

AN INFORMATION GUIDE FOR

**CCMP**

**AES ENCRYPTION**

A walkthrough for every concepts in CCMP



# Nội dung

Key topics

— CCMP Basics

— AES Encryption

— CBC - MAC

— CTR

# Định nghĩa của CCMP

- AES-CCMP (128-bit AES-counter mode with CBC-MAC Protocol) là giao thức sử dụng thuật toán mã hóa block cipher AES 128-bit .
- Phức tạp và an toàn hơn, thay thế phương thức RC4 stream cipher ở WEP, TKIP trong WPA.
- Được áp dụng ở chuẩn WP2.



# Long term solution

Dựa trên thuật toán  
mã hóa hiện đại  
nhất

---

Tương thích với  
802.11

---

Có khả năng mở  
rộng, cho phép cấu  
hình với bất cứ  
block cipher nào

---





# Security Goals

Prevent Frame  
Forgeries

---

Prevent Replay  
Attack

---

Never reuse keys

---



# Các bước mã hóa AES 128

## BƯỚC 3

---

### Byte Substitution

Sử dụng S-Box để hoán đổi vị trí byte của block

## BƯỚC 1

---

### Key Expansion

Tạo 10 RoundKey, có thể thay đổi theo số bit đầu vào (10 Key)

## BƯỚC 4

---

### Shift Rows

Dịch trái mỗi 4 byte

## BƯỚC 2

---

### XOR dữ liệu

XOR plaintext với lần lượt 10 key tạo ra từ Bước 1

## BƯỚC 5

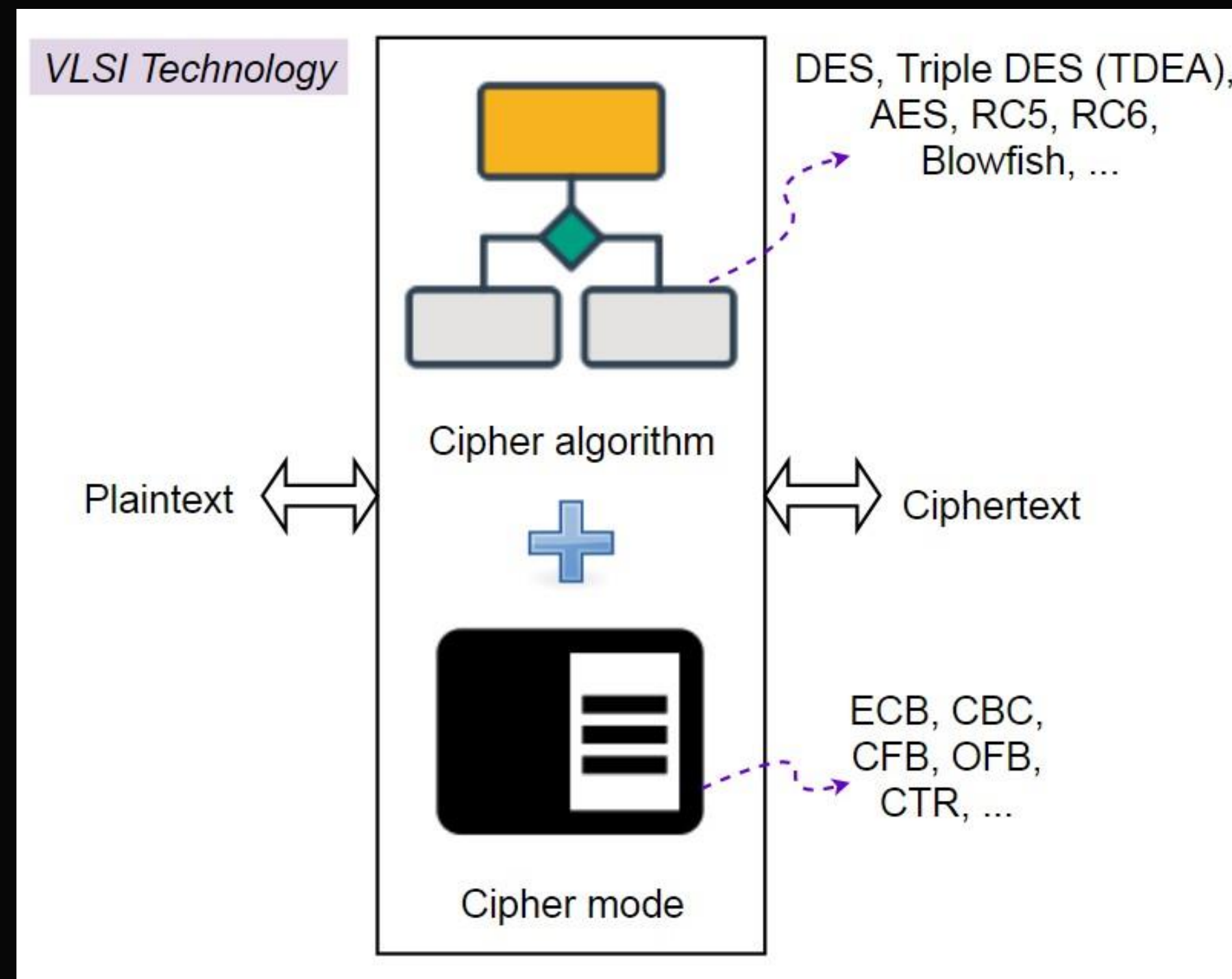
---

### Mix Columns

Nhân với một ma trận khả nghịch tạo thành một ma trận mới (4x4). Sau đó lặp lại từ bước 1

# Khái niệm Mode của AES

Khi cài đặt thuật toán mã AES người ta thường không sử dụng ở dạng nguyên gốc. AES thường hoạt động ở 5 chế độ cơ bản của mã khối n-bit (ECB, CBC, CFB, OFB và CTR)



# Phương pháp của CCMP



CTR Mode

Mã hóa dữ liệu



CBC - MAC

Xác thực và Toàn vẹn



$\text{CTR} + \text{CBC-MAC} = \text{CCM}$



# CBC-MAC

cipher block chaining message  
authentication code



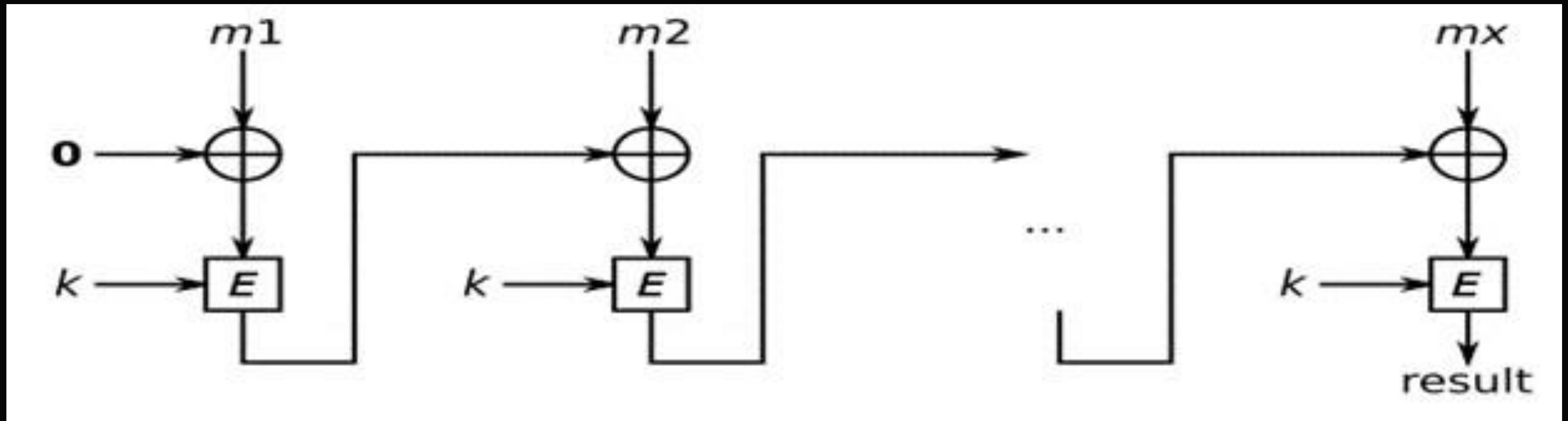
# Định nghĩa

CBC - MAC sẽ được tạo ra sử dụng AES với CBC mode để tạo thành một chuỗi các khối mà khối phía sau sẽ dựa trên khối phía trước, nó đảm bảo kẻ tấn công sẽ không thể đoán được dữ liệu nếu không có khóa.  
CCMP sử dụng CBC-MAC để tính toán MIC trên header gồm chiều dài và dữ liệu.



# Cách tính CBC - MAC

Để tính toán MAC của message  $m$ , ta mã hóa  $m$  với CBC mode, dùng Zero - IV và giữ lại Block cuối cùng





# Counter (CTR) Mode



# Counter?

- Counter có thể là bất kỳ hàm (Function) nào tạo ra một chuỗi được đảm bảo không lặp lại trong một thời gian dài
- Counter tăng dần 1 đơn vị là đơn giản nhất và phổ biến nhất.





# Nonce?

- Nonce là một số tùy ý chỉ được sử dụng một lần.
- Chúng thường là các số ngẫu nhiên hoặc giả ngẫu nhiên.



# Counter Mode (CTR)



- CTR được sử dụng để mã hóa dữ liệu và MIC (CBC - MAC) trong CCMP.
- Dữ liệu được mã hóa và giải mã bởi việc XOR với khóa được tạo bởi AES.

# Ưu điểm của CTR

ƯU ĐIỂM	
✓	Có thể chạy song song, nó phù hợp máy có thể chạy nhiều tiến trình một lúc
✓	Chỉ có thể giải mã khi và chỉ khi gói tin đã đến và nonce nó được gắn vào gói tin
✓	Cung cấp tính bảo mật rất cao nếu dùng đúng cách
✓	Nên được trao đổi khóa giữa hai bên liên tục
✓	Kết hợp với một thuật toán xác thực là cần thiết ví dụ: HMAC-SHA-1-96

# Hạn chế của CTR

HẠN CHẾ VÀ NHỮNG ĐIỀU CẦN LƯU Ý	
	Key kết hợp phải là duy nhất
	Người nhận sẽ không thể giải mã gói tin nếu gói tin chưa đến
	Sẽ là thảm họa nếu IV bị trùng, thì lập tức thông tin của plaintext bị lộ
	Không nên được sử dụng với khóa tĩnh
	Kẻ tấn công có thể gửi những nội dung giả mạo

# Phương pháp Counter Mode

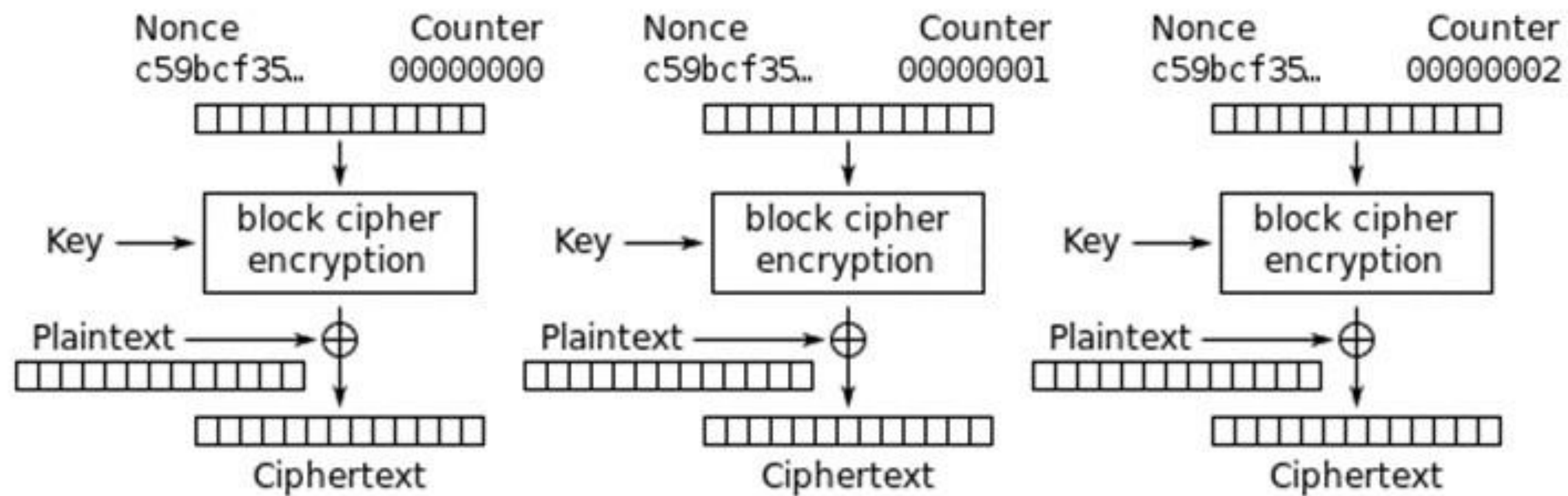
- AES-CTR sẽ thực hiện mã hóa bằng cách XOR 128-bit của block plaintext với 128-bit CTR bao gồm:
  - NONCE 32-bit đầu.
  - 64-bit tiếp theo là IV.
  - 32-bit cuối cùng sẽ được bật hết lên 1.
- Sau mỗi block thì 128-bit này sẽ cộng 1.
- Ở khối cuối cùng, hàm TRUNC() sẽ làm cho khối luôn là 128-bit.

```
PT = PT[1] PT[2] ... PT[n]

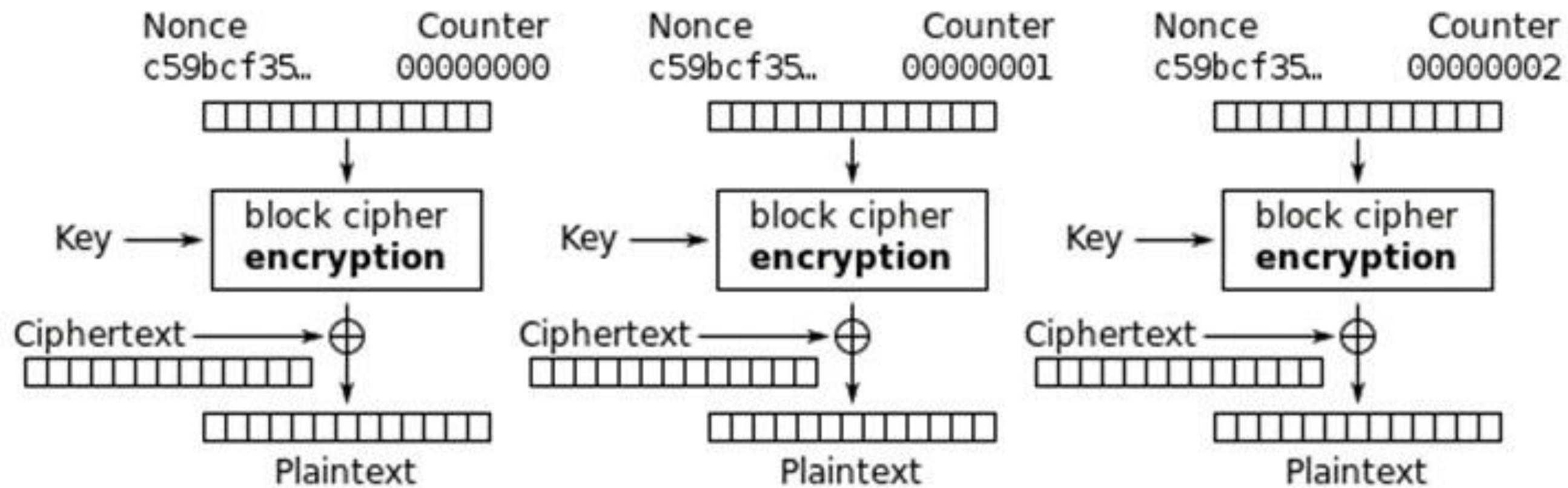
CTRBK := NONCE || IV || ONE
FOR i := 1 to n-1 DO
    CT[i] := PT[i] XOR AES(CTRBK)
    CTRBK := CTRBK + 1
END
CT[n] := PT[n] XOR TRUNC(AES(CTRBK))
```

- Đặc biệt ở AES-CTR, chúng ta không cần padding độ dài block vì 128-bit được sinh từ NONCE, IV và ONE luôn là 128.
- => Giới hạn chỉ là  $2^{31}-1$  blocks = 4,294,967,295 blocks.





Counter (CTR) mode encryption



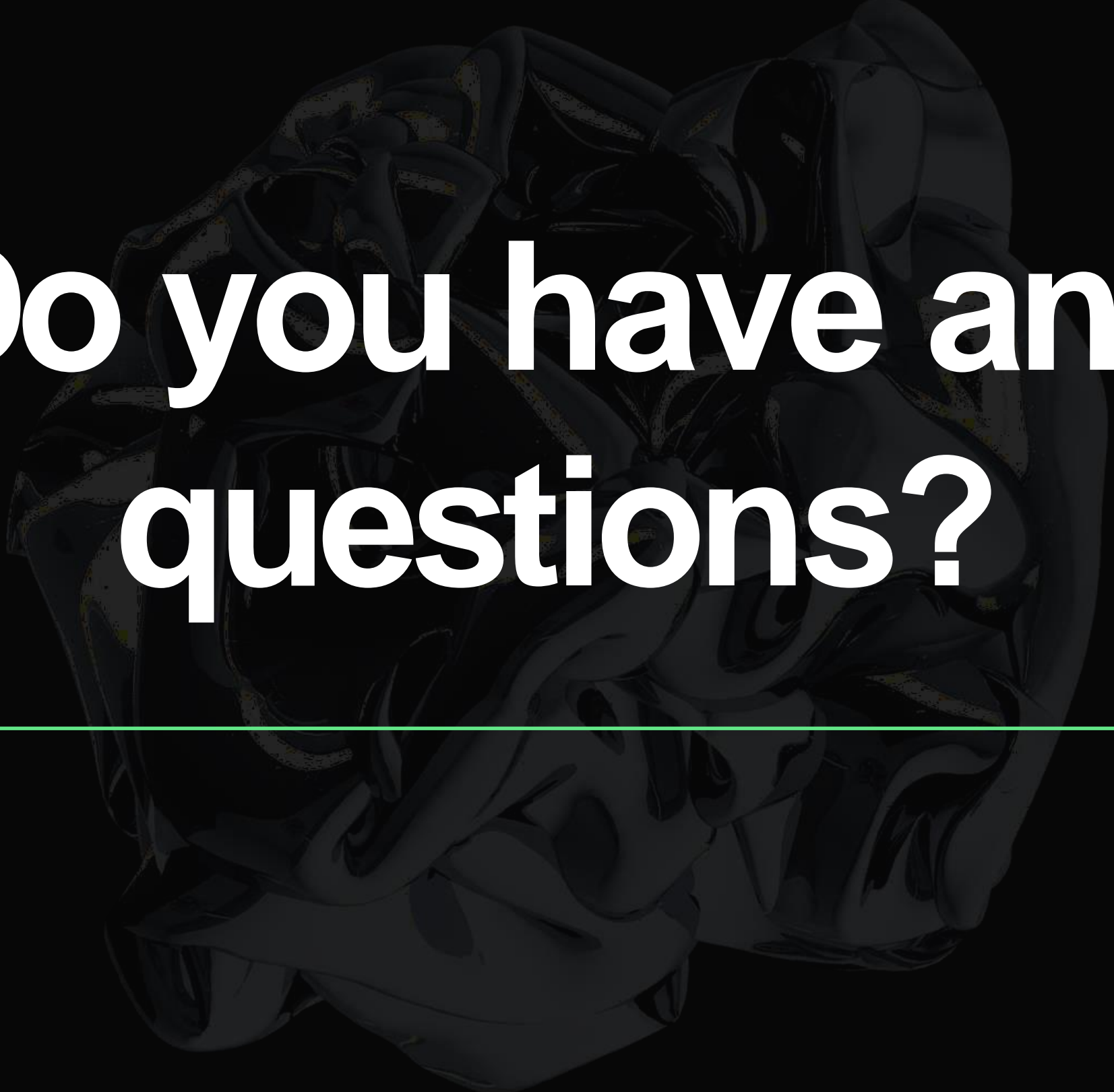


Counter (CTR) mode decryption

# So sánh CCMP

Data Protection Protocol Comparison			
	<u>WEP</u>	<u>TKIP</u>	<u>CCMP</u>
<i>Cipher</i>	RC4	RC4	AES
<i>Key Size</i>	40 or 104 bits	128 bits	128 bits
<i>Key Life</i>	24-bit IV, wrap	48-bit IV 48-bit IV	
<i>Packet Key</i>	Concat.	Mixing Fnc	Not Needed
<i>Integrity</i>			
<i>Data</i>	CRC-32	Michael	CCM
<i>Header</i>	None	Michael	CCM
<i>Replay</i>	None	Use IV	Use IV
<i>Key Mgmt</i>	None	802.11i 4-Way Handshake	802.11i 4-Way Handshake

- Mặc dù TKIP và CCMP đều được giới thiệu trong 802.11i như những giao thức bảo mật mạnh mẽ hơn thay cho WEP trong bảo mật không dây, tuy nhiên CCMP trội hơn nhiều so với TKIP về mặt an toàn.



**Do you have any  
questions?**

---