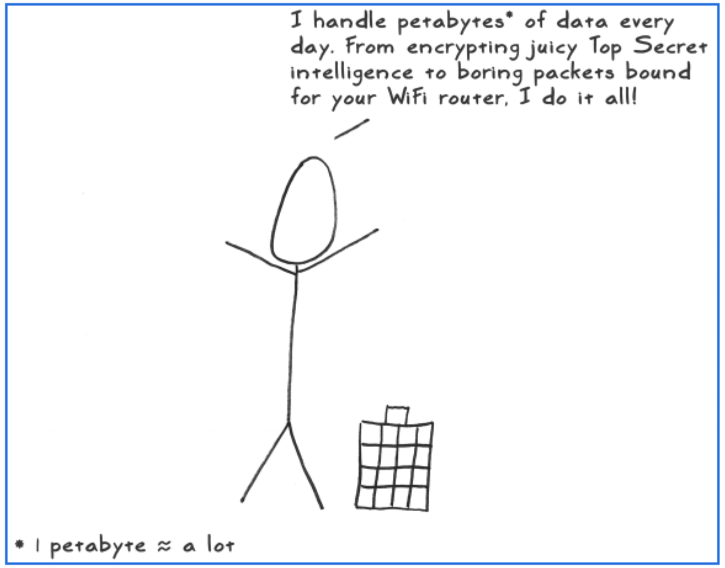
ciphertext

010001001111011000

Advanced Encryption Standard (AES)

- Advanced Encryption Standard (AES)
- **AES key size**: 128, 192, 256 bits
- **AES block size**: 128 bits
- Unclassified, publicly disclosed, royalty-free
- Internal steps of AES (not required)
- Demo in CrypTool Online
  - https://legacy.cryptool.org/en/cto/aes-animation

A very interesting illustration of AES

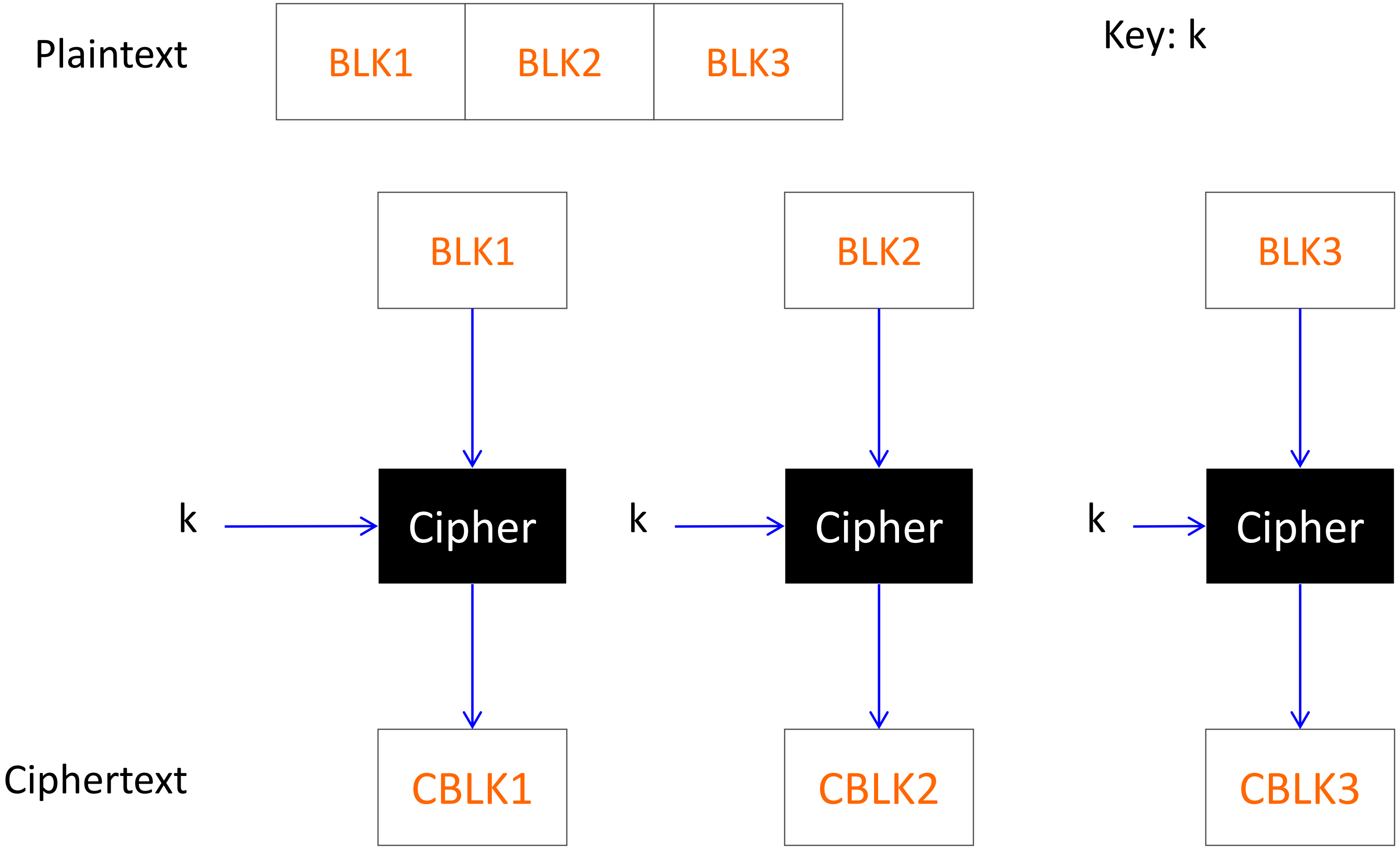

I handle petabytes* of data every day. From encrypting juicy Top Secret intelligence to boring packets bound for your WiFi router, I do it all!
* 1 petabyte ≈ a lot

Modes of Encryption

- AES is a block cipher. The algorithm and the specific key determine a mapping between blocks.
- Symmetric key encryption: use a block cipher to encrypt a message consisting of **multiple blocks**.
  - Should the relation among blocks be considered?
- **Three modes** to encrypt messages.
  - ECB: Electronic Code Book
  - CBC: Cipher Block Chaining
  - CTR: Counter

The block cipher key only specifies the plaintext-ciphertext block mapping. It does not deal with the relation among blocks, i.e. mode of encryption.

ECB Mode


Plaintext
BLK1
BLK2
BLK3
Key: k
BLK1
BLK2
BLK3
k
Cipher
k
Cipher
k
Cipher
Ciphertext
CBLK1
CBLK2
CBLK3

CBC Mode

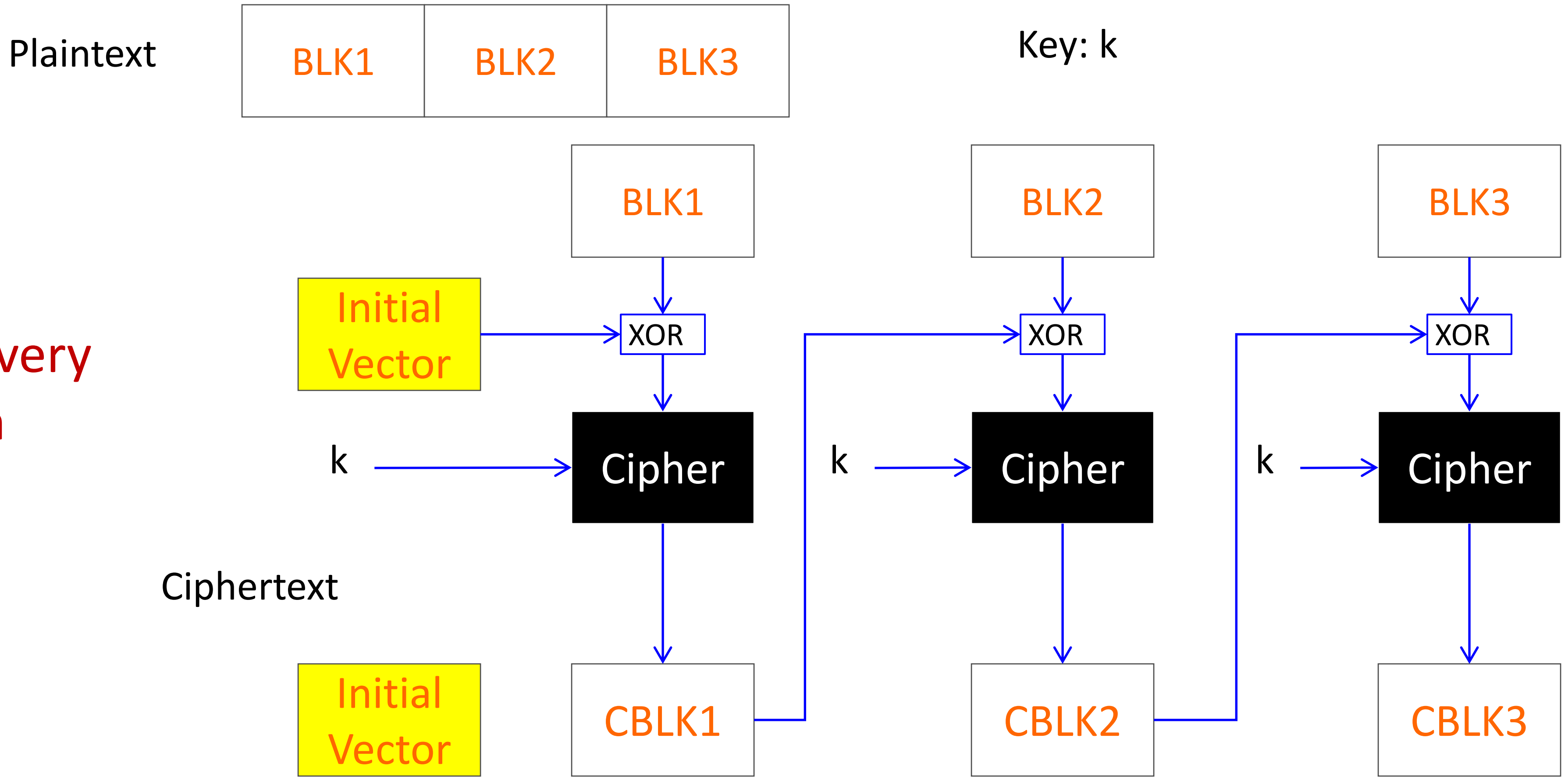
- Before applying AES upon the plaintext, a random block is chosen as the Initial Vector (IV).
  - The length of IV is the same as the block size
- IV needs NOT be a secret.
- IV is considered as the first block in the ciphertext.
- The purpose of IV:
  - to introduce randomness into the encryption process

CBC Mode

- The first block has index 1
- Encryption
  - $C_i = Enc_k(P_i \oplus C_{i-1})$, $C_0 = IV$
- Decryption
  - $P_i = Dec_k(C_i) \oplus C_{i-1}$, $C_0 = IV$
- Encryption must be sequential and decryption can be parallel.

CBC Mode Encryption

Initial Vector (IV) is freshly chosen for every plaintext encryption



$\mathrm{CBLK}_i = \mathbf{Cipher}_K(\ \mathrm{BLK}_i \oplus \mathrm{CBLK}_{i-1}\ ),\ \mathrm{CBLK}_0 = \mathrm{IV}$

CBC – A toy example (encryption)

- Let us consider a toy 3-bit block cipher with the following mapping:

Plaintext Block	000	001	010	011	100	101	110	111
Ciphertext Block	111	110	011	100	001	000	101	010

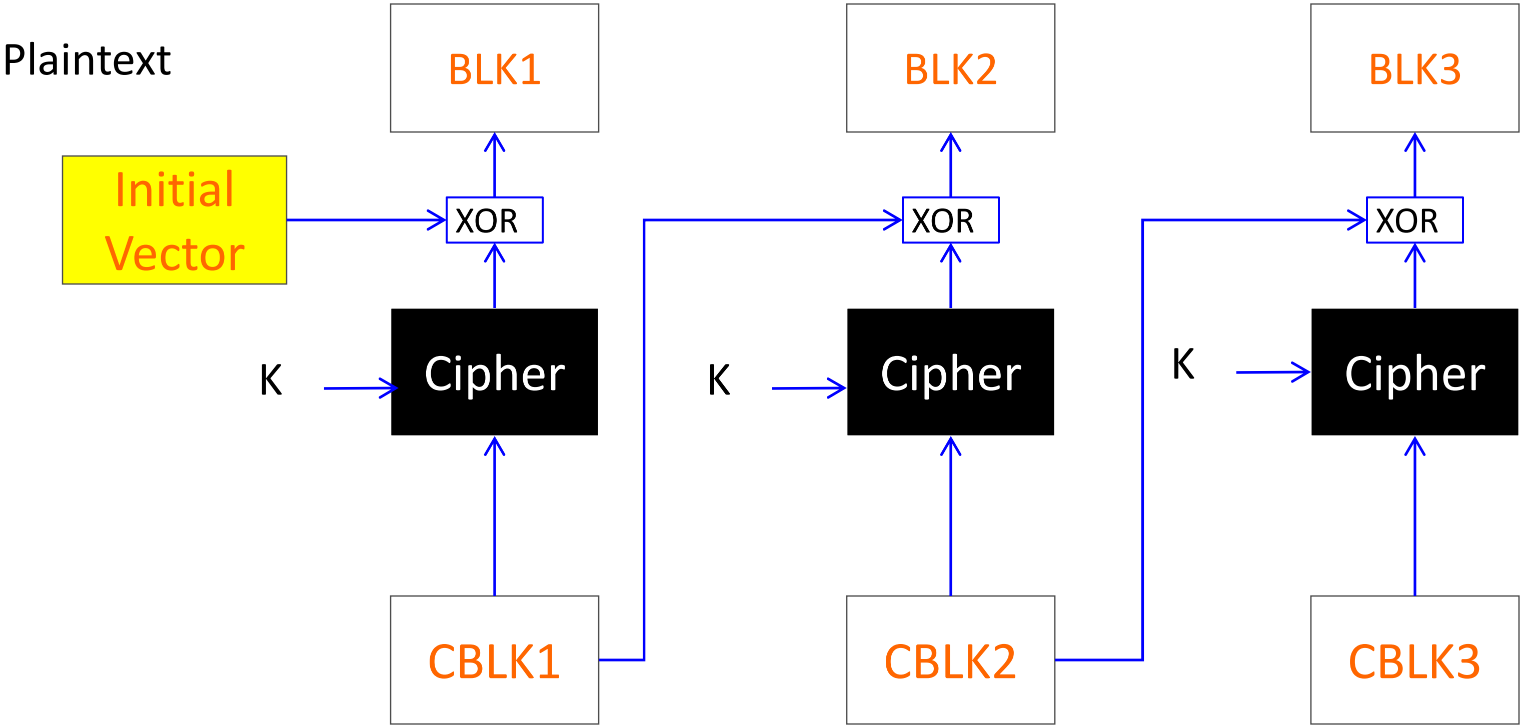
encryption with **IV=111**

Plaintext	101	101	110	010
(After XOR)				
Ciphertext				

CBC Mode Decryption

Ciphertext	Initial Vector	CBLK1	CBLK2	CBLK3

CBC ciphertext includes the IV used in encryption



BLK_i = $\mathbf{Dec}_K(CBLK_i) \oplus CBLK_{i-1}$, $CBLK_0$=IV

CBC – A toy example (decryption)

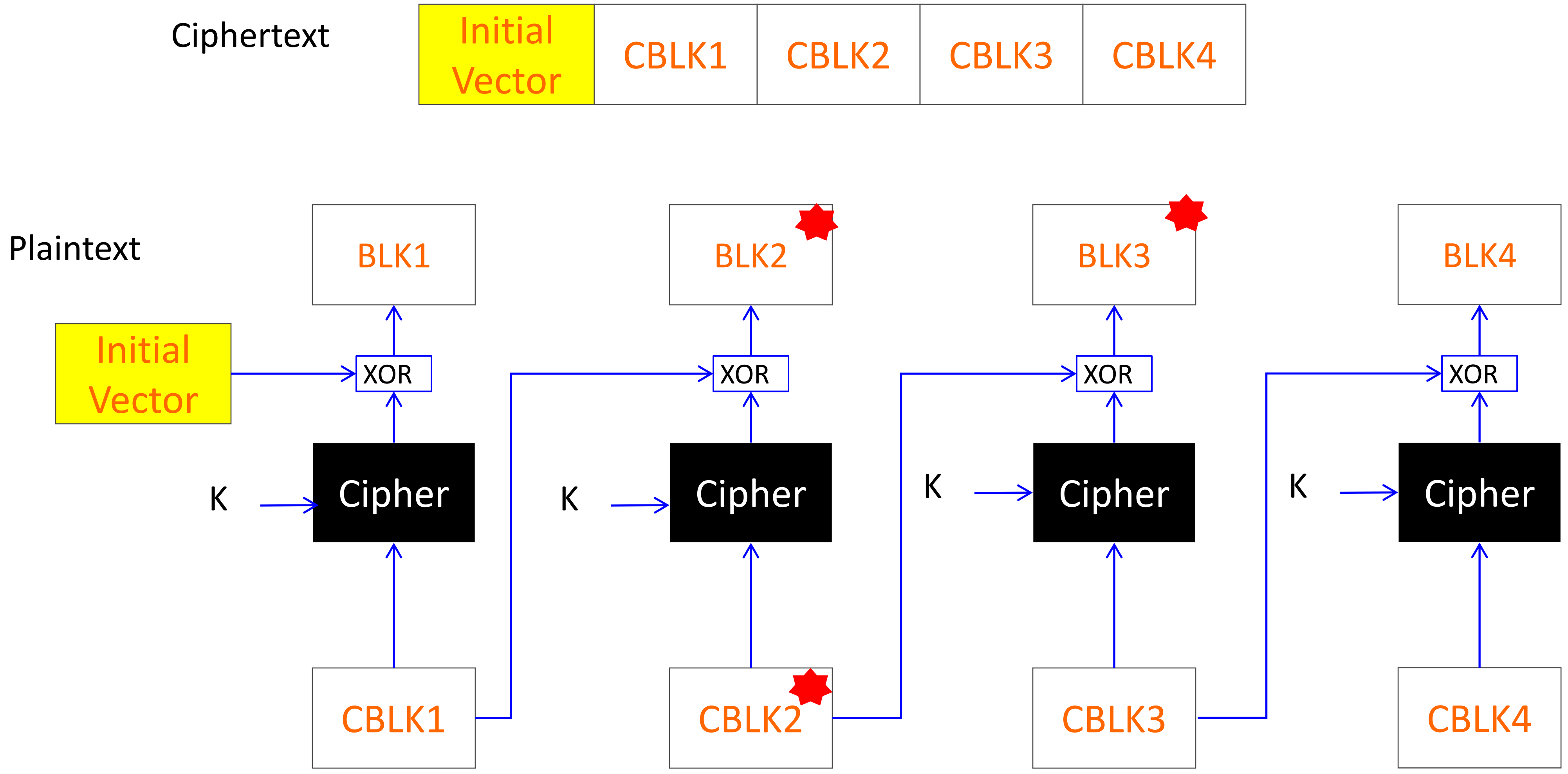
- Let us consider a toy 3-bit block cipher with the following mapping:

Plaintext Block	000	001	010	011	100	101	110	111
Ciphertext Block	111	110	011	100	001	000	101	010

Decryption with **IV=111**

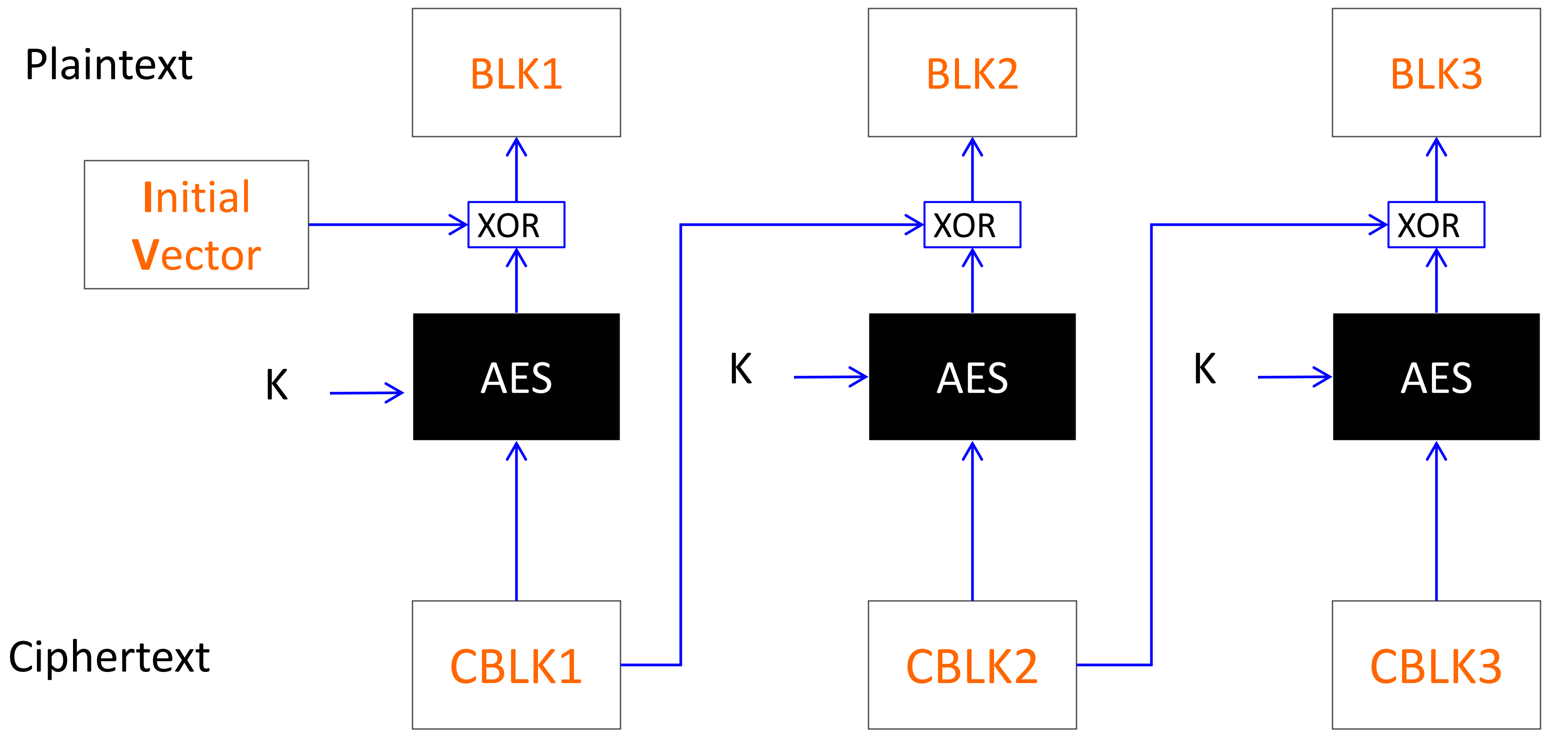
Plaintext				
(before XOR)				
Ciphertext	011	101	100	101

Error Propagation in CBC Decryption

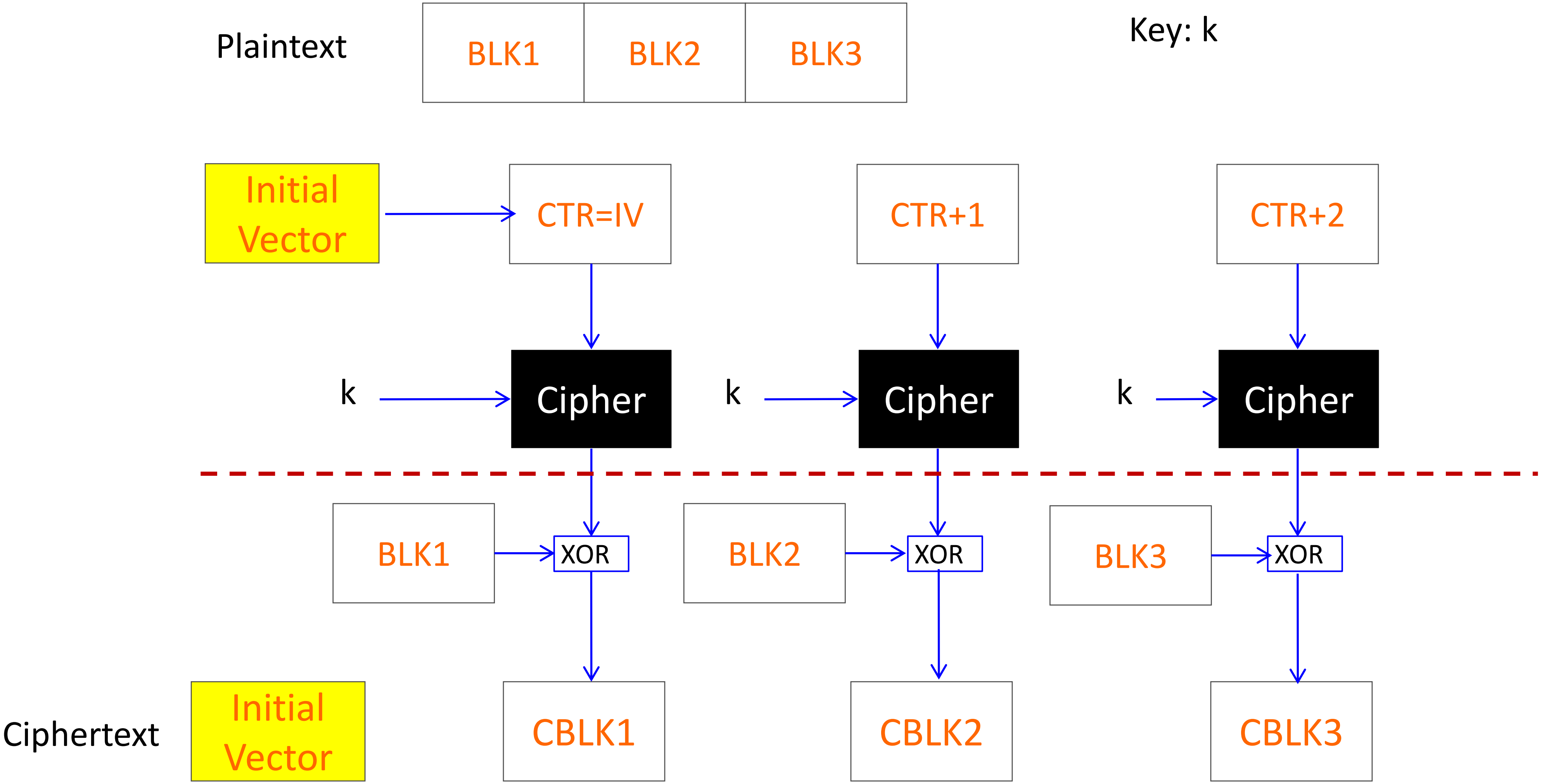


$\text{BLK}_i = \textbf{Dec}_K(\text{CBLK}_i) \oplus \text{CBLK}_{i-1}, \quad \text{CBLK}_0\text{=IV}$

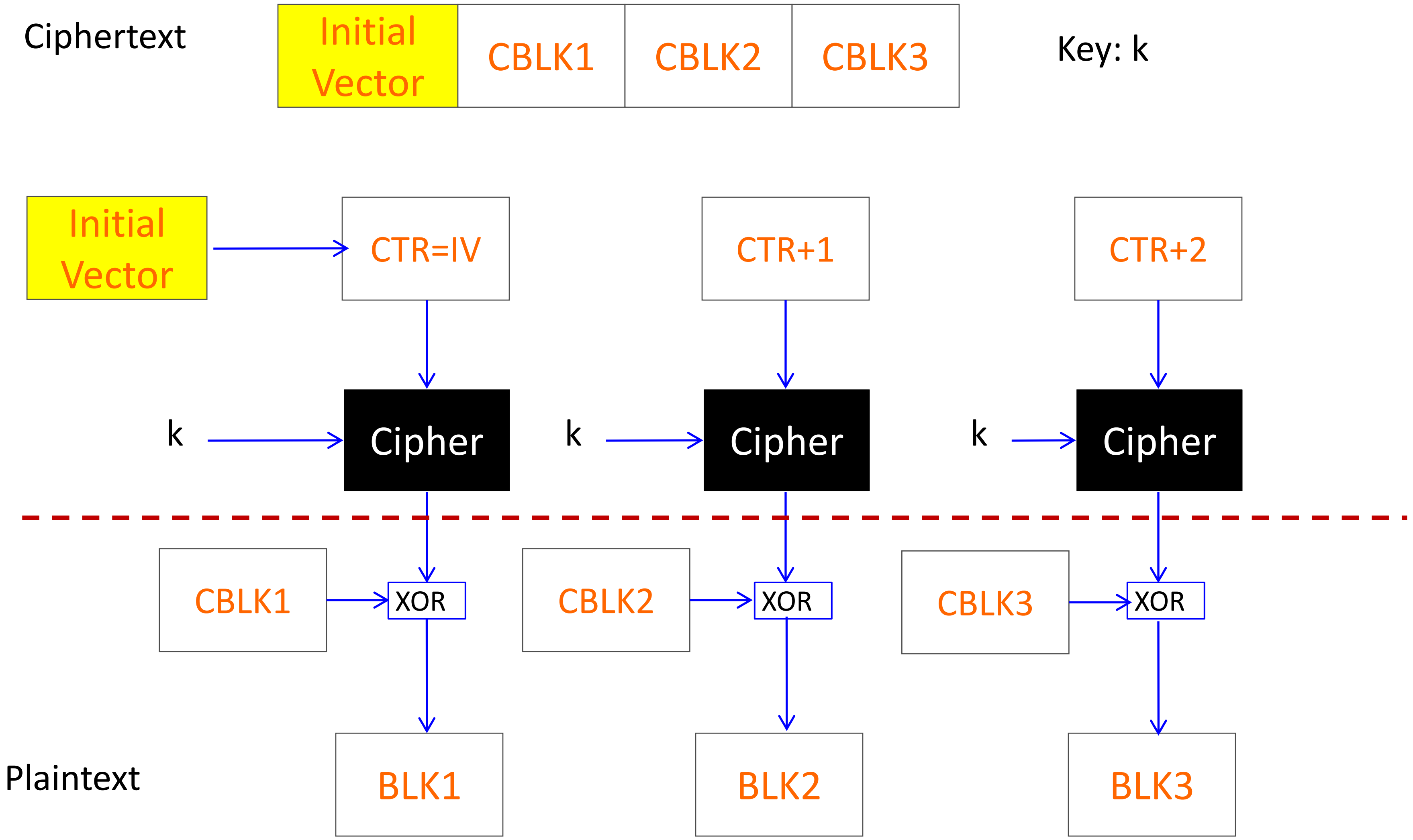
CBC mode (parallel) Decryption



CTR Mode Encryption



CTR Mode Decryption



Main Properties of Three Encryption Modes

	ECB mode	CBC mode	CTR mode
identical plaintext blocks result in	identical ciphertext blocks	different ciphertext blocks	different ciphertext blocks
chain dependency	blocks are enciphered independently	proper encryption/decryption requires a correct preceding plaintext/ciphertext block.	blocks are enciphered independently (with an increasing counter value)
error propagation	none	a ciphertext block’s error affects decipherment of itself and the next block.	none

Takeaways

- The rationale of encryption
- One-time pad cipher
- AES: key size, block sizes
- ECB, CBC and CTR mode encryption