Mật mã đồng thời là gì ?

Mật mã đồng thời (Authenticated Encryption - AE) là kỹ thuật kết hợp giữa mã hóa và kiểm tra toàn vẹn, giúp đảm bảo rằng thông điệp được bảo mật và không bị sửa đổi trong quá trình truyền tải. Một ví dụ tiêu biểu là AES-GCM.

Tại sao phải sử dụng nó?

Chúng ta có thể sử dụng nó để mã hóa thông tin hoặc những dữ liệu thành những kí tự phức tạp khó để đoán và nhận diện bằng cách khái quát của chúng ta.

Chúng ta ở đây có thể sử dụng AES để tiếng hành mã hóa

**AES (Advanced Encryption Standard)** là một thuật toán mã hóa đối xứng mạnh mẽ, được sử dụng rộng rãi để **bảo vệ dữ liệu**. Khi bạn muốn **mã hóa một đoạn văn bản** để người khác **không đọc được nội dung**, AES sẽ biến đoạn văn bản gốc (gọi là *plaintext*) thành một đoạn mã hóa (*ciphertext*) không thể hiểu được nếu không có **khóa giải mã**.

Tuy nhiên, việc chỉ mã hóa thôi là **chưa đủ an toàn**, vì kẻ tấn công có thể cố tình **thay đổi dữ liệu** mà bạn không biết.

Đó là lý do vì sao **GCM (Galois/Counter Mode)** ra đời.

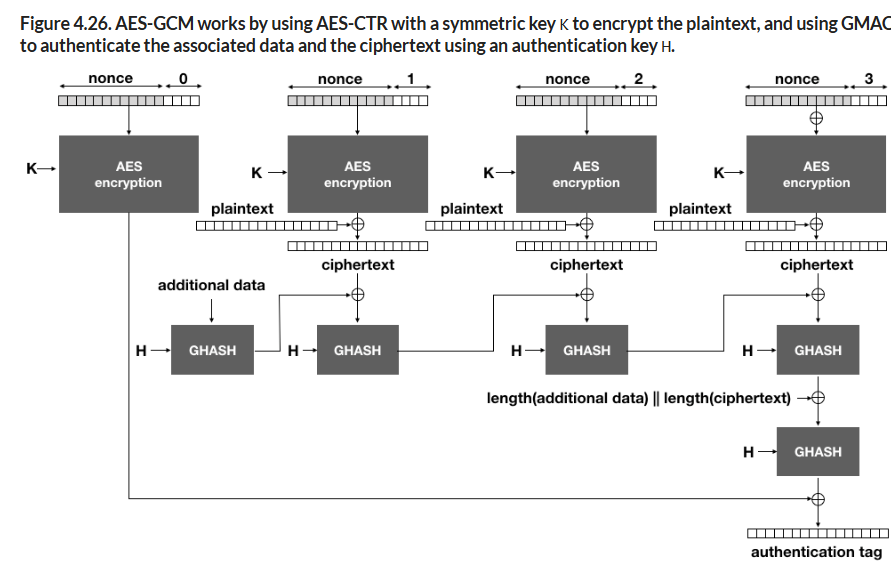
Có mode GCM

**AES-GCM là gì?**

* **AES-GCM** kết hợp:
  + **AES-CTR** để **mã hóa** dữ liệu.
  + **GMAC (GHASH)** để **kiểm tra tính toàn vẹn và xác thực** của dữ liệu.

Khi bạn sử dụng AES-GCM để mã hóa văn bản:

1. Văn bản được biến thành **dữ liệu mã hóa khó hiểu**.
2. Đồng thời, nó sinh ra một **mã xác thực (authentication tag)** để đảm bảo dữ liệu **không bị chỉnh sửa** trên đường truyền.
3. Nếu người khác **không có đúng khóa bí mật**, họ sẽ **không giải mã được**, và cũng **không thể giả mạo dữ liệu** vì hệ thống sẽ phát hiện ngay.

s