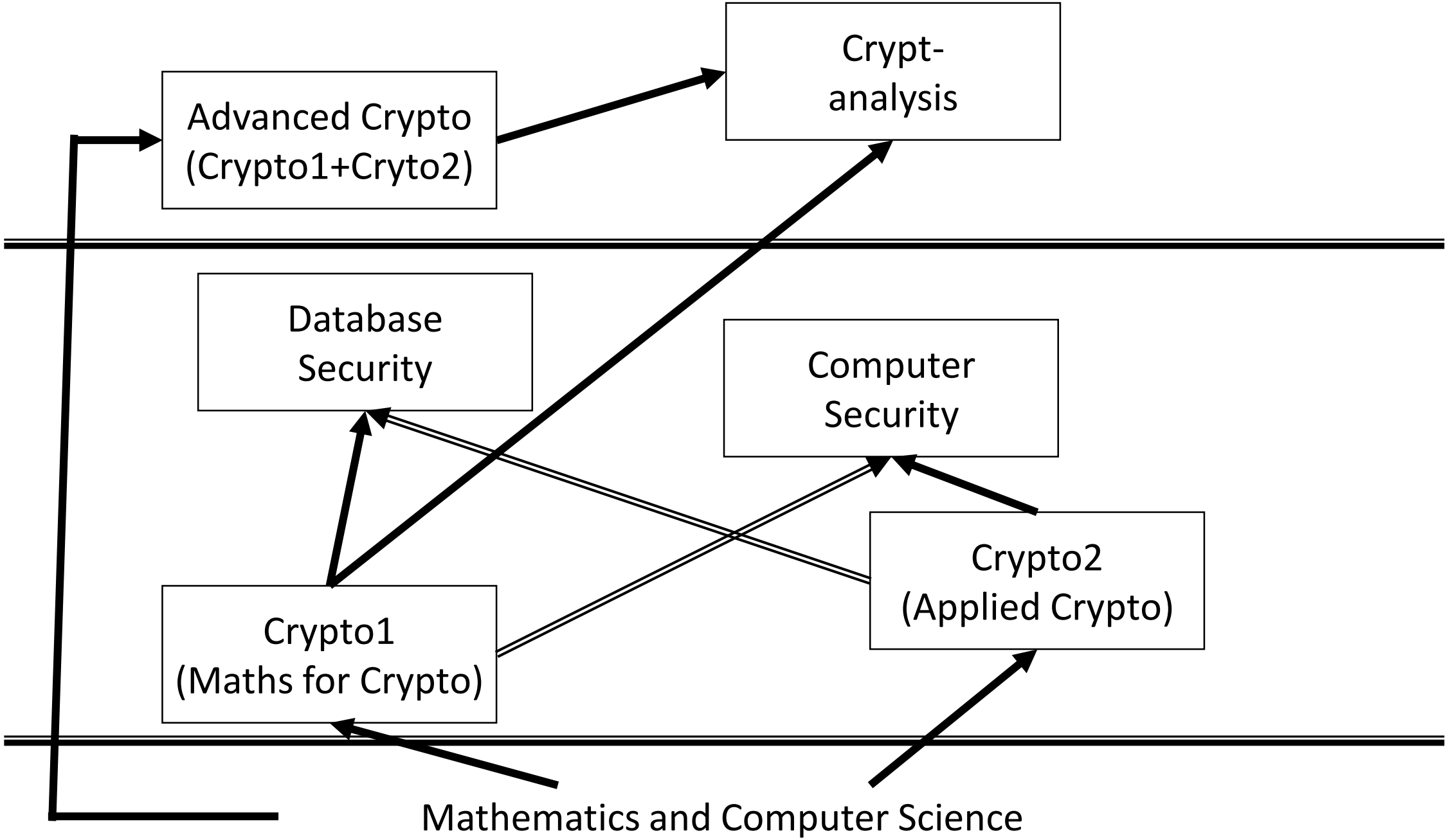
Lesson 10.

Cryptography

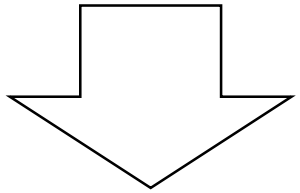

Crypt-
analysis
Advanced Crypto
(Crypto1+Cryto2)
Database
Security
Computer
Security
Crypto2
(Applied Crypto)
Crypto1
(Maths for Crypto)
Mathematics and Computer Science

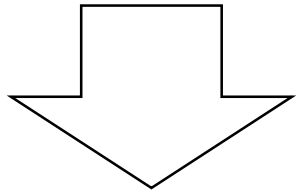
Một số thuật ngữ

- **Plaintext:** bản rõ (bản gốc) – *the original message*
- **Ciphertext**: bản mã (bản mật – *the coded message*), là kết quả của bản rõ sau khi mã hóa
- **Encryption** (encipher**)**: mã hóa, là quá trình chuyển đổi bản rõ thành bản mã – *converting plaintext to ciphertext*
- **Decryption** (decipher): giải mã, là quá trình biến đổi bản mã thành bản rõ
- **Cryptosystem**: hệ mã, là phương pháp ngụy trang bản rõ
- **Cryptanalysis** (codebreaking): phá mã, là quá trình cố gắng chuyển đổi bản mã thành bản rõ mà không có khóa – *the study of principles/methods of deciphering ciphertext without knowing key*

Mã hóa ứng dụng – giới thiệu

Cryptology = Cryptography + Cryptanalysis





Building a cryptosystem

Analyzing a cryptosystem

Định nghĩa

$$E_k: \mathcal{M} \rightarrow \mathcal{C}, \exists D_{k'}: \mathcal{C} \rightarrow \mathcal{M} / \forall m \in \mathcal{M}, k \in \mathcal{K}: D_{k'}\left(E_k(m)\right) = m$$

- $k \cong k'$: Symmetric/Secret key/Pre-share key Cryptosystem.

- $k \neq k'(k' = Gen(k))$: Assymmetric/Public key Cryptosystem.

- $M = m_1 \dots m_n, m_i \in \mathcal{M}\ (i = 1, \dots, n)$: Cryptographic Hash Function

Bảo mật

Tính chất

- *Confidentiality*
- *Integrity*
- *Authenticity* (xác thực)

Thám mã

- *Brute-Force Attack*
- *Cipher-text-Only Attack*
- *Known-Plaintext Attack*
- *Chosen-Plaintext Attack*
- *Chosen-Cipher-text Attack*

- *Meet-in-the-Middle*

Nguyên tắc

Tính chất

- Diffusion

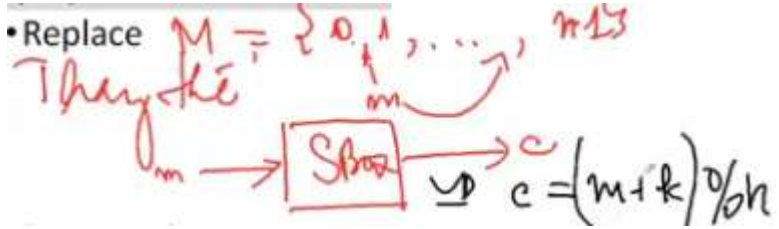
(phát tán)

- Confusion

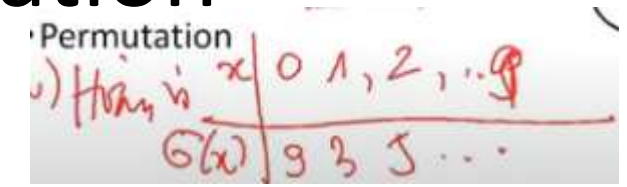
(Rối)

Kỹ thuật

- Replace



- Permutation



Mật mã khóa đối xứng

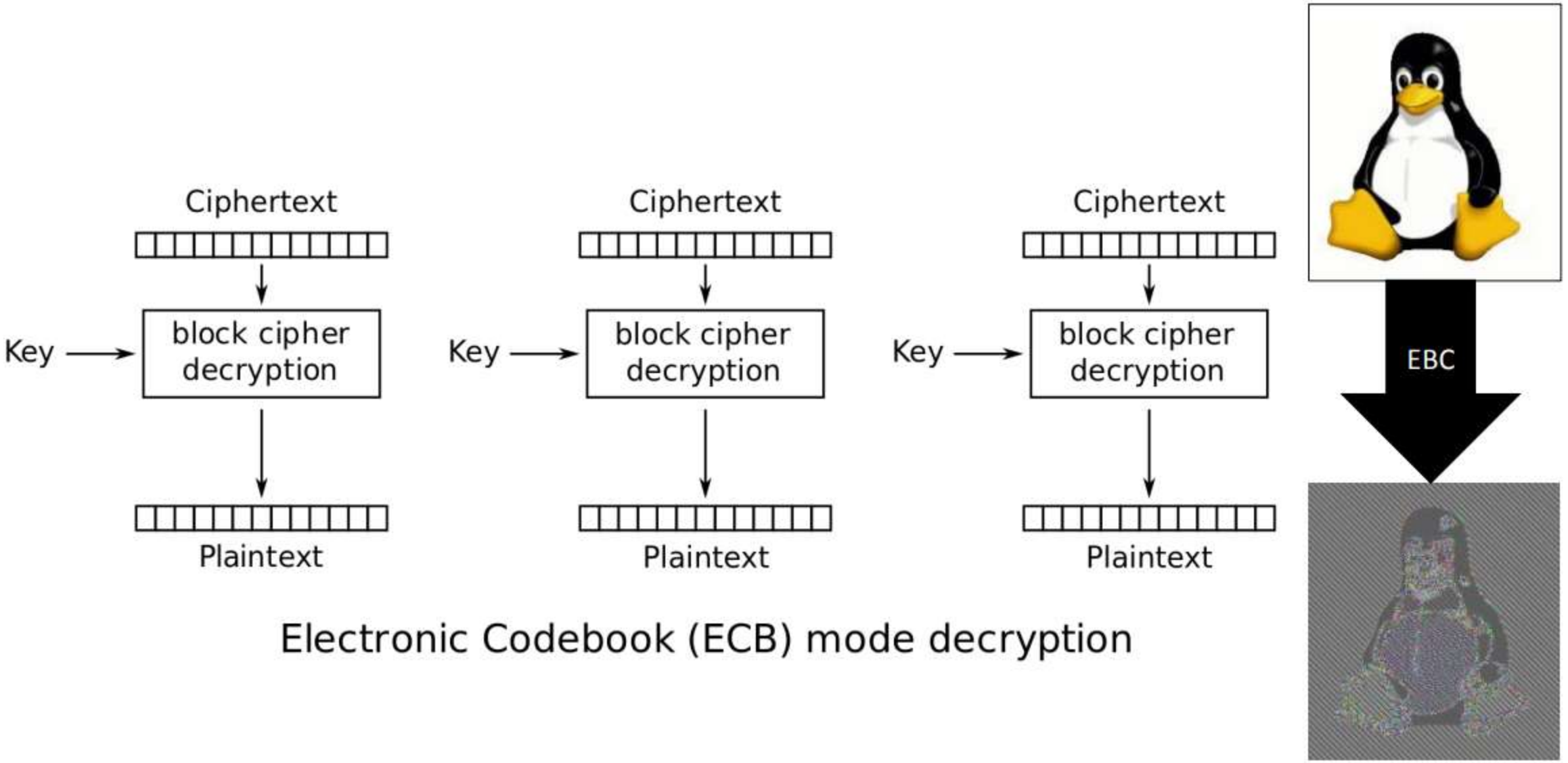
Khái niệm

$$E_k: \mathcal{M} \rightarrow \mathcal{C},$$
$$\exists D_k \equiv E_k^{-1}: \mathcal{C} \rightarrow \mathcal{M}$$
$$s.c. \forall m \in \mathcal{M}, c = E_k(m) \in \mathcal{C} \Rightarrow D_k(c) = m, k \in \mathcal{K}$$

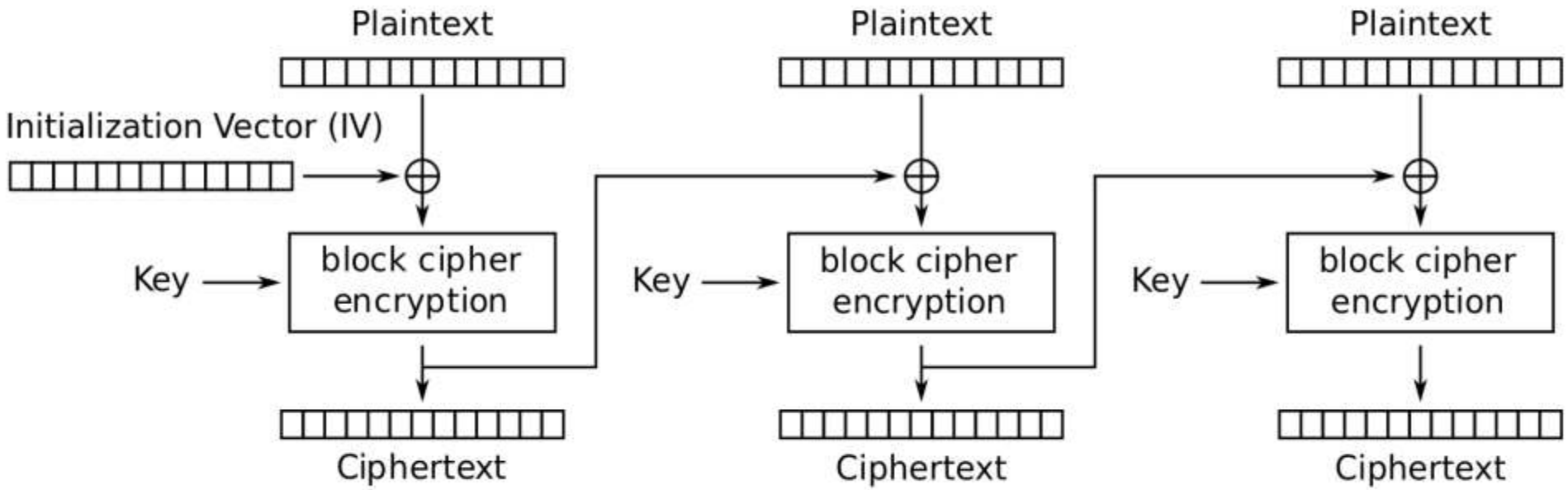
m $\in \boldsymbol{\mathcal{M}}$

- Nếu length(m) > unit, E: mã khối (block cipher)
- Nếu length(m) = unit, E: mã dòng (stream cipher)

Các mode cài đặt

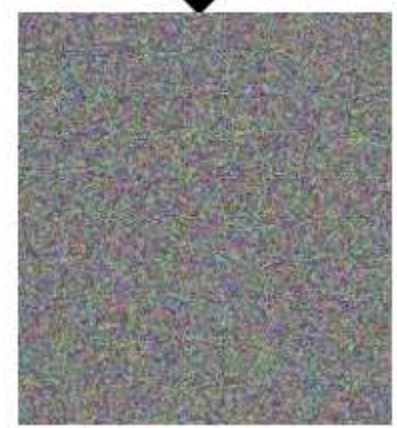


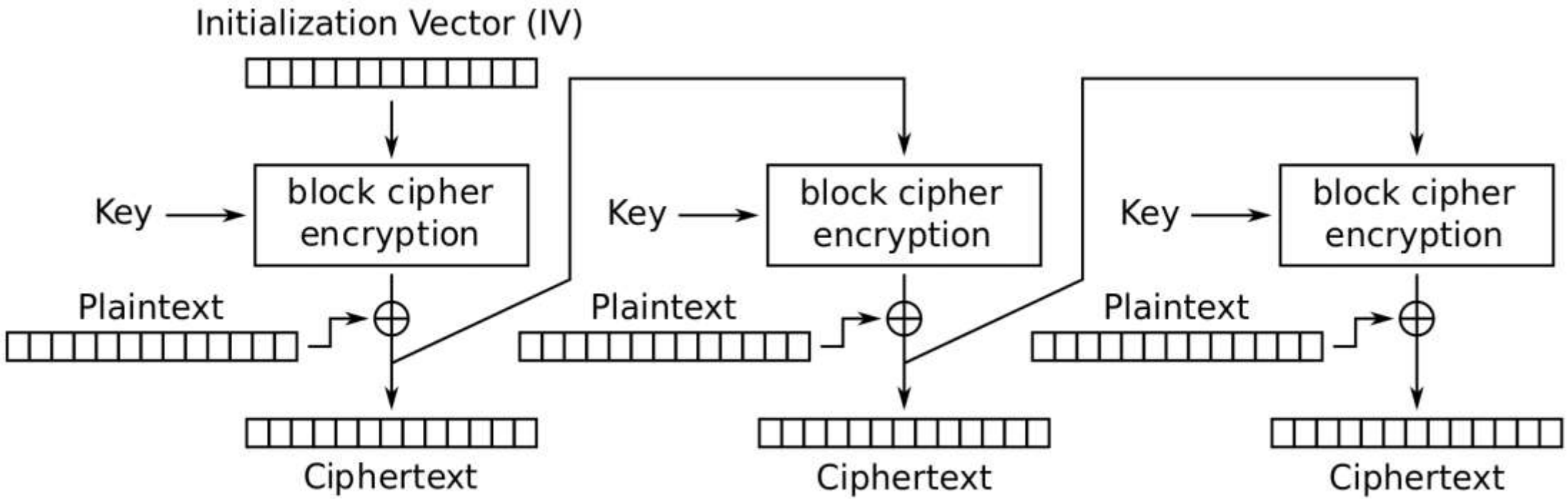
Electronic Codebook (ECB) mode decryption



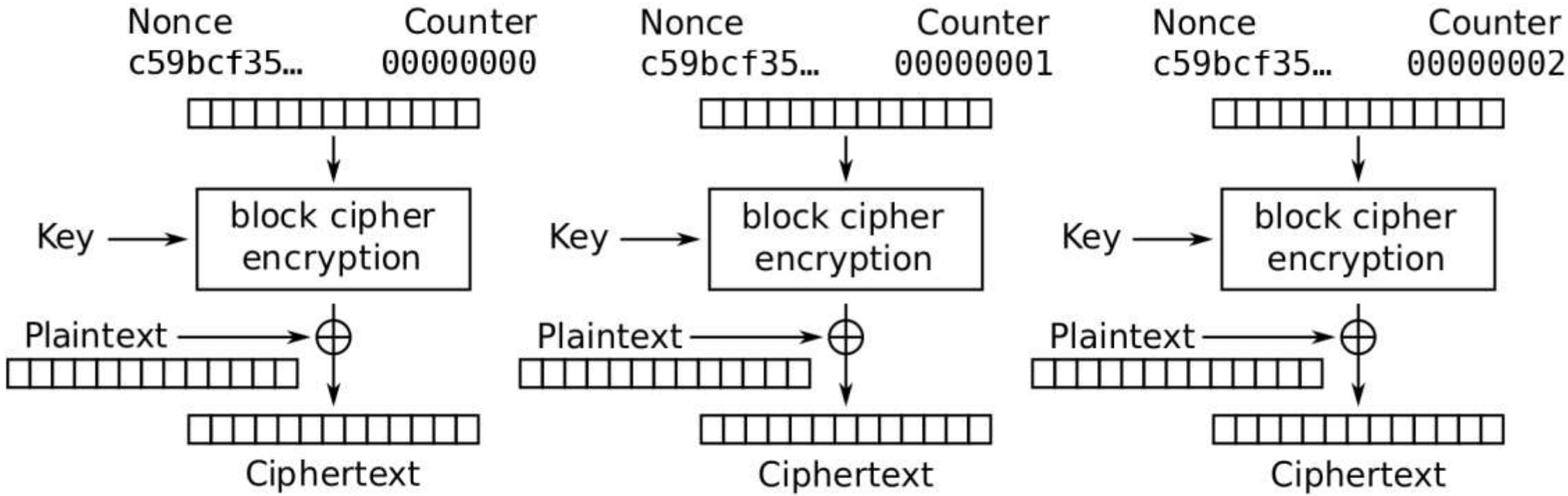
Cipher Block Chaining (CBC) mode encryption

EBC





Cipher Feedback (CFB) mode encryption



Counter (CTR) mode encryption

Public Key Cryptosystems

Mã (khóa) công khai

$$E_e: \mathcal{M} \rightarrow \mathcal{C} \; and \; D_d: \mathcal{C} \rightarrow \mathcal{M}:$$

$$\forall m \in \mathcal{M}, c \in \mathcal{C}, e, d \in \mathcal{K}$$

$$c = E_e(m) \leftrightarrow m = D_d(c);$$

$$\forall e, d \in \mathcal{K}: R(e, d)$$

Ví dụ

$$\mathcal{C} \equiv \mathcal{M} \equiv \{0, 1, \dots, 9\}$$

$$e = 3, d = 7$$

$$\forall m \in \mathcal{M}, c = E_e(m) = m^3 \; mod \; 11 \in \mathcal{C};$$

$$\forall c \in \mathcal{C}, m = D_d(c) = c^7 \; mod \; 11 \in \mathcal{M}$$

- m = 0, 1, 2, 3, 4, 5, 6, 7, 8, 9
- c = 0, 1, 8, 5, 9, 4, 7,2, 6, 3

Hàm một chiều có cửa sập

S, T: *tập hữu hạn*

$f: S \rightarrow T$, *khả nghịch, thỏa*

[1] $\forall x \in S, y = f(x)$ *tính dễ*

[2] $\forall y, x = f^{-1}(y)$ *tính khó*

[3] $x = f^{-1}(y)$ *tính dễ*
nếu biết thông tin cửa sập

Các hàm 1 chiều thông dụng

- [1] $f: pq \rightarrow n$

(p, q là các số nguyên tố lớn.)

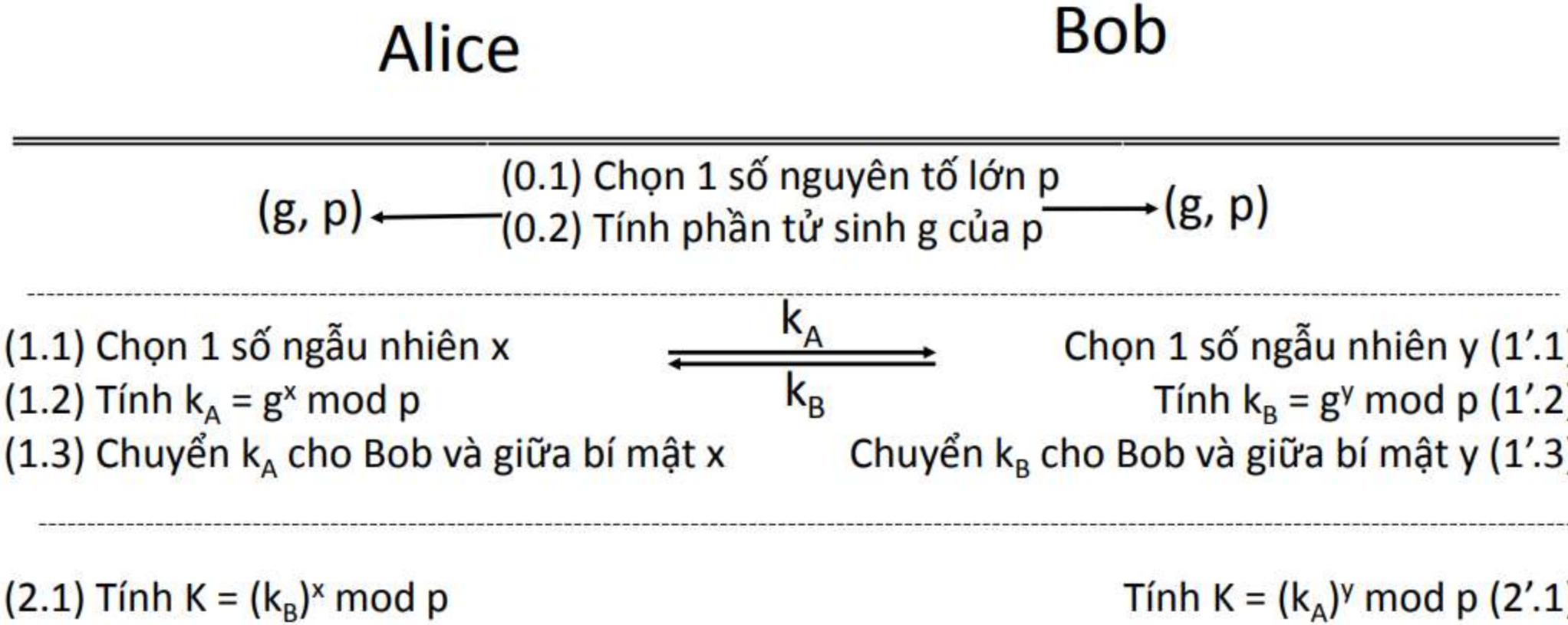
- [2] $f_{g,N}: x \rightarrow g^x \ mod \ N$
- [3] $f_{k,N}: x \rightarrow x^k \ mod \ N$

(N = pq, p, q là các số nguyên tố lớn)

Giao thức RSA

Alice	Bob $m \in \{0,1,\ldots,n\}$
(1.1) Tạo 2 số nguyên tố lớn p, q (1.2) Tính n = pq và N = (p-1)(q-1) (1.3) Chọn e, d thỏa ed mod N = 1 (1.4) Công bố (e, n) và giữ bí mật d	$\longrightarrow$ (e, n)
c $\longleftarrow$	(2.1) Tính $c = m^e \bmod n$ (2.2) Chuyển c cho Alice
(3.1) Tính $m = c^d \bmod n$	

Giao thức Diffie-Hellman



Phần tử sinh (của snt p hay Z_p)

- VD: Xét Z_7={1, 2, 3, 4, 5, 6}

Chọn g=2. 2^0 %7=1, 2^1 %7=2, 2^3 %7=1

g=3.

Giao thức ElGamal

Alice		Bob
(0.1) Chọn 1 số nguyên tố lớn p (0.2) Tính phần tử sinh g của p (0.3) Chọn khóa giải mã d (0.4) Tính và công bố $e = g^d \bmod p$	⟶	(e, p, g)
		Chọn 1 số ngẫu nhiên y (1.1) Tính $c_1 = g^y \bmod p$ (1.2) Tính $c_2 = e^y.m \bmod p$ (1.3) Gửi $C = (c_1, c_2)$ cho Alice (1.4)
$C = (c_1, c_2)$	⟵	
(2.1) Tính $m = (1/(c_1)^d).c_2 \bmod p$		