

NGHIÊN CỨU CÁC GIẢI THUẬT MÃ HÓA

Báo cáo môn Cấu Trúc Dữ Liệu và Giải Thuật

Giáo viên hướng dẫn: TS. Phạm Trung Thông

Nhóm thực hiện: Nhóm 9

Các thành viên trong nhóm:

Nguyễn Xuân An

Võ Đình Đại

Trần Ngọc Phúc

Trịnh Trọng Phước

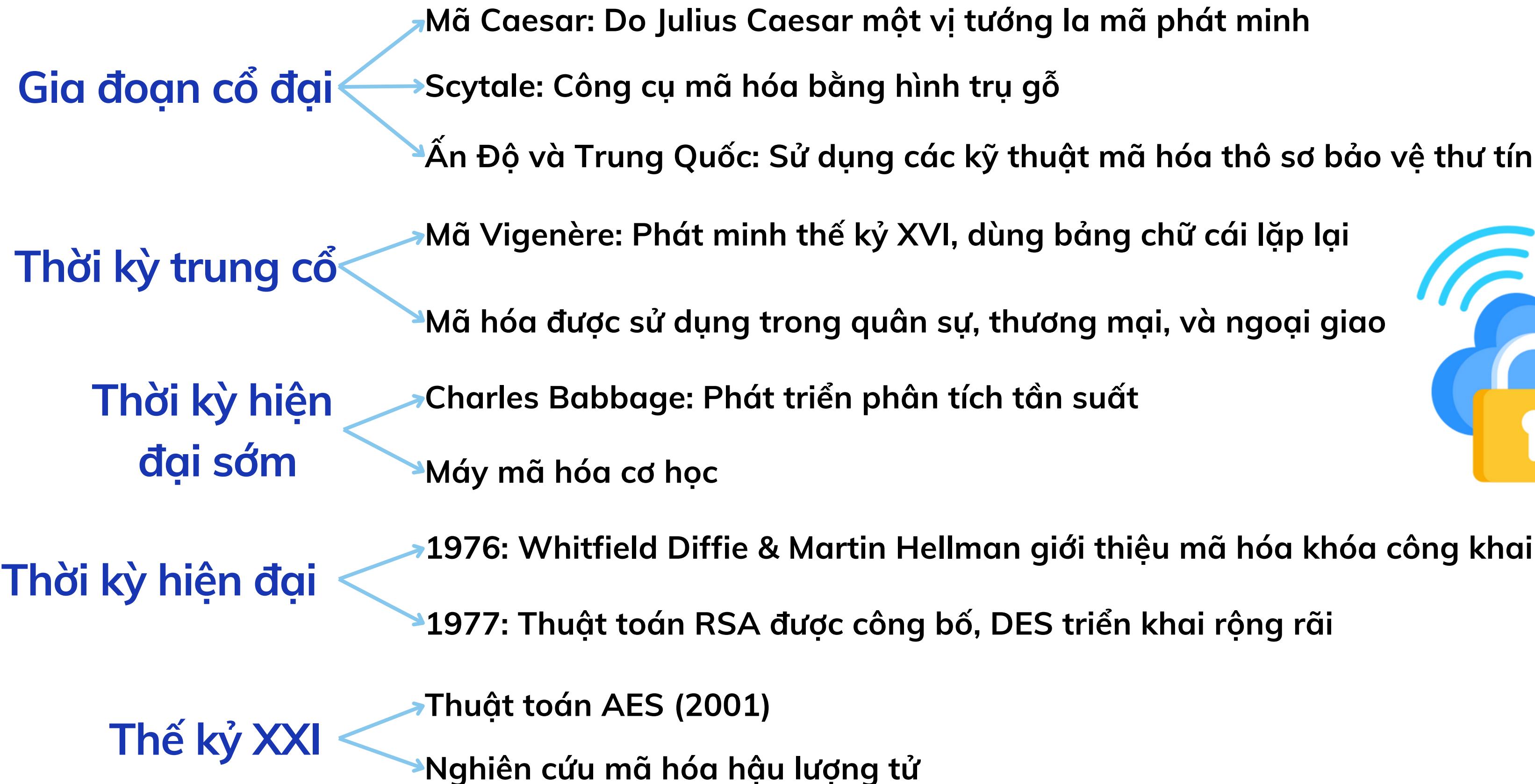
Nguyễn Hữu Thắng

Mục lục

- I. Lịch sử hình thành của mã hóa
- II. Phân loại mã hóa
- III. Giải thuật Casear Cipher
- IV. Giải thuật AES
- V. Giải thuật RSA
- VI. Giải thuật SHA256
- VII. Mô phỏng
- VIII. Tài liệu tham khảo



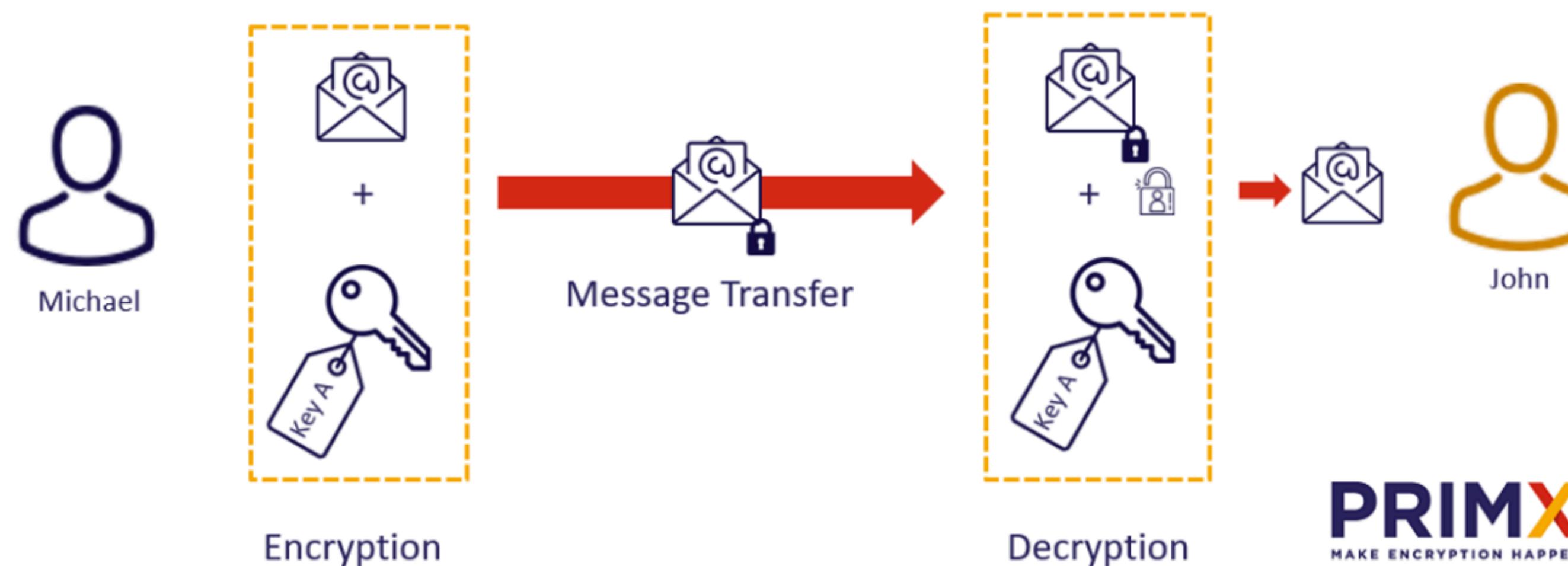
I. Lịch sử hình thành của mã hóa



II. Phân loại mã hóa

Mã hóa đối xứng

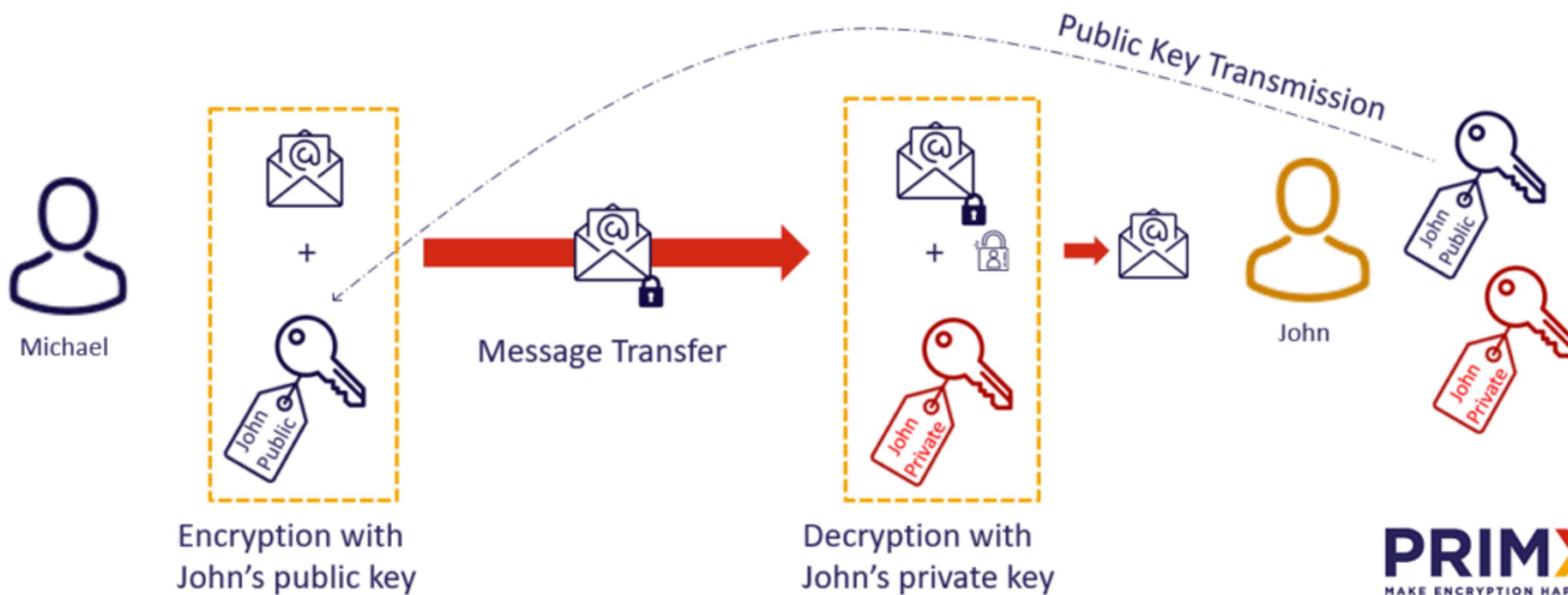
- ❖ Sử dụng một khóa duy nhất để mã hóa và giải mã.
- ❖ Nhanh, hiệu quả, nhưng yêu cầu chia sẻ khóa an toàn.
- ❖ Ví dụ: DES, AES.



II. Phân loại mã hóa

Mã hóa bất đối xứng

- ❖ Sử dụng cặp khóa công khai và khóa riêng (một khóa mã hóa, một khóa giải mã).
- ❖ Bảo mật cao, phù hợp trao đổi dữ liệu trên Internet.
- ❖ Ví dụ: RSA, ECC.

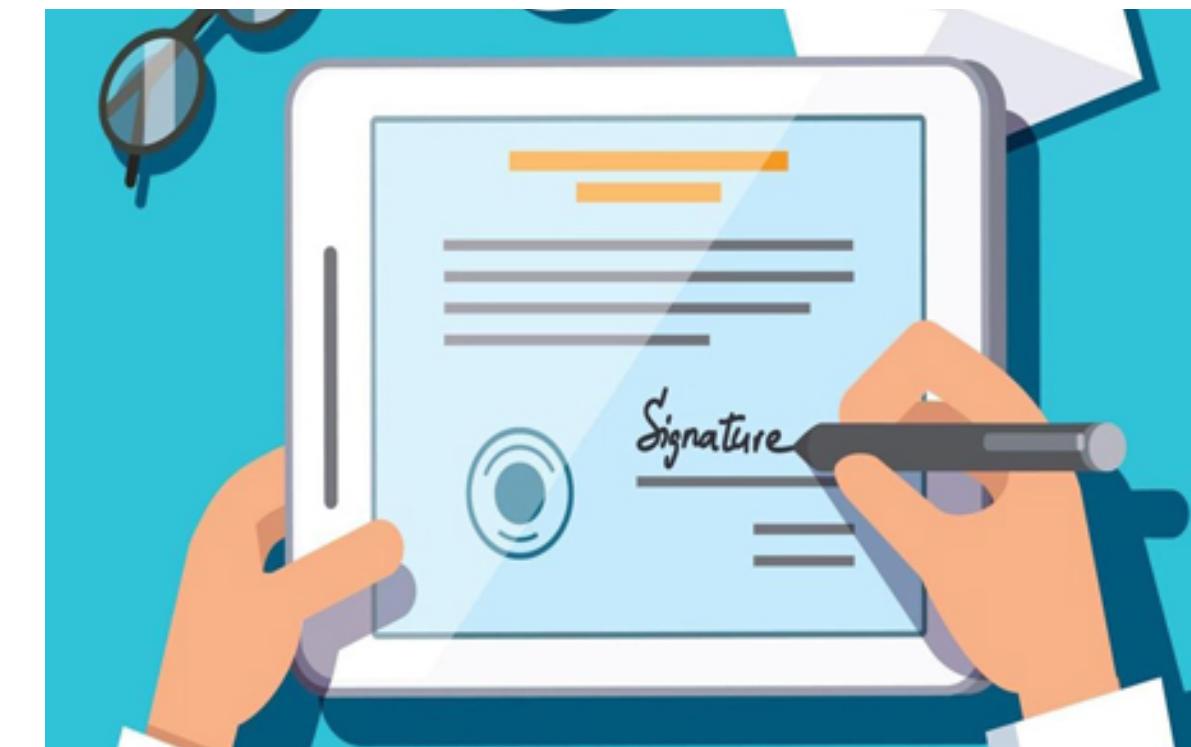
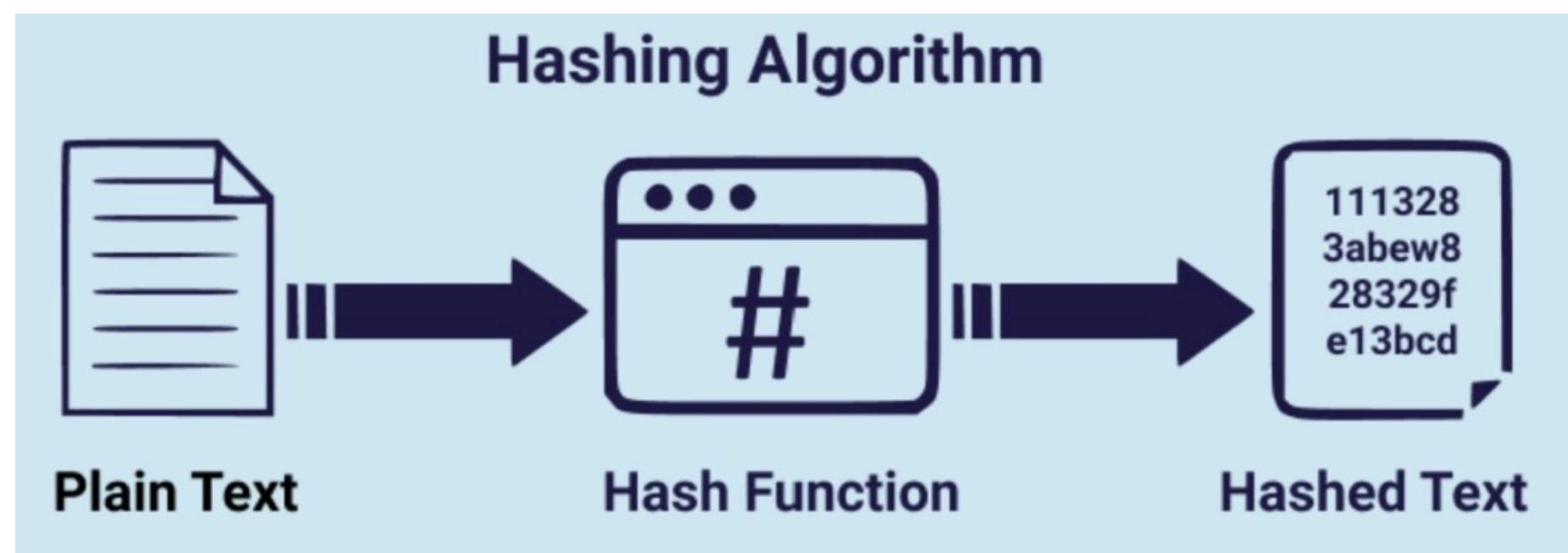


II. Phân loại mã hóa

Kỹ thuật bổ trợ trong bảo mật

HASHING

- Chuyển đổi dữ liệu thành chuỗi mã hóa cố định (hash).
- Không thể đảo ngược, dùng kiểm tra tính toàn vẹn dữ liệu.
- Ví dụ: SHA-256, MD5.



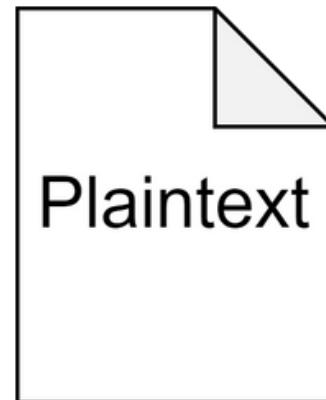
Chữ ký số

- Sử dụng mã hóa bất đối xứng để xác minh nguồn gốc và toàn vẹn dữ liệu.
- Quy trình: Hash dữ liệu → Mã hóa hash bằng khóa riêng → Tạo chữ ký số.
- Giải mã chữ ký bằng khóa công khai để xác minh.
- Ứng dụng: Email, giao dịch trực tuyến.

III. Giải thuật Casear Cipher

Cấu trúc dữ liệu

Input



Plaintext: Chuỗi ký tự cần mã hóa, gồm các ký tự từ bảng chữ cái (A-Z hoặc a-z).

Ví dụ: "HELLO".



Key: Số nguyên đại diện cho số vị trí dịch chuyển.

Ví dụ: $k = 3$.



Output

Ciphertext: Chuỗi ký tự đã được mã hóa bằng cách dịch chuyển từng ký tự trong plaintext theo giá trị của khóa.

Ví dụ: Ciphertext = "KHOOR".

III. Giải thuật Casear Cipher

Hoạt động

Mã hóa

Công thức: $C=P+K \text{ mod } 26$

Trong đó:

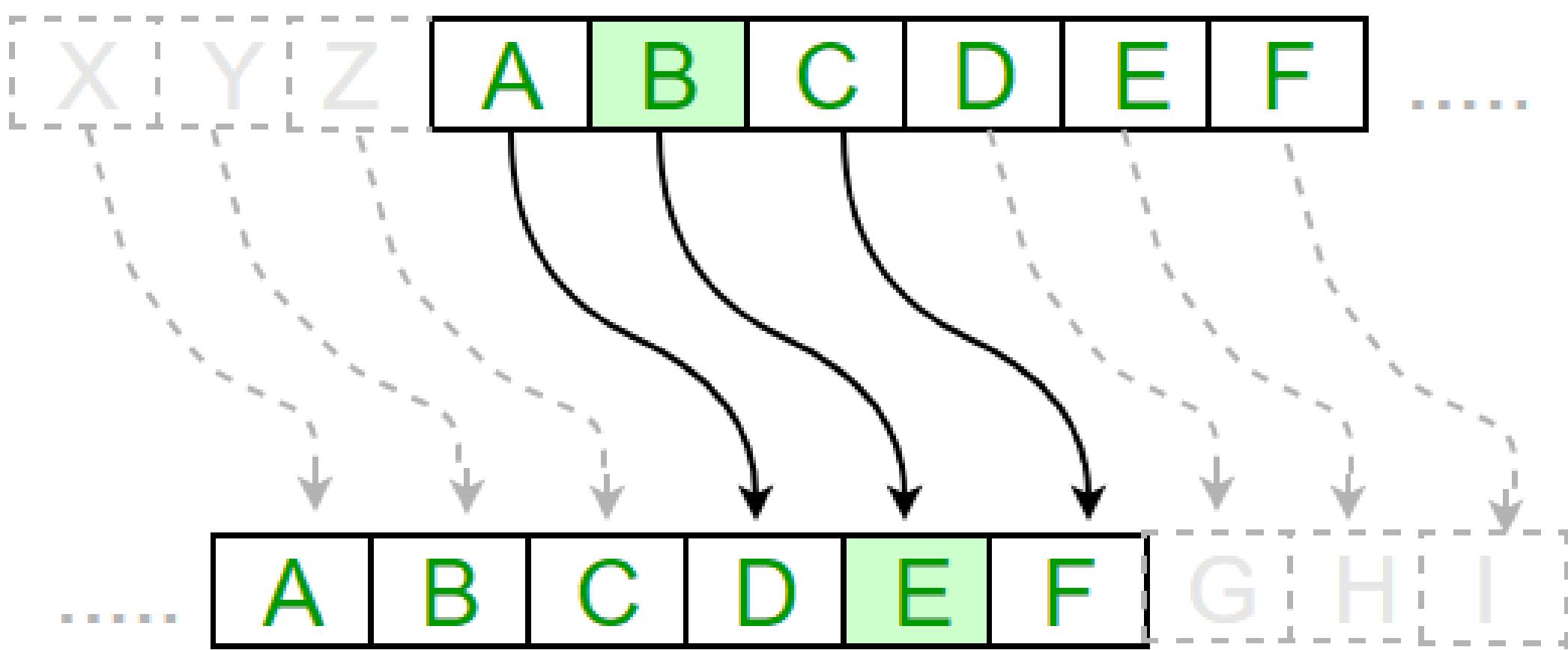
- C là ký tự mã hóa
- P ký tự gốc
- K là số vị trí dịch chuyển

Giải mã

Công thức: $P=C-K \text{ mod } 26$

Độ phức tạp của thuật toán

- Thời gian: $O(n)$, với n là độ dài của chuỗi.
- Không gian: $O(1)$, không yêu cầu bộ nhớ bổ sung ngoài bảng chữ cái (cố định).



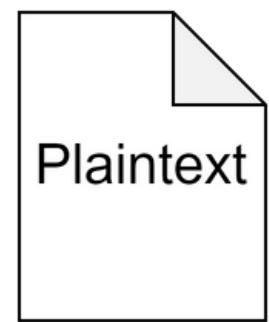
IV. Giải thuật AES

Giới thiệu

AES là thuật toán mã hóa đối xứng được chuẩn hóa bởi NIST vào năm 2001.

Bảo mật cao, hiệu năng tốt, sử dụng rộng rãi trong ngân hàng, mạng, và thương mại điện tử.

Cấu trúc dữ liệu Input



Khối dữ liệu (plaintext): Kích thước cố định 128 bit (16 byte).



Khóa mã hóa: Dài 128, 192, hoặc 256 bit.



Output: Khối dữ liệu đã mã hóa (ciphertext).

Output

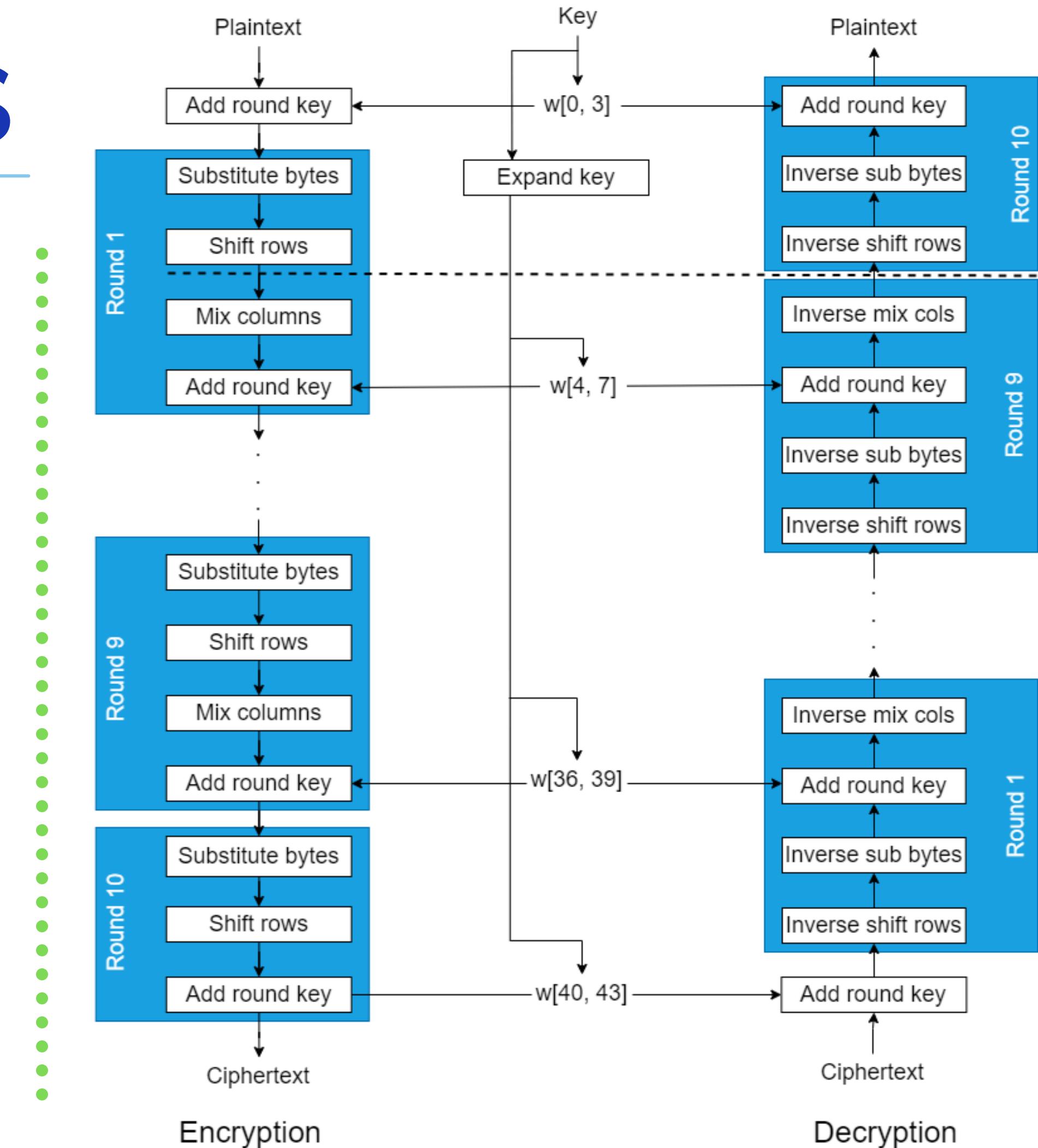
IV. Giải thuật AES

Hoạt động

AES sử dụng cấu trúc Substitution-Permutation Network (SPN), gồm N vòng lặp (10, 12, hoặc 14 vòng tùy độ dài khóa).

Các bước chính trong mỗi vòng:

- **SubBytes:** Thay thế byte trong khối bằng bảng S-box.
- **ShiftRows:** Dịch vòng các hàng trong khối.
- **MixColumns:** Trộn các cột trong khối (trừ vòng cuối).
- **AddRoundKey:** Kết hợp khối dữ liệu với khóa con (bằng XOR).



IV. Giải thuật AES

Hoạt động

Substitute Bytes (Thay thế byte): Thay thế từng byte bằng giá trị từ bảng S-box được công bố ban đầu.

VD : byte có giá trị 30 -> 04

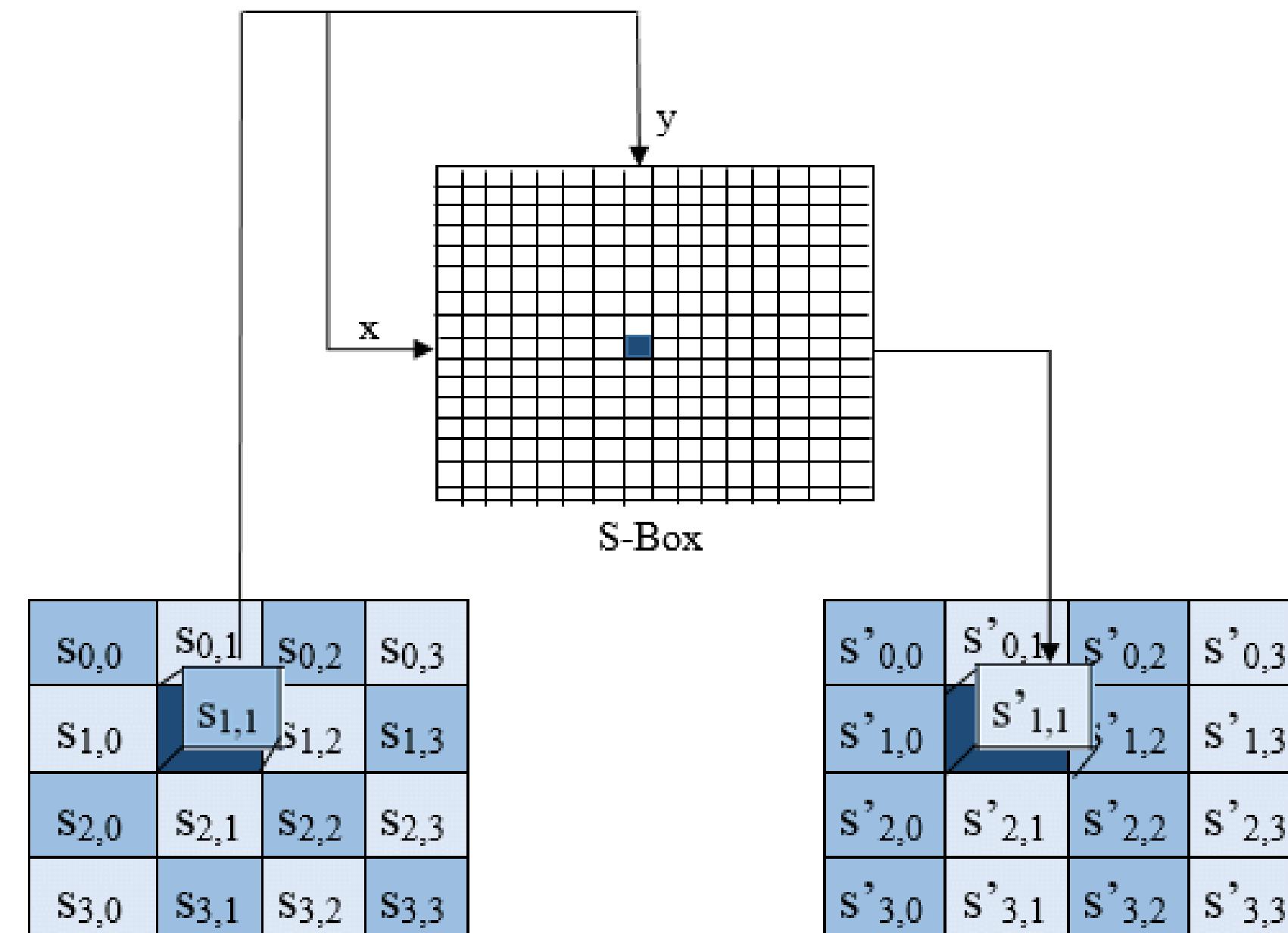
| | | y | | | | | | | | | | | | | | | |
|---|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| | | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |
| x | 0 | 63 | 7C | 77 | 7B | F2 | 6B | 6F | C5 | 30 | 01 | 67 | 2B | FE | D7 | AB | 76 |
| | 1 | CA | 82 | C9 | 7D | FA | 59 | 47 | F0 | AD | D4 | A2 | AF | 9C | A4 | 72 | C0 |
| | 2 | B7 | FD | 93 | 26 | 36 | 3F | F7 | CC | 34 | A5 | E5 | F1 | 71 | D8 | 31 | 15 |
| | 3 | 04 | C7 | 23 | C3 | 18 | 96 | 05 | 9A | 07 | 12 | 80 | E2 | EB | 27 | B2 | 75 |
| | 4 | 09 | 83 | 2C | 1A | 1B | 6E | 5A | A0 | 52 | 3B | D6 | B3 | 29 | E3 | 2F | 84 |
| | 5 | 53 | D1 | 00 | ED | 20 | FC | B1 | 5B | 6A | CB | BE | 39 | 4A | 4C | 58 | CF |
| | 6 | D0 | EF | AA | FB | 43 | 4D | 33 | 85 | 45 | F9 | 02 | 7F | 50 | 3C | 9F | A8 |
| | 7 | 51 | A3 | 40 | 8F | 92 | 9D | 38 | F5 | BC | B6 | DA | 21 | 10 | FF | F3 | D2 |
| | 8 | CD | 0C | 13 | EC | 5F | 97 | 44 | 17 | C4 | A7 | 7E | 3D | 64 | 5D | 19 | 73 |
| | 9 | 60 | 81 | 4F | DC | 22 | 2A | 90 | 88 | 46 | EE | B8 | 14 | DE | 5E | 0B | DB |
| | A | E0 | 32 | 3A | 0A | 49 | 06 | 24 | 5C | C2 | D3 | AC | 62 | 91 | 95 | E4 | 79 |
| | B | E7 | C8 | 37 | 6D | 8D | D5 | 4E | A9 | 6C | 56 | F4 | EA | 65 | 7A | AE | 08 |
| | C | BA | 78 | 25 | 2E | 1C | A6 | B4 | C6 | E8 | DD | 74 | 1F | 4B | BD | 8B | 8A |
| | D | 70 | 3E | B5 | 66 | 48 | 03 | F6 | 0E | 61 | 35 | 57 | B9 | 86 | C1 | 1D | 9E |
| | E | E1 | F8 | 98 | 11 | 69 | D9 | 8E | 94 | 9B | 1E | 87 | E9 | CE | 55 | 28 | DF |
| | F | 8C | A1 | 89 | 0D | BF | E6 | 42 | 68 | 41 | 99 | 2D | 0F | B0 | 54 | BB | 16 |

Bảng S-box

IV. Giải thuật AES

Hoạt động

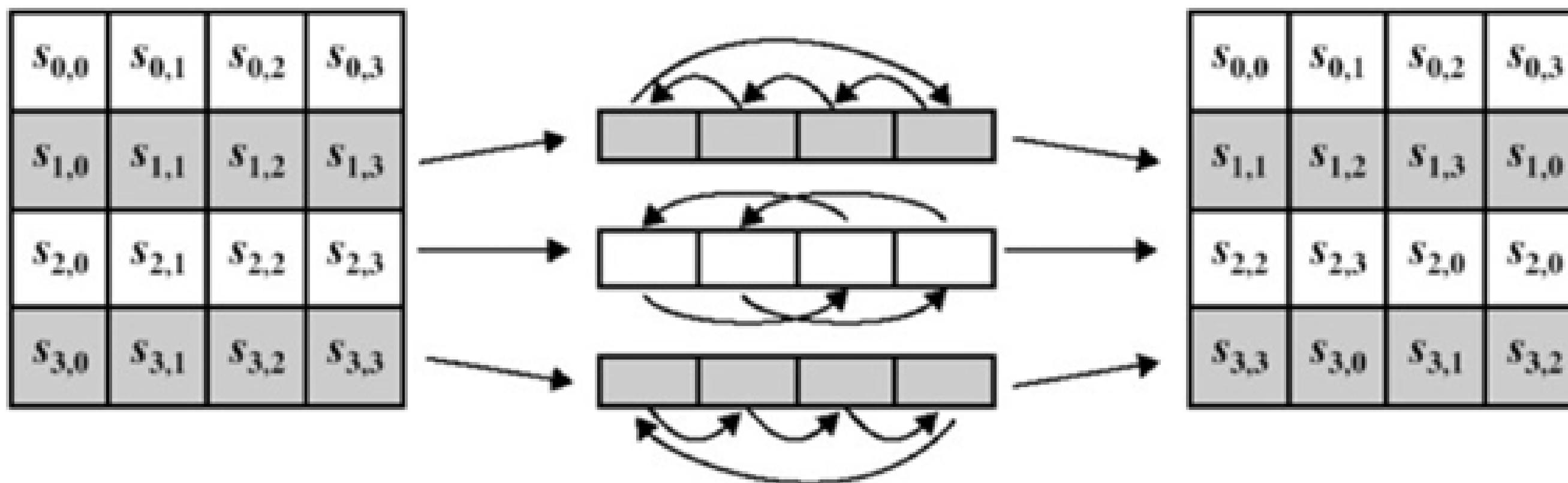
Substitute Bytes (Thay thế byte): Thay thế từng byte bằng giá trị từ bảng S-box.



IV. Giải thuật AES

Hoạt động

Shift Rows (Dịch hàng): Dịch vòng các hàng trong ma trận trạng thái.



IV. Giải thuật AES

Hoạt động

MixColumns, thực chất là một phép thay thế nhưng sử dụng phép toán đại số trong trường hữu hạn $GF(2^8)$.

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} s_{0,0} & s_{0,1} & s_{0,2} & s_{0,3} \\ s_{1,0} & s_{1,1} & s_{1,2} & s_{1,3} \\ s_{2,0} & s_{2,1} & s_{2,2} & s_{2,3} \\ s_{3,0} & s_{3,1} & s_{3,2} & s_{3,3} \end{bmatrix} = \begin{bmatrix} s'_{0,0} & s'_{0,1} & s'_{0,2} & s'_{0,3} \\ s'_{1,0} & s'_{1,1} & s'_{1,2} & s'_{1,3} \\ s'_{2,0} & s'_{2,1} & s'_{2,2} & s'_{2,3} \\ s'_{3,0} & s'_{3,1} & s'_{3,2} & s'_{3,3} \end{bmatrix}$$

Ví dụ phép nhân trong trường $GF(2^8)$:

$$02 * 30 \Leftrightarrow 0000\ 0010 * 0011\ 0000$$

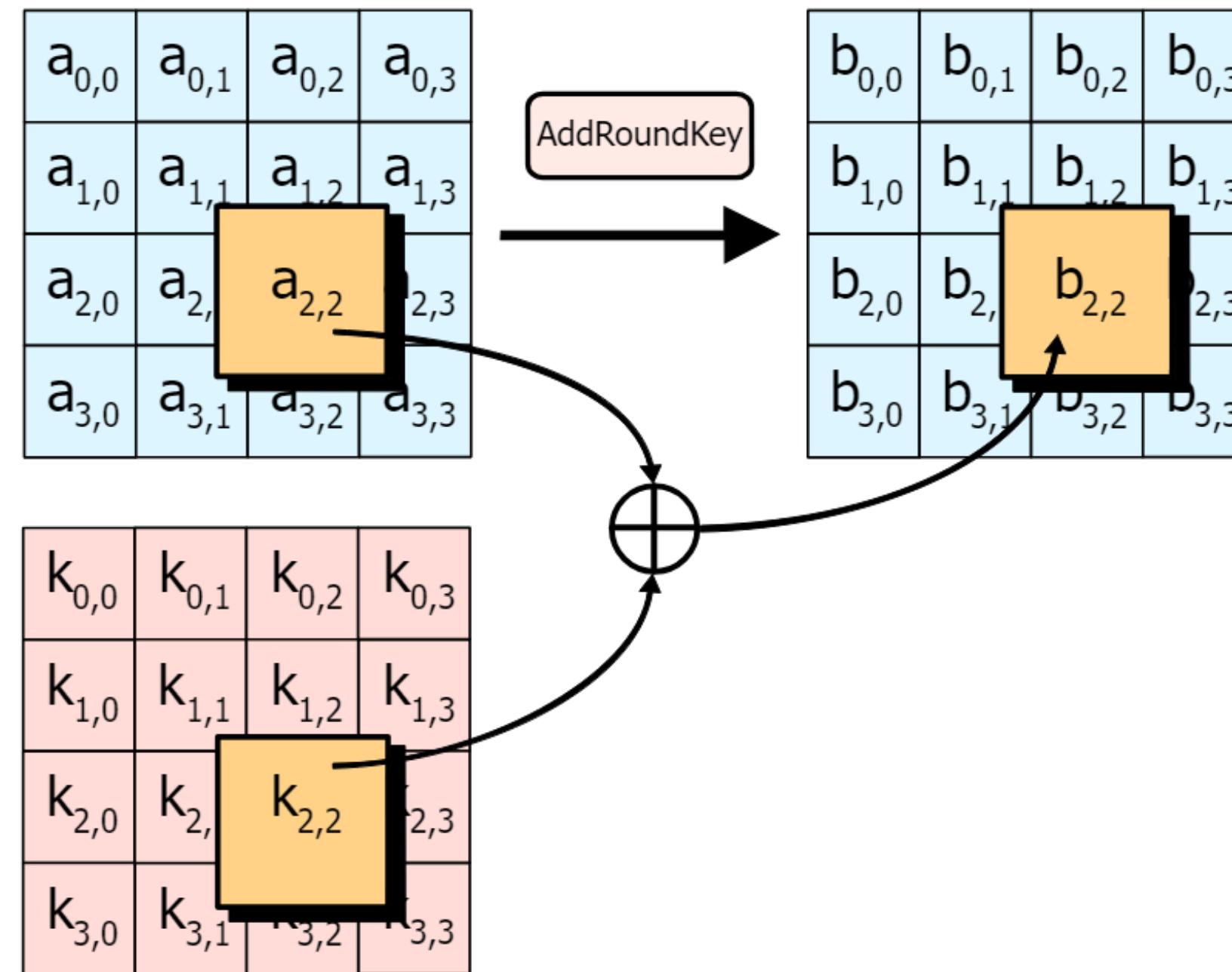
$$f(x) = x, g(x) = x^5 + x^4$$

$$f(x) * g(x) = x^6 + x^5 = 0110\ 0000 = 60$$

IV. Giải thuật AES

Hoạt động

AddRoundKey: Kết hợp khối dữ liệu với khóa con (bằng XOR).



IV. Giải thuật AES

Mở rộng khóa

RotWord

Dịch vòng $W[i-1]$ theo byte (byte đầu tiên trở thành byte cuối cùng).

SubBytes

Thay thế từng byte bằng giá trị trong S-box.

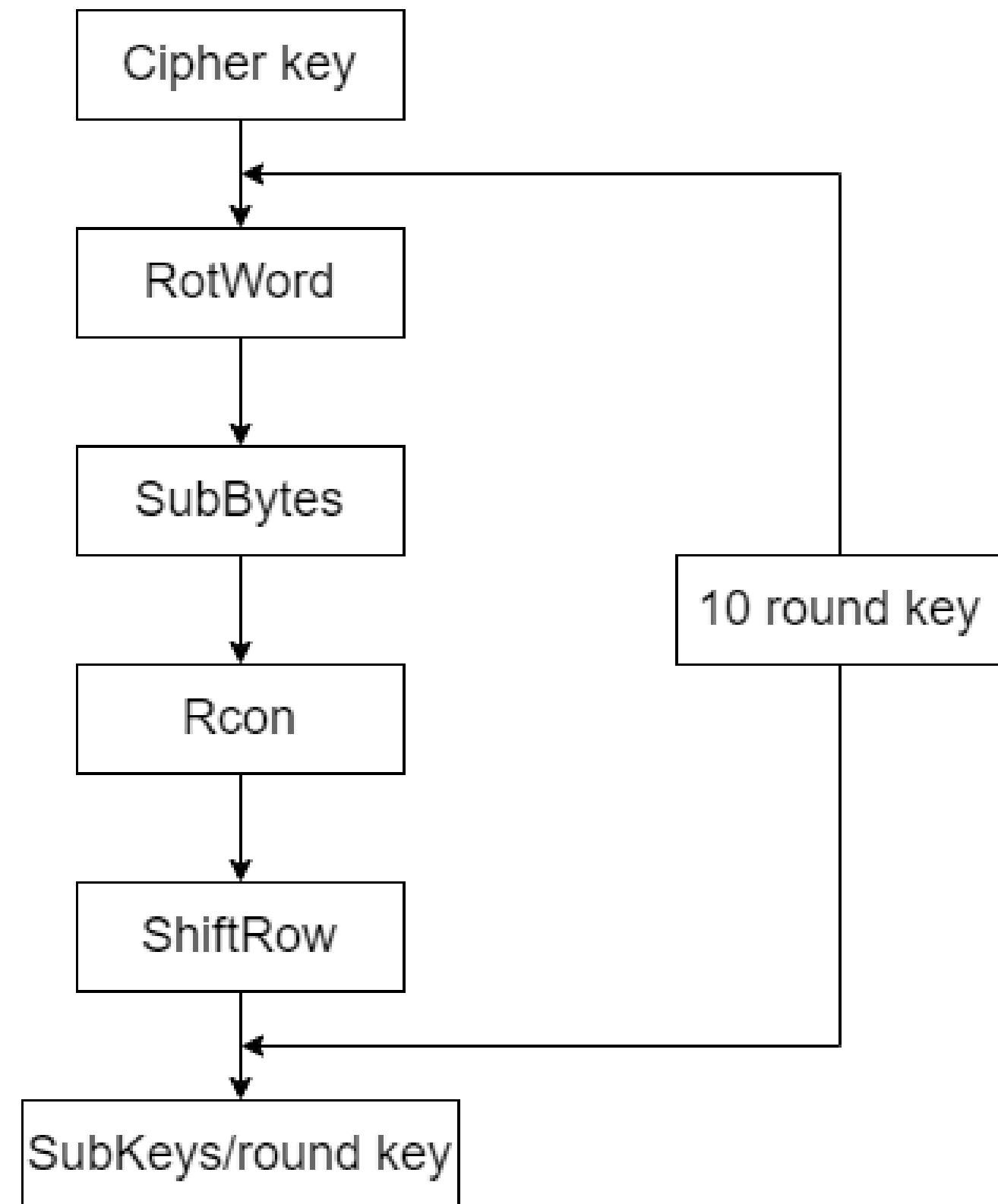
Rcon

$$Rcon[j] = (RC[j], 0, 0, 0)$$

$$RC[1] = 1, RC[j] = 2 \cdot RC[j-1],$$

ShiftRow

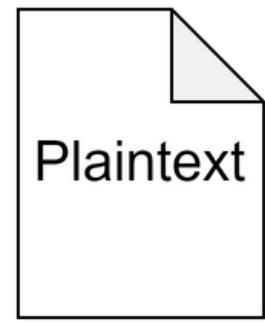
Dịch bước tương ứng theo hàng



V. Giải thuật RSA

Cấu trúc dữ liệu

Input



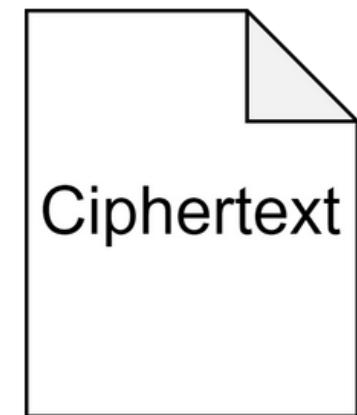
Plaintext: Chuỗi ký tự cần mã hóa, gồm các ký tự trong bảng mã ASCII, thực hiện mã hóa từng ký tự trong chuỗi.



Public key: Khóa công khai để mã hóa



Private key: Khóa bí mật để giải mã



Output

Ciphertext: Chuỗi ký tự đã được mã hóa bằng cách thực hiện các quy trình tính toán thông qua các vòng lặp. Đầu ra là một chuỗi mã hóa

V. Giải thuật RSA

Hoạt động

Giới thiệu

Dựa trên bài toán tìm bộ 3 số tự nhiên e, d, n thỏa mãn :

$$m^e \text{ mod } n = m^d \text{ mod } n$$



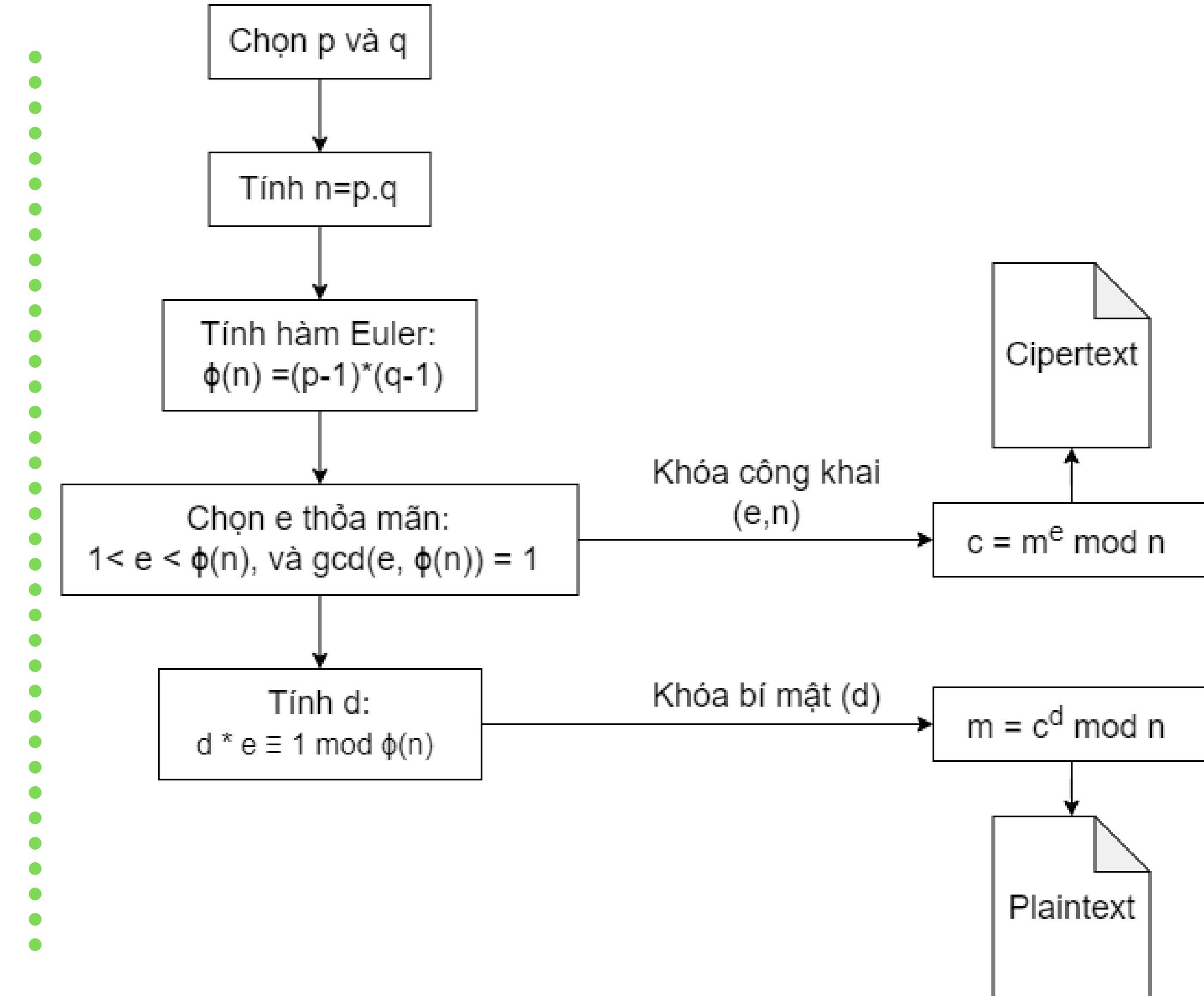
Bao gồm 3 quy trình xử lý

- Tạo cặp khóa công khai và khóa riêng dựa trên hai số nguyên tố lớn.
- Mã hóa bằng khóa công khai.
- Giải mã ciphertext để khôi phục dữ liệu gốc bằng khóa riêng.

V. Giải thuật RSA

Hoạt động

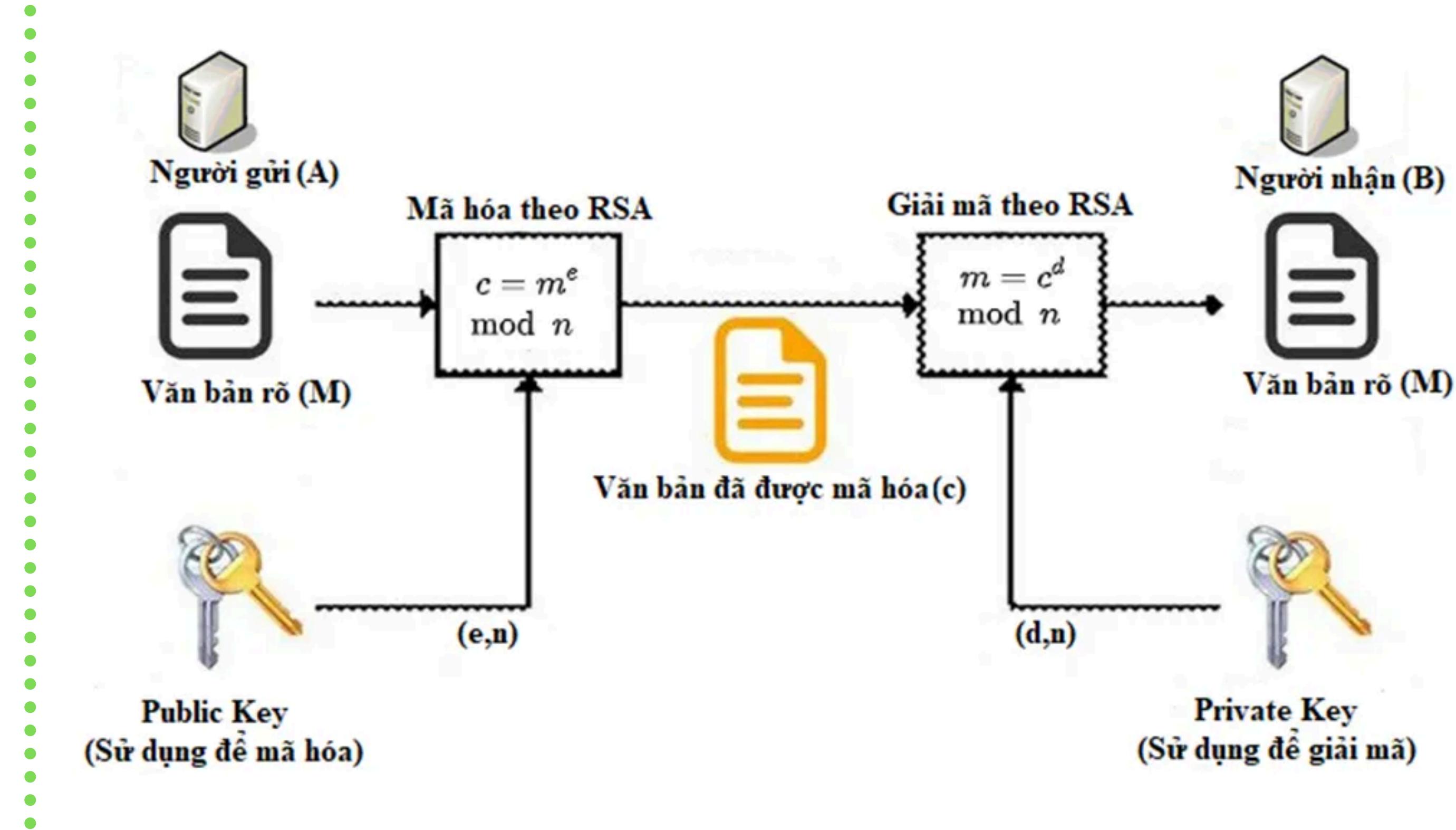
Quá trình tạo khóa: Tạo cặp khóa công khai và khóa riêng dựa trên hai số nguyên tố lớn.



V. Giải thuật RSA

Hoạt động

- **Encryption (Mã hóa):**
Mã hóa dữ liệu gốc thành ciphertext bằng khóa công khai.
- **Decryption (Giải mã):**
Giải mã ciphertext để khôi phục dữ liệu gốc bằng khóa riêng.



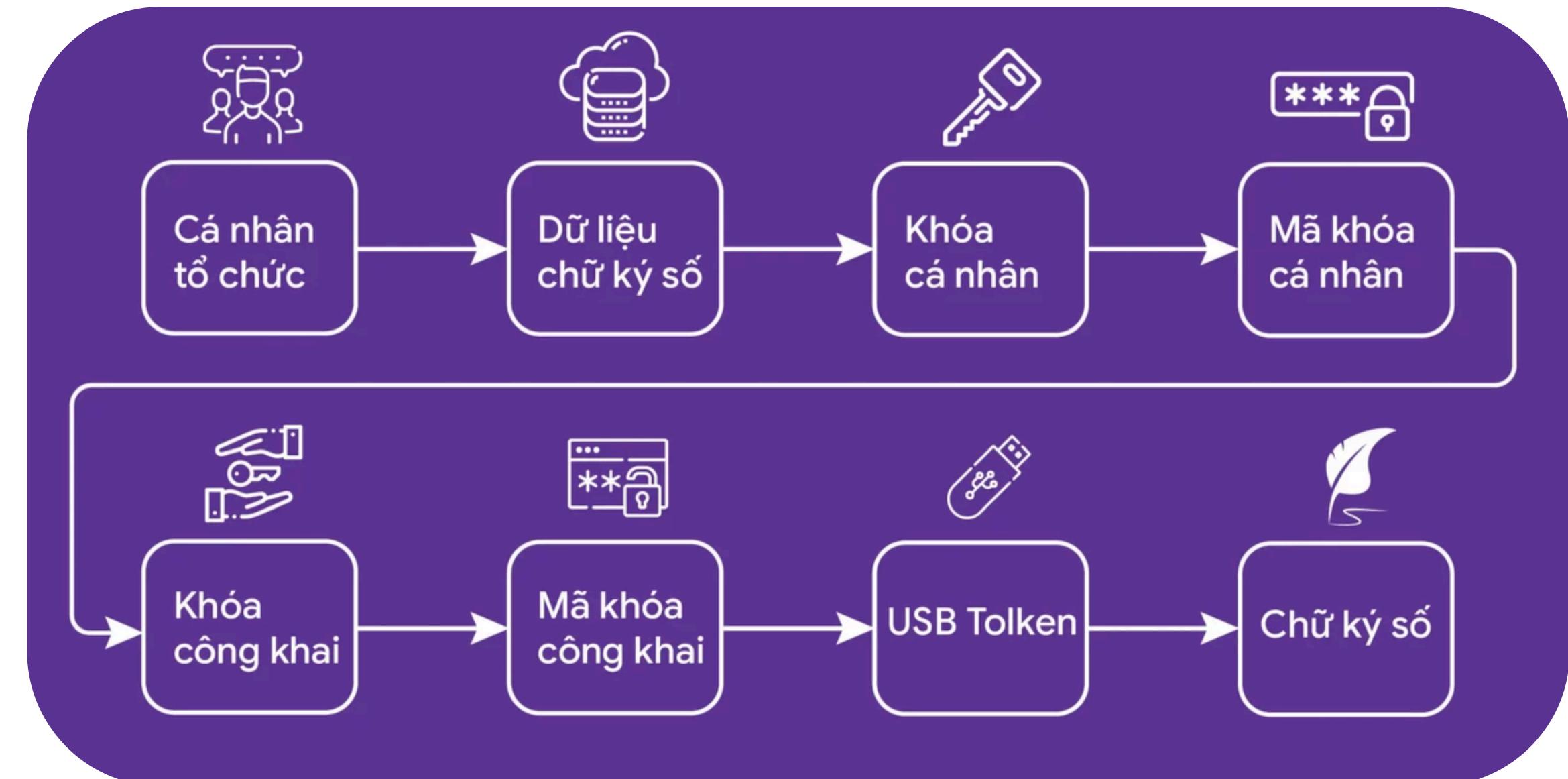
V. Giải thuật RSA

Độ phức tạp của thuật toán

- Thời gian: Mã hóa/Giải mã: $O(k^3)$, với k là số bit của khóa (thường từ 1024 đến 4096 bit).
- Không gian: $O(k)$, vì cần lưu trữ các số lớn như khóa công khai, khóa riêng, và các thông điệp mã hóa.

Ứng dụng

- Chữ ký số
- Bảo mật kết nối trên web, email, VPN và các ứng dụng chat
- Giao thức TLS/SSL



VI. Giải thuật SHA256

Giới thiệu

- SHA-256 là một thuật toán băm thuộc họ SHA-2, được thiết kế bởi NSA và chuẩn hóa bởi NIST.
- Kết quả là một chuỗi băm cố định dài 256 bit (32 byte), bất kể kích thước input.
- Thường được dùng trong chữ ký số, chứng chỉ SSL/TLS, và blockchain.

Cấu trúc dữ liệu

- Input: Chuỗi dữ liệu bất kỳ
- Output: Chuỗi băm dài 256 bit (hexadecimal gồm 64 ký tự).

VI. Giải thuật SHA256

Độ phức tạp của thuật toán

- Thời gian: $O(n)$, với n là số bit của thông điệp đầu vào.
- Không gian: $O(1)$, vì chỉ cần một lượng không gian cố định để lưu trữ các giá trị tạm thời (256 bit) và lịch trình thông điệp.

VI. Giải thuật SHA256

Hoạt động

Convert to Binary:
Chuyển thông điệp gốc
thành dạng mã nhị
phân để xử lý dễ dàng.

Input Message: hello123

Step 1: Convert characters to binary

Character: '3' ASCII: 51

Binary conversion:

Step 1: $51 \div 2 = 25$ remainder 0
Step 2: $25 \div 2 = 12$ remainder 0
Step 3: $12 \div 2 = 6$ remainder 0
Step 4: $6 \div 2 = 3$ remainder 0
Step 5: $3 \div 2 = 1$ remainder 0
Step 6: $1 \div 2 = 0$ remainder 0
Step 7: $0 \div 2 = 0$ remainder 0
Step 8: $0 \div 2 = 0$ remainder 0

Final binary: 00110011

Converted results:

'h' = 01101000
'e' = 01100101
'l' = 01101100
'l' = 01101100
'o' = 01101111
'1' = 00110001
'2' = 00110010

SHA-256 Algorithm Visualization

VI. Giải thuật SHA256

Hoạt động

Padding (Đệm dữ liệu): Bổ sung các bit để độ dài của thông điệp là bội số của 512 bit, bao gồm cả bit biểu diễn độ dài thông điệp ban đầu.

Step 2: Padding

Add 'T' bit

01101000011001010110110001101100011011110011000100110010001100111

Add '0' padding:

Add message length (64 bits):

VI. Giải thuật SHA256

Hoạt động

Message Scheduling (Lập lịch thông điệp): Chia thông điệp đã đệm thành các khối 512 bit và chuẩn bị các khối con 32 bit theo lịch trình cụ thể.

[Step 3: Split into 512-bit blocks](#)

Block 1: 01101000011001010110110001101100...000000000000000000000000001000000 (512 bits)

VI. Giải thuật SHA256

Hoạt động

Compression (Nén): Thực hiện các phép toán logic (AND, OR, XOR, dịch bit, cộng) trên các khối, kết hợp với các hằng số cố định, để nén thông điệp từng vòng.

SHA-256 Algorithm Visualization

Input Message: hello123

Step 3: Split into 512-bit blocks
Block 1: 01101000011001010110110001101100...00000000000000000000000000000000 (512 bits)

Step 4: Message Schedule (W Array)

W48: 5e43153a
W49: cfbb3ac9
W50: c6f4651e
W51: e7a9f98e
W52: 08f3ffef
W53: 4f20631e
W54: 170d74ce
W55: ab253f8d
W56: 24a94bbe
W57: 036c62b9
W58: 10227b17
W59: 3b122cf5
W60: cd337141
W61: faabd3c4
W62: 49c892d1
W63: 6068b10d

$\sigma_0(x) = (x \gg 7) \oplus (x \gg 18) \oplus (x \gg 3)$
 $\sigma_1(x) = (x \gg 17) \oplus (x \gg 19) \oplus (x \gg 10)$

K Constants:

K48: 19a4c116
K49: 1e376c08
K50: 2748774c
K51: 34b0bcb5
K52: 391c0cb3
K53: 4ed8aa4a
K54: 5b9cca4f
K55: 682e6ff3
K56: 748f82ee
K57: 78a5636f
K58: 84c87814
K59: 8cc70208
K60: 90beffa
K61: a4506ceb
K62: bef9a3f7
K63: c67178f2

Calculating W63:

$$\begin{aligned} W63 &= \sigma_1(W61) + W56 + \sigma_0(W48) + W47 \\ &= \sigma_1(faabbd3c4) + 24a94bbe + \sigma_0(5e43153a) + ede0a93e \\ &= 6068b10d \end{aligned}$$

VI. Giải thuật SHA256

Hoạt động

Finalization (Hoàn tất): Kết hợp giá trị nén cuối cùng từ các vòng lặp để tạo ra chuỗi băm 256 bit duy nhất đại diện cho thông điệp.

SHA-256 Algorithm Visualization

Input Message: hello123

Step 5: Final Hash Computation

Initial Hash Values (a b c d e f g h):

a: 6a09e667 b: bb67ae85 c: 3c6ef372 d: a54ff53a e: 510e527f f: 9b05688c g: 1f83d9ab h: 5be0cd19

Round 64 Calculations

$Ch(e, f | g) = (e \wedge f) \oplus (\neg e \wedge g)$

$Maj(a, b, c) = (a \wedge b) \oplus (a \wedge c) \oplus (b \wedge c)$

$\Sigma_0(a) = (a \gg 2) \oplus (a \gg 13) \oplus (a \gg 22)$

$\Sigma_1(e) = (e \gg 6) \oplus (e \gg 11) \oplus (e \gg 25)$

$T_1 = h + \Sigma_1(e) + Ch(e, f | g) + K63 + W63$

$T_2 = \Sigma_0(a) + Maj(a, b, c)$

$Ch(e, f | g) = (fb5c4199 \wedge 6b58f8a0) \oplus (\neg fb5c4199 \wedge 4a4d3708) = 6b597680$

$Maj(a, b, c) = (bdc2832d \wedge 40b45349) \oplus (bdc2832d \wedge 29ead34b) \oplus (40b45349 \wedge 29ead34b) = 29e2d349$

$\Sigma_0(a) = (bdc2832d \gg 2) \oplus (bdc2832d \gg 13) \oplus (bdc2832d \gg 22) = 7c11f828$

$\Sigma_1(e) = (fb5c4199 \gg 6) \oplus (fb5c4199 \gg 11) \oplus (fb5c4199 \gg 25) =faf2d673$

$T_1 = 9bd05271 + faf2d673 + 6b597680 + c67178f2 + 6068b10d = 809f7b70$

$T_2 = 7c11f828 + 29e2d349 = 3d2307bd$

Updates: $h=g, g=f, f=e, e=d+T_1, d=c, c=b, b=a, a=T_1+T_2$

Updated Values:

a: bdc2832d, b: 40b45349, c: 29ead34b, d: 3759c162, e: fb5c4199, f: 6b58f8a0, g: 4a4d3708, h: 9bd05271

Final Hash Values:

a: 27cc6994 b: fc1c01ce c: 6659c6bd d: dca9b69c e: 4c6a9418 f: 065e612c g: 69d110b3 h: f7b11f8a

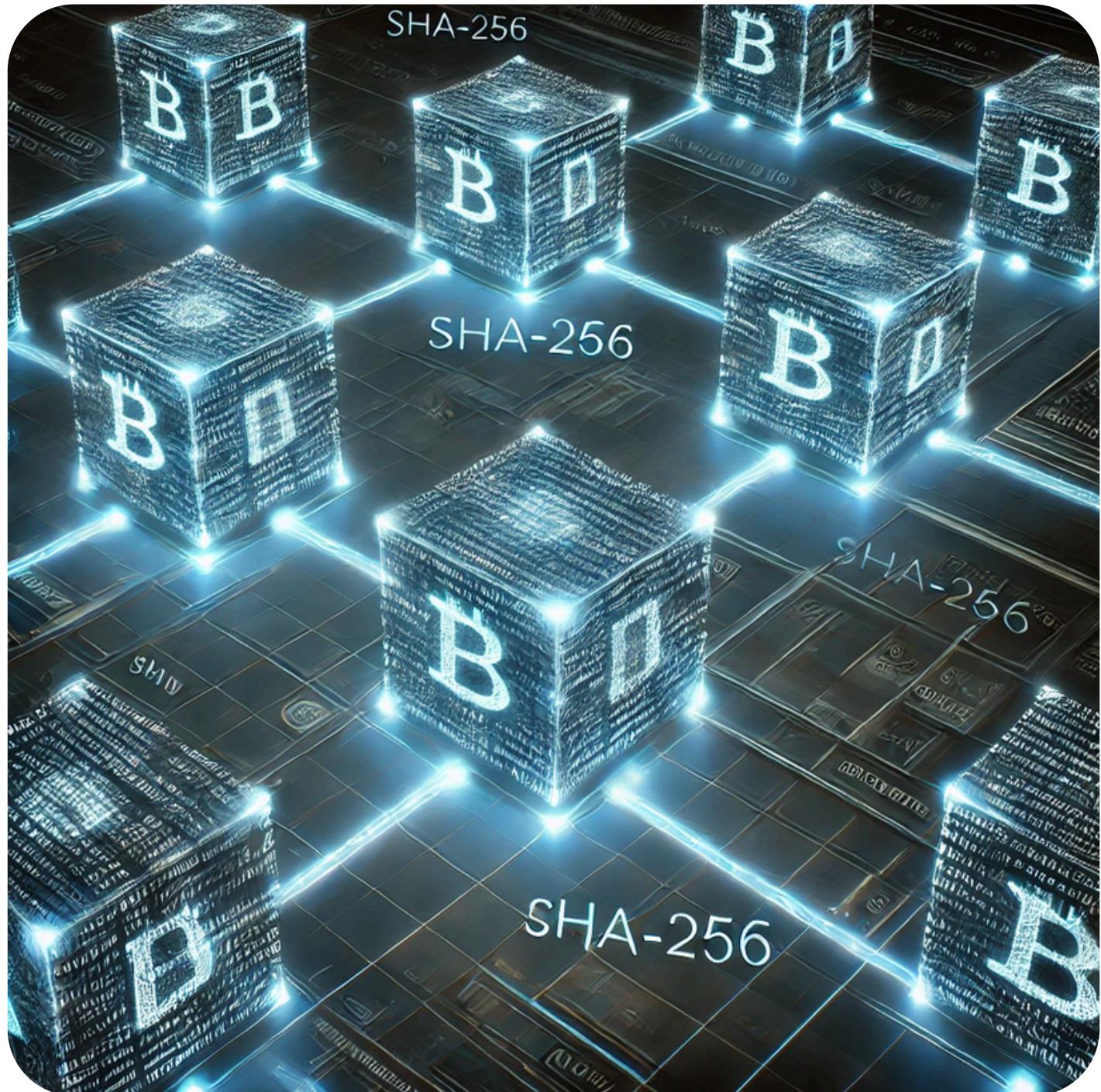
Final Hash: 27cc6994fc1c01ce6659c6bddca9b69c4c6a9418065e612c69d110b3f7b11f8a

SHA-256 Result: 27cc6994fc1c01ce6659c6bddca9b69c4c6a9418065e612c69d110b3f7b11f8a

VI. Giải thuật SHA256

Ứng dụng

- Xác minh tính toàn vẹn dữ liệu
- Bảo mật trong Blockchain
- Lưu trữ mật khẩu
- Chữ ký số và chứng thực
- Mã hóa trong chứng chỉ số (SSL/TLS)
- Hệ thống tiền điện tử
- Bảo vệ dữ liệu trong hệ thống lưu trữ



VII. Mô phỏng

Giải thuật Casear Cipher

Giải thuật SHA-256

Giải thuật RSA

Giải thuật AES

Mã hóa File

VIII. Tài liệu tham khảo

- [1] Pandya, Dwiti, et al. "Brief history of encryption." *International Journal of Computer Applications* 131.9 (2015): 28-31.
- [2] Yu, Lili, Zhijuan Wang, and Weifeng Wang. "The application of hybrid encryption algorithm in software security." *2012 Fourth International Conference on Computational Intelligence and Communication Networks*. IEEE, 2012.
- [3] Buchmann, Johannes, Erik Dahmen, and Michael Szydlo. "Hash-based digital signature schemes." *Post-quantum cryptography*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009. 35-93.
- [4] Kaur, Ravneet, and Amandeep Kaur. "Digital signature." *2012 International Conference on Computing Sciences*. IEEE, 2012.
- [5] National Institute of Standards and Technology (NIST), "FIPS PUB 197: Advanced Encryption Standard (AES)," updated January 2019. [Online]. Available: <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197-upd1.pdf>

THANKS FOR WATCHING