



CHƯƠNG 2: MÃ KHÓA BÍ MẬT

Giảng viên: Nguyễn Văn Nhân

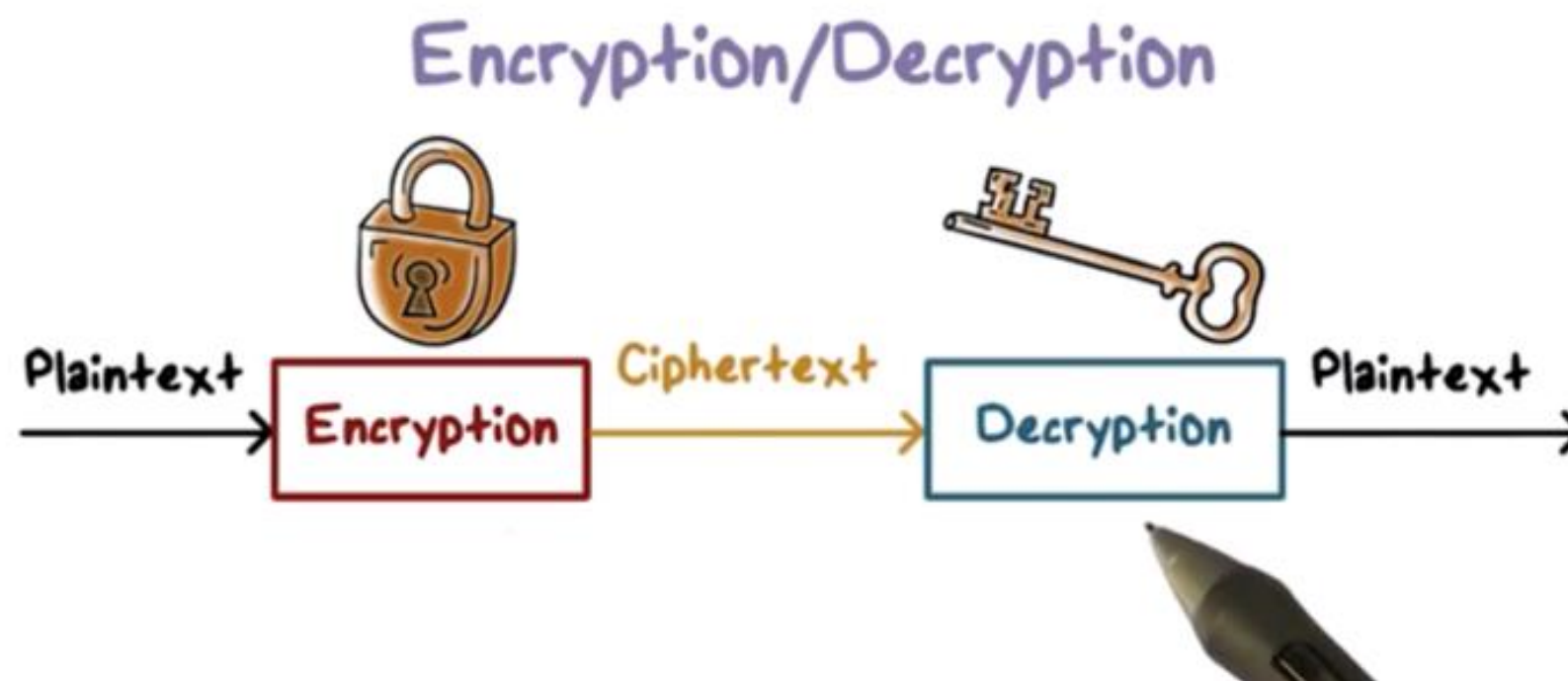
Điện thoại: 0346542854

Email: nhannv@dainam.edu.vn

Mật mã học (cryptography)

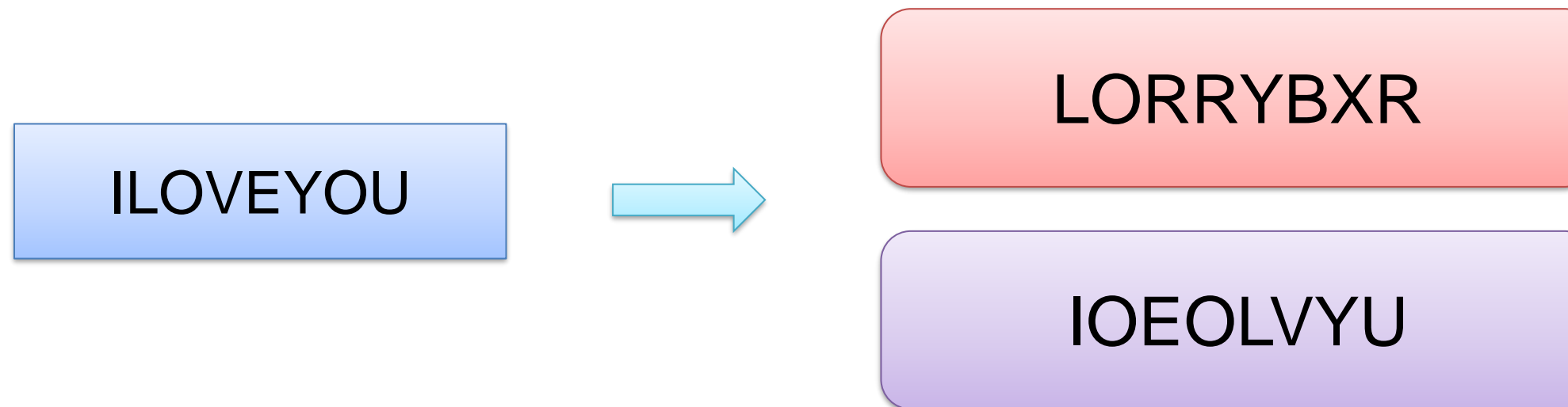
- Ngành khoa học nghiên cứu các phương pháp toán học để mã hóa giữ mật thông tin. Bao gồm mã hóa và giải mã.

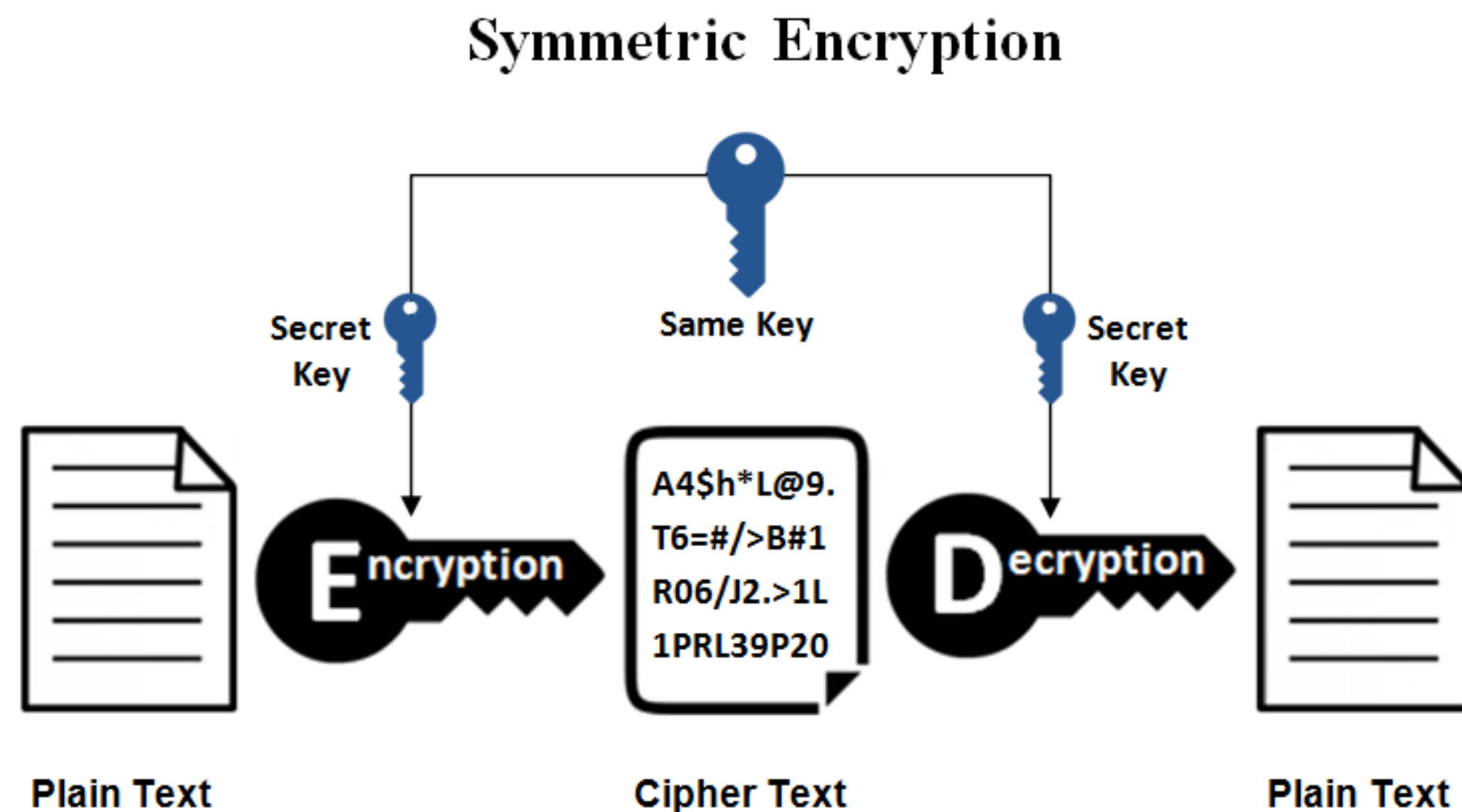
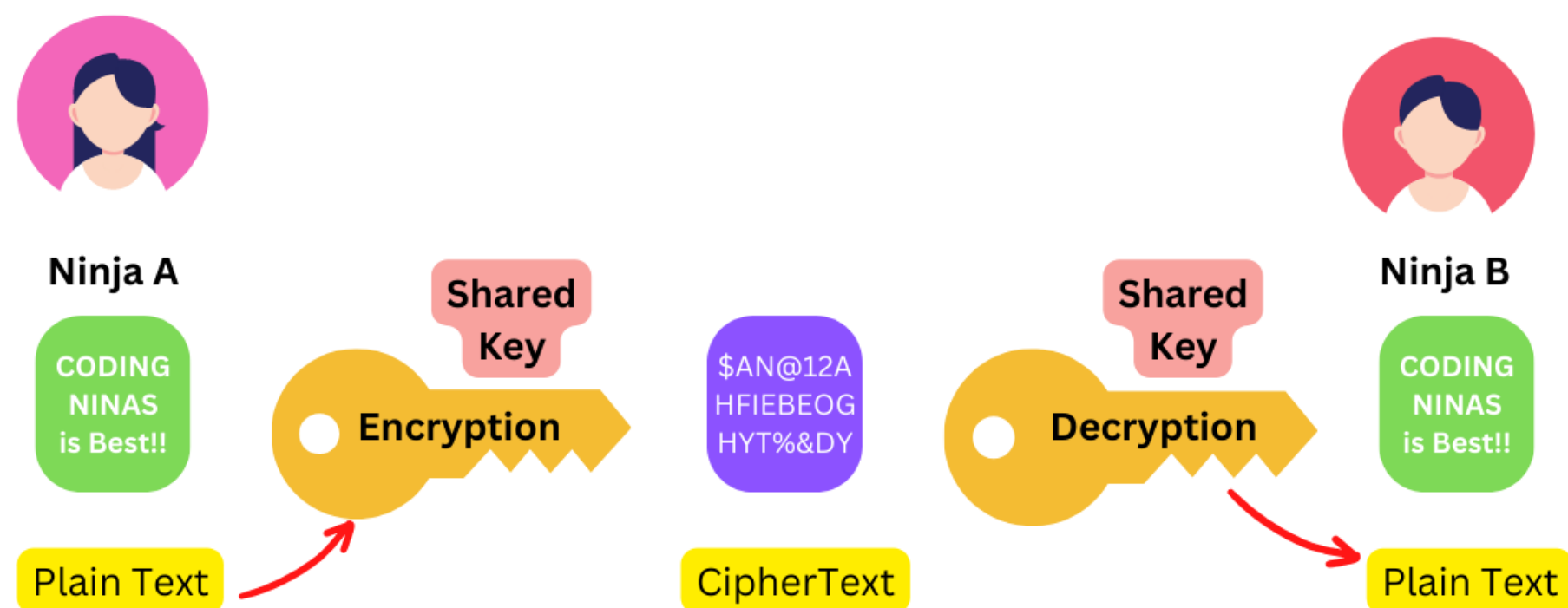
- **Mã hóa:** biến đổi cách thức biểu diễn thông tin từ dạng **bản rõ** sang dạng **bản mã** => che giấu, giữ mật thông tin (lưu trữ, truyền thông tin đi)
- **Giải mã:** ngược lại **Mã hóa** là biến bản mã thành bản rõ.



Mật mã học (cryptography)

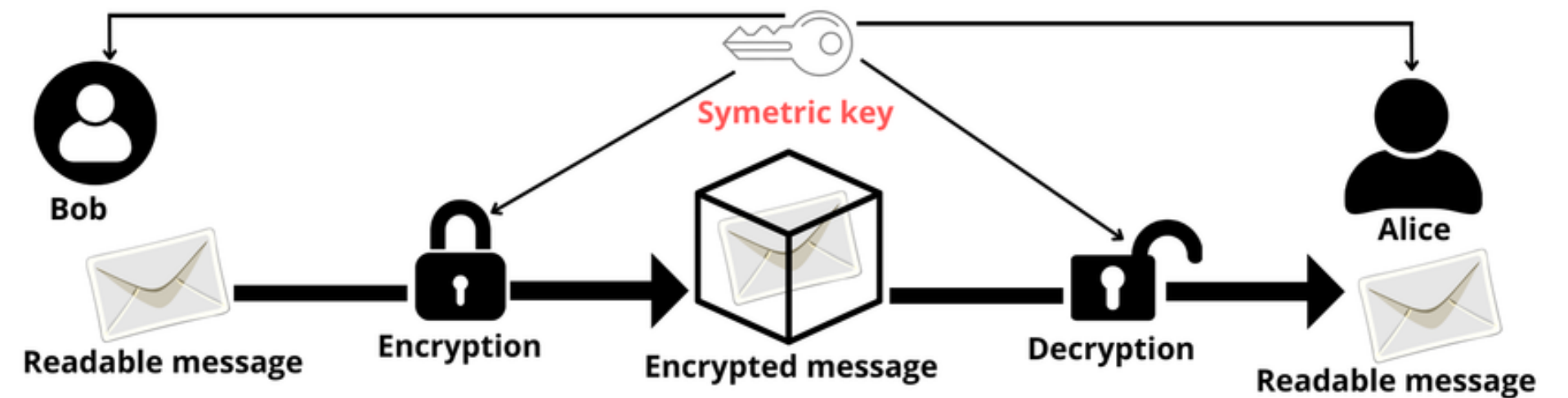
- ✓ Bản rõ / thông điệp gốc (Plaintext - **P**) (mọi người có thể hiểu được)
- ✓ Bản mã / thông điệp mã hóa (Ciphertext - **C**) (chỉ người giải mã hiểu được)
- ✓ Mã hóa (Encryption - **E**)
- ✓ Giải mã (Decryption - **D**)





Nội dung Chương 2: Mã hóa đối xứng

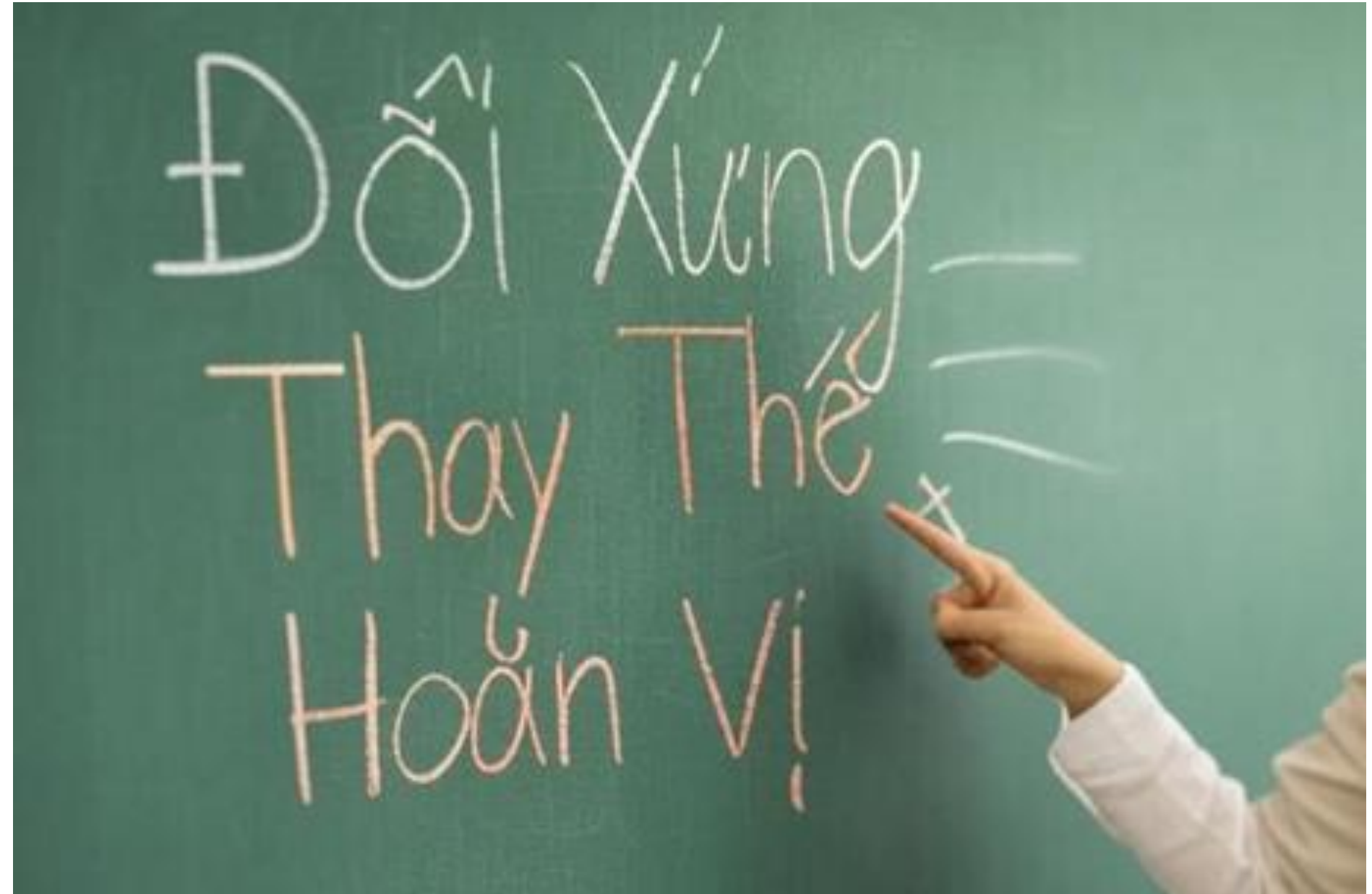
1. Kỹ thuật mã cổ điển
2. Mã khối DES
3. Mã khối AES

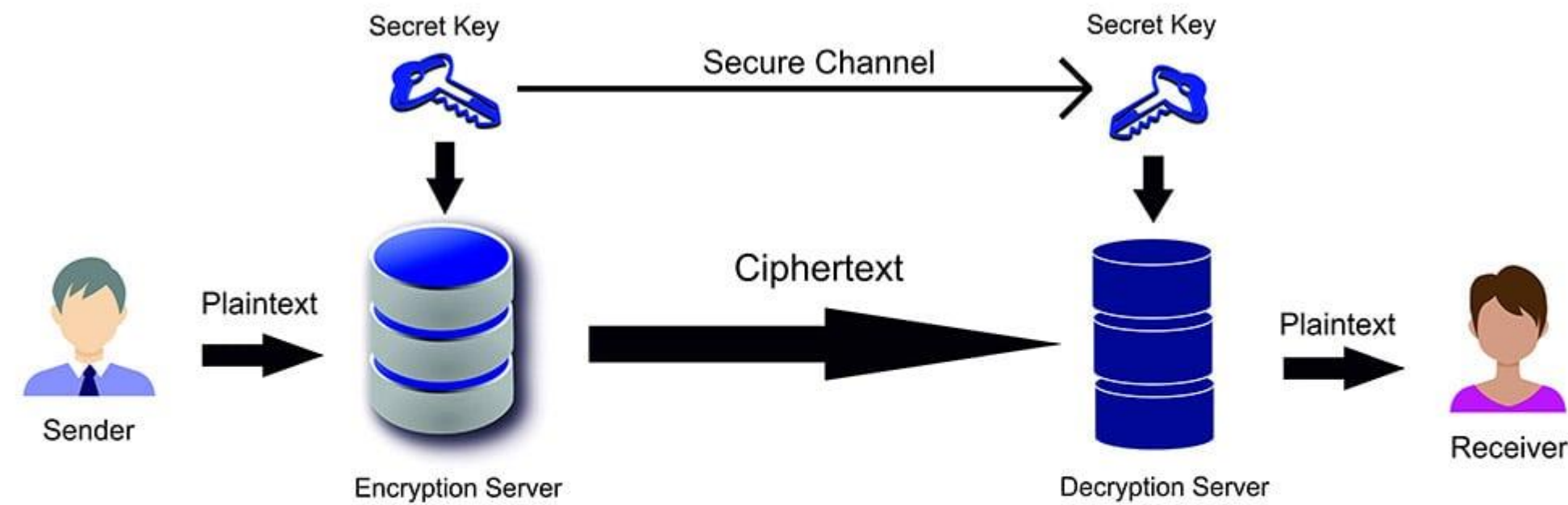


Bài 3

KỸ THUẬT MÃ CỔ ĐIỂN

- 1. Mã đối xứng**
- 2. Mã thay thế**
- 3. Mã chuyển vị**





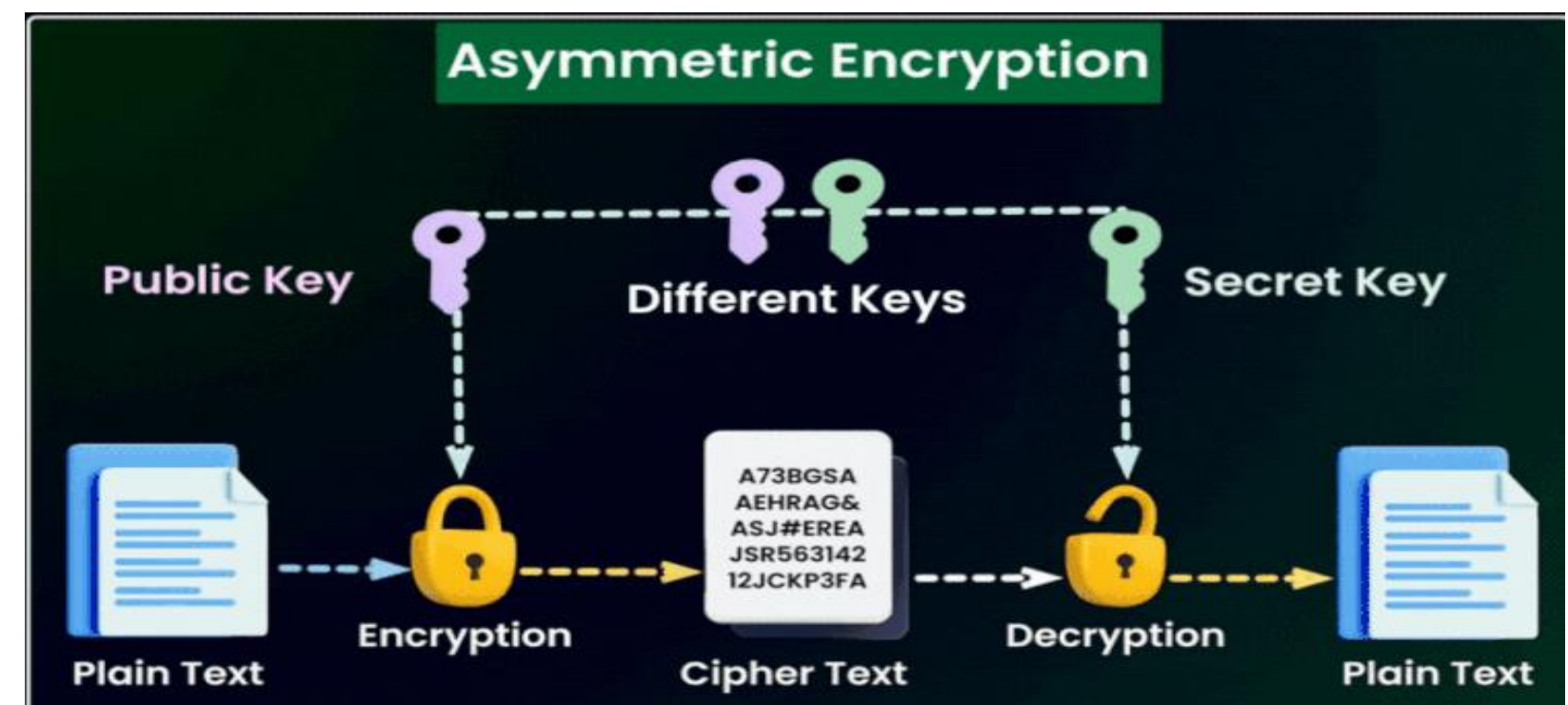
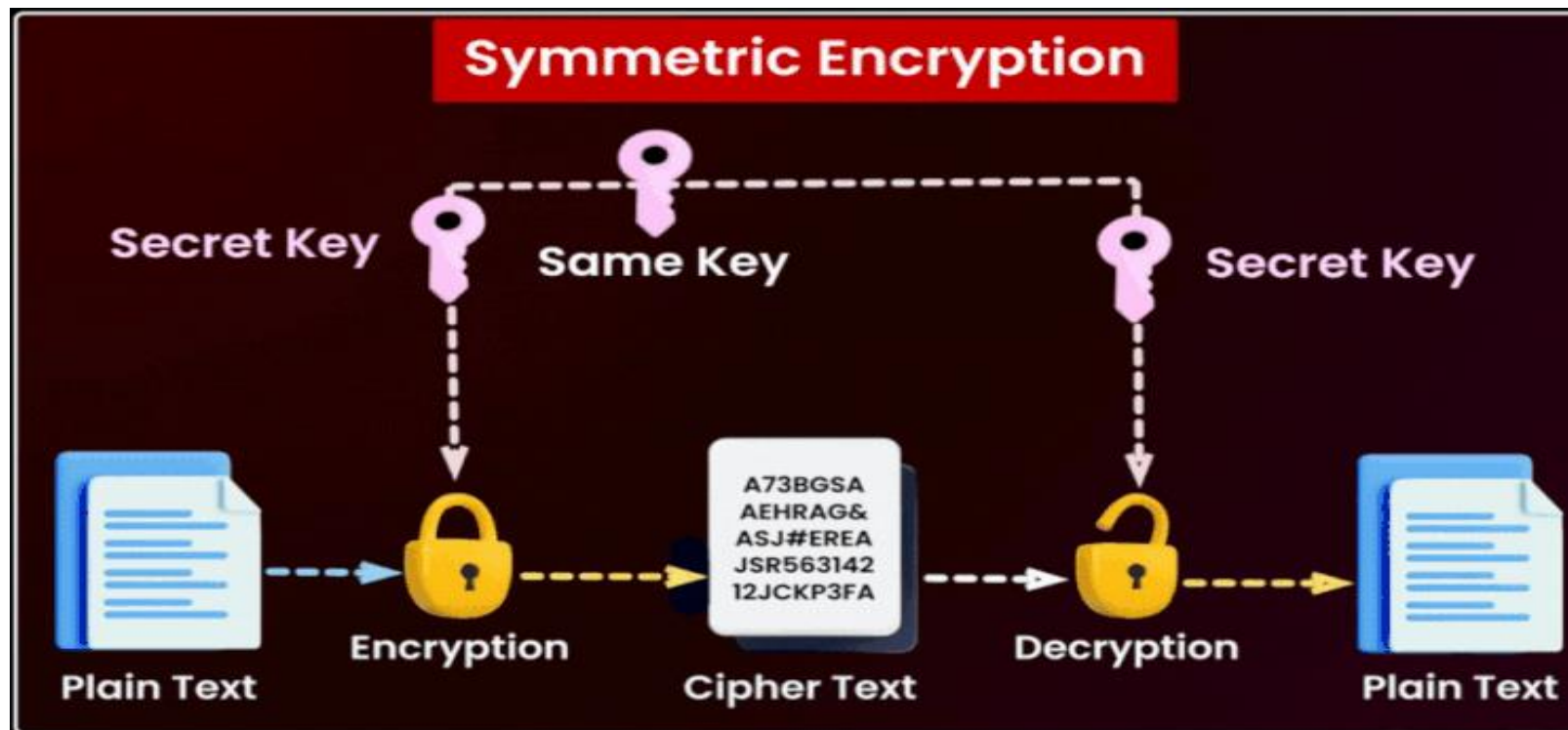
Symmetric Cryptography

Những hệ mật được sử dụng chung 1 khóa trong quá trình mã hóa và mã hóa.

Điều gì đảm bảo thông tin không bị lộ?

=> Khóa phải được giữ bí mật tuyệt đối

- Mã đối xứng sử dụng **cùng một khóa** cho cả quá trình mã hóa và giải mã.
- Công thức mã hóa và giải mã đều sử dụng cùng một khóa **K (Secret key)**.



➤ **Ưu điểm:**

Tốc độ cao và hiệu quả, phù hợp cho việc mã hóa khối lượng lớn dữ liệu nhờ sử dụng cùng một khóa cho cả mã hóa và giải mã.

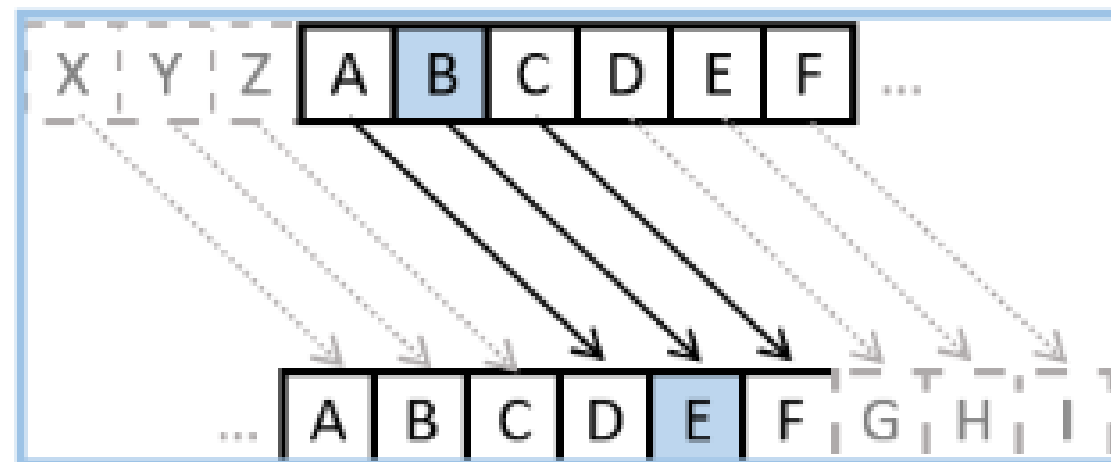
➤ **Nhược điểm:**

Vấn đề quản lý và phân phối khóa an toàn, dễ bị phá vỡ nếu khóa bị lộ.

MÃ THAY THẾ

Mã thay thế

- Mã thay thế là phương pháp mã hóa trong đó mỗi ký tự trong văn bản gốc được **thay thế** bằng một ký tự khác dựa trên một quy tắc cố định.
- Quy tắc này có thể là một bảng thay thế, một phép toán nào đó (Caesar)



SHIFT +3

This Caesar cipher has a shift of 3 characters.

The letter 'A' becomes a 'D'. The letter 'B' becomes 'E'.

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	

Plaintext

Ciphertext

Mã hóa "HELLO" bằng Caesar Cipher với khóa là 3:

- **Plaintext (P):** "HELLO"
 - **Khóa bí mật (K):** 3 (Dịch chuyển 3 bước trong bảng chữ cái)
 - **Mã hóa (E):** $C = (P + K) \bmod 26$
- ✓ Sau các bước mã hóa: $E(K, P) \Rightarrow$ Ciphertext (C): "KHOOR"
- ✓ Giải mã (D) với cùng khóa K: $D(K, C) \Rightarrow$ Plaintext (P) : "HELLO"

Quá trình mã hóa (E)

➤ Các bước mã hóa :

- 'H' (vị trí 7 trong bảng chữ cái) → 'K' (vị trí 10)
- 'E' (4) → 'H' (7)
- 'L' (11) → 'O' (14)
- 'L' (11) → 'O' (14)
- 'O' (14) → 'R' (17)

=> **Ciphertext (C): "KHOOR"**

Giải mã (D) với cùng khóa 3:

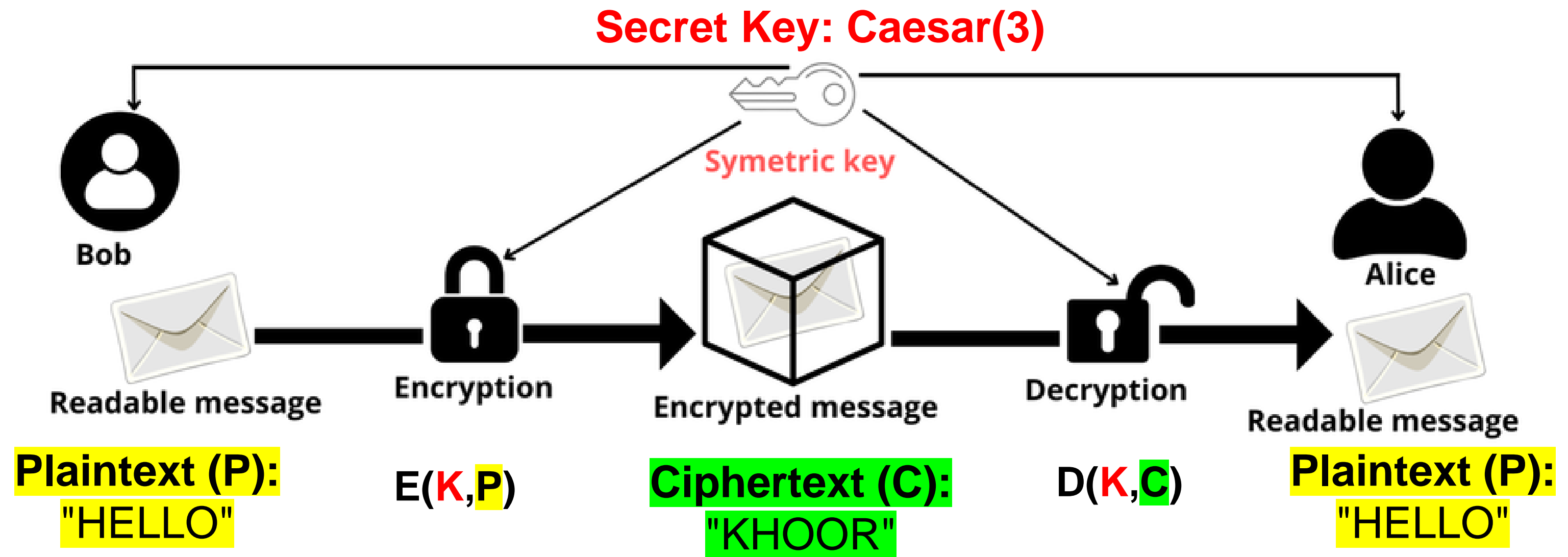
➤ Để giải mã, ta sẽ trừ đi khóa từ mỗi ký

tự của ciphertext **$P = (C - K) \bmod 26$** :

- 'K' (vị trí 10) → 'H' (vị trí 7)
- 'H' (7) → 'E' (4)
- 'O' (14) → 'L' (11)
- 'O' (14) → 'L' (11)
- 'R' (17) → 'O' (14)

=> **Plaintext (P): "HELLO"**

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





Phá Mã Caesar bằng Brute Force


Phá Mã Caesar bằng Brute Force

- **Brute Force:** Phương pháp thử tất cả các khóa khả thi để tìm khóa đúng.
- Với mã Caesar cần thử bao nhiêu khóa?
Chỉ cần thử 25 khóa (từ 1 đến 25, vì 26 không thay đổi thông điệp).

➤ Cách hoạt động

- Nhận thông điệp mã hóa ("LORYHBXR").
- Thử dịch ngược với từng khóa (1, 2, 3, ...).
- Kiểm tra kết quả để tìm thông điệp có ý nghĩa (ví dụ: "ILOVEYOU" với khóa 3).

➤ Ví dụ

- 1) Khóa 1: "KNQXGAXQ"
- 2) Khóa 2: "JMPWFZWP"
- 3) Khóa 3: "ILOVEYOU" 

MÃ CHUYỂN VỊ

- ❖ Các ký tự của bản rõ (P) được sắp xếp lại theo một quy tắc nhất định để tạo thành bản mã (C), mà không thay đổi bản chất của các ký tự.
 - ❖ **Nguyên tắc cơ bản:** Bản rõ được viết vào một cấu trúc (thường là ma trận hoặc bảng) theo một thứ tự nhất định.
 - Các ký tự được đọc ra theo một thứ tự khác để tạo bản mã.
 - Để giải mã, cần biết cấu trúc và thứ tự hoán vị ban đầu.
- ✓ Mã hóa chuyển vị hàng rào từ “HELLO”



❖ **Chuyển vị hàng rào (Rail Fence Cipher):** Sắp xếp ký tự theo dạng zig-zag trên các "hàng rào" và đọc theo hàng.

Mã hóa chuyển vị hàng rào từ “HELLO”

➤ **Nguyên tắc:**

- Chọn số hàng (rails) để tạo "hàng rào" .
- Viết bản rõ theo dạng zig-zag qua các hàng.
- Đọc bản mã theo từng hàng từ trên xuống dưới.



H . L . O
. E . L .

- Hàng 1: HLO
- Hàng 2: EL

=> **Bản mã(C): HLOEL**

- Mã đối xứng
- Mã thay thế
- Mã chuyển vị





Thực hành bài Lab



Thank You