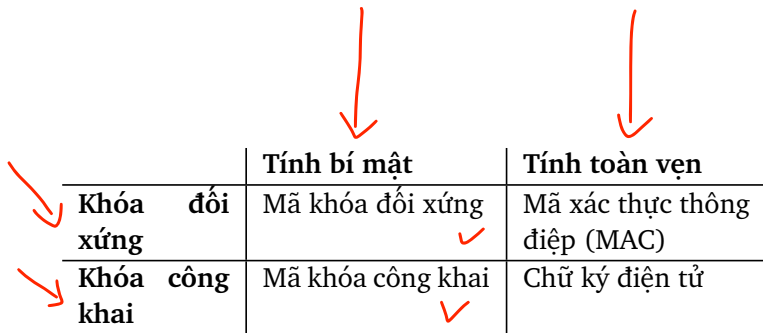


Mật mã ứng dụng

Các thành phần mật mã cơ bản

Một phần bức tranh mật mã



	Tính bí mật	Tính toàn vẹn
Khóa đối xứng	Mã khóa đối xứng ✓	Mã xác thực thông điệp (MAC)
Khóa công khai	Mã khóa công khai ✓	Chữ ký điện tử

Mật mã khóa đối xứng

Thuật toán:

$K \leftarrow \text{Gen}(1^\lambda)$ sinh khóa độ dài λ

$C \leftarrow \text{Enc}(K, M)$ mã hóa thông điệp M với khóa K , kết quả là bản mã C

$M = \text{Dec}(K, C)$ giải mã C dùng khóa K để lấy được M .

Sử dụng trong thực tế.

- Nếu chỉ cần tính bí mật: AES-128 với CBC mode hoặc CTR mode.
- Nếu cần cả tính bí mật và xác thực: EAX, CCM, hoặc GCM mode

Mật mã khóa công khai

Thuật toán:

$(SK, PK) \leftarrow Gen(1^\lambda)$ sinh cặp khóa (bí mật, công khai) độ dài λ
 $C \leftarrow Enc(PK, M)$ mã hóa thông điệp M với khóa công khai PK , kết quả là bản mã C
 $M = Dec(SK, C)$ giải mã C dùng khóa bí mật SK để được M .

Ví dụ.

- Giao thức trao đổi khóa Diffie-Hellman (DH)

Mật mã khóa công khai

Thuật toán:

$(SK, PK) \leftarrow Gen(1^\lambda)$ sinh cặp khóa (bí mật, công khai) độ dài λ
 $C \leftarrow Enc(PK, M)$ mã hóa thông điệp M với khóa công khai PK , kết quả là bản mã C
 $M = Dec(SK, C)$ giải mã C dùng khóa bí mật SK để được M .

Ví dụ.

- Giao thức trao đổi khóa Diffie-Hellman (DH)
- Hệ mật mã RSA

Mật mã khóa công khai

Thuật toán:

$(SK, PK) \leftarrow Gen(1^\lambda)$ sinh cặp khóa (bí mật, công khai) độ dài λ
 $C \leftarrow Enc(PK, M)$ mã hóa thông điệp M với khóa công khai PK , kết quả là bản mã C
 $M = Dec(SK, C)$ giải mã C dùng khóa bí mật SK để được M .

Ví dụ.

- Giao thức trao đổi khóa Diffie-Hellman (DH)
- Hệ mật mã RSA
- Hệ mật mã dựa trên đường cong Elliptic (ECC)

Kích thước khóa (theo bit)

Khuyến nghị của NIST

AES	DH & RSA	ECC
80	1024	160 ✓
112	2048	224 ✓
128	3072	256 ✓
192	7680	384 ✓
<u>256</u>	<u>15360</u>	512 ✓

Mã xác thực thông điệp



Thuật toán:

$k \leftarrow \text{Gen}(1^\lambda)$ sinh khóa độ dài λ
 $t \leftarrow S(k, m)$ tạo chữ ký thông điệp m dùng khóa k
 $V(k, m, t)$ “yes” hoặc “no” cho biết chữ ký t có phải là chữ ký hợp lệ của m hay không.

Ví dụ. HMAC.

Chữ ký điện tử

Thuật toán:

$(sk, pk) \leftarrow Gen(1^\lambda)$ sinh khóa bí mật và công khai độ dài λ
 $t \leftarrow S(sk, m)$ tạo chữ ký thông điệp m dùng khóa bí mật sk
 $V(pk, m, t)$ “yes” hoặc “no” cho biết chữ ký t có phải là chữ ký hợp lệ của m hay không.

Ví dụ. RSA, DSA, ECDSA