Mã hóa bí mật hoàn hảo

Bằng tiến sĩ. Nguyễn Đình Dương

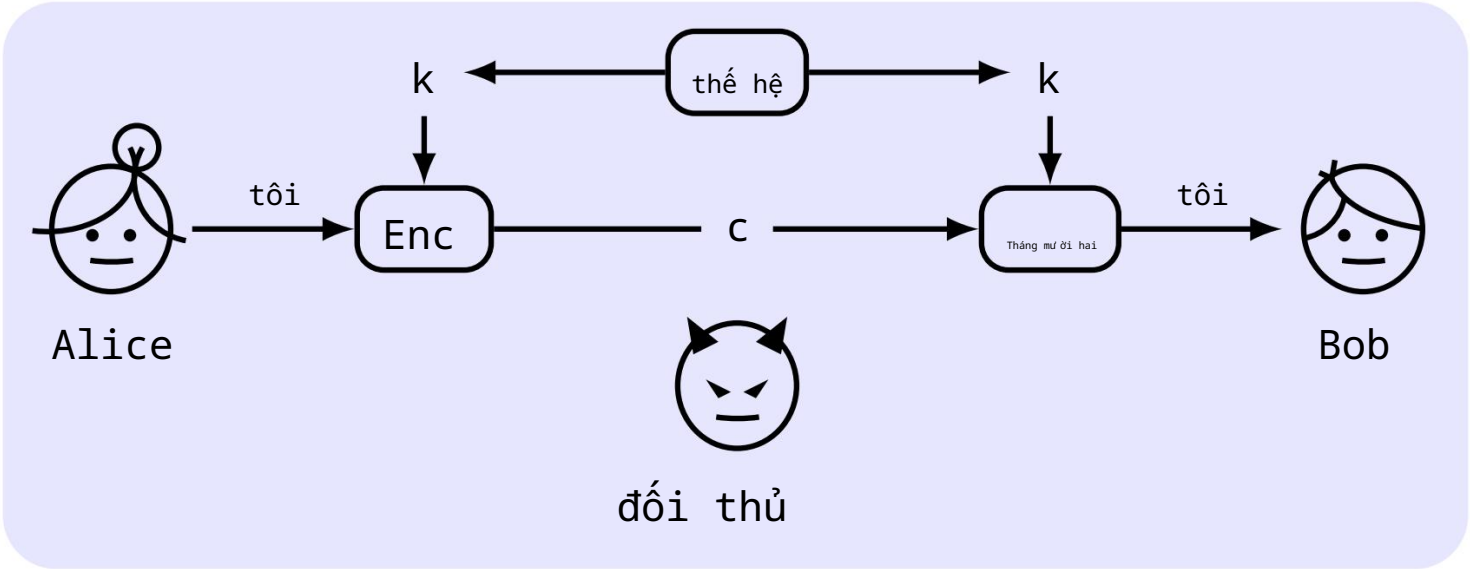
FIT - Trường Đại học Giao thông Vận tải

Mật Mã, Mùa Xuân, 2023

Đề cư ơng

Nội dung

Nhớ lại cú pháp mã hóa



- k K, m M, c C.
- k Gen, c := Enck(m), m := Deck(c).
- Sơ đồ mã hóa: Π = (Gen, Enc, Dec).
- Biến ngẫu nhiên: K, M, C cho khóa, bản rõ, bản mã.
- Xác suất: Pr[K = k],Pr[M = m],Pr[C = c].
- Yêu cầu chính xác cơ bản là gì?

Định nghĩa 'Bí mật hoàn hảo'

Trực giác: Đối thủ biết phân bố xác suất trên M. c sẽ không ảnh hưởng gì đến kiến thức của đối thủ; khả năng hậu nghiệm rằng một số m đã được gửi sẽ không khác với xác suất tiên nghiệm mà m sẽ được gửi.

Định nghĩa 1

Π trên M là hoàn toàn bí mật nếu với mọi phân bố xác suất trên M, m M và c C mà Pr[C = c] > 0:

$$\Pr[M = m | C = c] = \Pr[M = m].$$

Rút gọn: xác suất khác 0 đối với m M và c C.

Kế hoạch dưới đây có hoàn toàn bí mật không?

Với M = K = {0, 1}, Enck(m) = m k.

Bí mật hoàn hảo trên một bit

XOR một bit là hoàn toàn bí mật.

Đặt Pr[M = 1] = p và Pr[M = 0] = 1 p. Chúng ta hãy xem xét trư ờng hợp M = 1 và C = 1.

$$\Pr[M = 1 \mid C = 1] = \Pr[C = 1 \mid M = 1] \cdot \Pr[M = 1] / \Pr[C = 1]$$

$$= \frac{\Pr[K = 1 \quad 1] \cdot p}{\Pr[C = 1 \mid M = 1] \cdot \Pr[M = 1] + \Pr[C = 1 \mid M = 0] \cdot \Pr[M = 0]}$$

$$= \frac{1/2 \cdot}{1/2 \cdot (1 \quad p)} \cancel{p = p} = \Pr[M = 1] \; 1/2 \cdot p +$$

Chúng ta có thể làm tư ơng tự với những trư ờng hợp khác.

Lư u ý rằng $\Pr[M = 1 \mid C = 1] \neq \Pr[M = 1, C = 1] = \Pr[C = 1 \mid M = 1] \cdot \Pr[M = 1] = 1/2 \cdot p$.

Một công thức tương đương

Bổ đề 2

Π trên M là hoàn toàn bí mật với mọi phân bố xác suất trên M, m M và c C:

$$\Pr[C = c|M = m] = \Pr[C = c].$$

Bằng chứng.

: Nhân cả hai vế với Pr[M = m]/Pr[C = c], sau đó sử dụng Định lý Bayes. [1]

Pr[C = c|M = m] · Pr[M = m]/Pr[C = c] = Pr[M = m]

Pr[M = m|C = c] · Pr[C = c]/Pr[C = c] = Pr[M = m|C = c] : Nhân cả hai vế với Pr[C = c]/Pr[M = m], sau đó sử dụng Định lý Bayes.

□

[1] Nếu Pr[B] ≠ 0 thì Pr[A|B] · Pr[B] = Pr[B|A] · Pr[A])

Khả năng phân biệt hoàn hảo

Bổ đề 3

Π trên M là hoàn toàn bí mật với mọi phân bố xác suất trên M, m0, m1 M và c C:

$$\Pr[C = c \mid M = m_0] = \Pr[C = c \mid M = m_1].$$

Bằng chứng.

: Theo Bổ đề 2: $\Pr[C = c \mid M = m] = \Pr[C = c]$.

chắc chắn : p $= \Pr[C = c \mid M = m_0]$.

$$\Pr[C = c] = \sum_{m \in M} \Pr[C = c \mid M = m] \cdot \Pr[M = m]$$

$$= \sum_{m \in M} p \cdot \Pr[M = m] = p = \Pr[C = c \mid M = m_0].$$

□

Nội dung

Sổ tay dùng một lần (Mật mã Vernam)

- M = K = C = {0, 1} $^{\ell}$.
- Gen chọn ngẫu nhiên a k với xác suất đúng 2 c := $^{\ell}$.
- Enck(m) = k m. m :=
- Bộ bài(c) = k c.

Định lý 4

Sơ đồ mã hóa pad một lần là hoàn toàn bí mật.

Bằng chứng.

$$\Pr[C = c|M = m] = \Pr[M \quad K = c|M = m]$$

$$= \Pr[m \quad K = c] = \Pr[K = m \quad c] = 2 \quad \ell .$$

Khi đó Bổ đề 3: Pr[C = c|M = m0] = Pr[C = c|M = m1]. □

Nội dung

Hạn chế của OTP và Bảo mật hoàn hảo

Key k dài bằng m, khó lưu trữ và chia sẻ k.

Định lý 5

Giả sử Π hoàn toàn bí mật trên M, và K được xác định bởi Gen. Khi đó |K| ≥ |M|.

Bằng chứng.

Giả sử |K| < |M|. M(c) = {m^ | m^ = Deck(c) đối với một số ^k chắc chắn K}.

Vì với một k, có nhiều nhất một m sao cho m = Deck(c), |M(c)| ≤ |K| < |M|.

Vậy m′ M/ (c). Sau đó

$$\Pr[M = m' \mid C = c] = 0 \neq \Pr[M = m']$$

và do đó không hoàn toàn bí mật. □

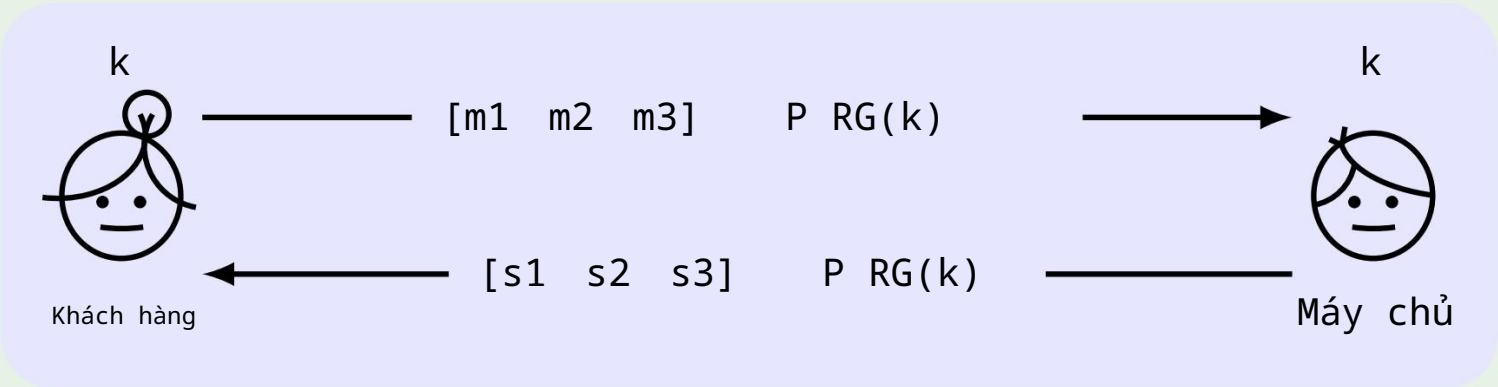
Hai bảng thời gian: Các trư ờng hợp trong thế giới thực

Chỉ đư ợc sử dụng một lần cho cùng một khóa, nếu không

$$c \quad c' = (m \quad k) \quad (m' \quad k) = m \quad m' \quad .$$

Học m từ m m′ do tính dư thừa của ngôn ngữ.

MS-PPTP (Win NT)



Cải tiến: sử dụng riêng 2 phím cho C-to-S và S-to-C.

Nội dung

Định lý Shannon

Định lý 6

Đối với |M| = |K| = |C|, Π hoàn toàn bí mật

1. Mọi k K được chọn với xác suất 1/|K| bởi Gen.
2. m M và c C, duy nhất k K: c := Enck(m).

Bằng chứng.

: Pr[C = c|M = m] = 1/|K|, sử dụng Bổ đề 3.

(2): Í t nhất một k, nếu không Pr[C = c|M = m] = 0;
nhiều nhất là một k, vì {Enck(m)}k K = C và |K| = |C|.
(1): ki sao cho Encki (mi) = c.

$$\begin{aligned}
\Pr[M = m_i] &= \Pr[M = m_i \mid C = c] \\
&= (\Pr[C = c \mid M = m_i] \cdot \Pr[M = m_i]) / \Pr[C = c] \\
&= (\Pr[K = k_i] \cdot \Pr[M = m_i]) / \Pr[C = c],
\end{aligned}$$

nên Pr[K = ki] = Pr[C = c] = 1/|K|. □

Ứng dụng Định lý Shannon

Kế hoạch dư ới đây có hoàn toàn bí mật không?

Cho M = C = K = {0, 1, 2, . . . , 255}

Enck(m) = m + k mod 256

Deck(c) = c k mod 256

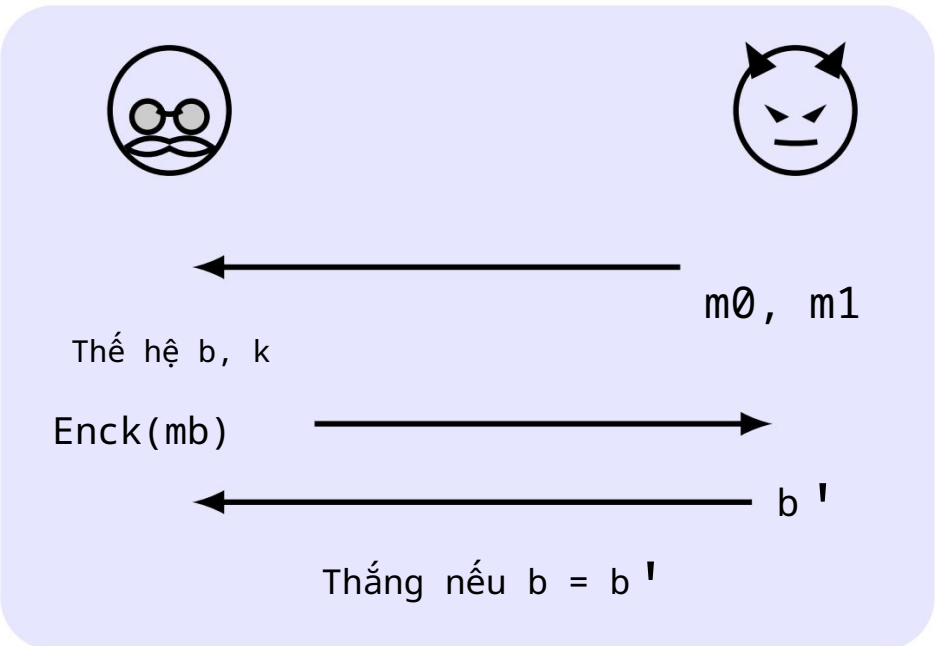
Nội dung

Thí nghiệm nghe lén không thể phân biệt

PrivKeav biểu thị một thử nghiệm mã hóa khóa riêng cho một A,Π Π cho trư ớc trên M và một đối thủ nghe lén A.

1. A xuất ra một cặp thông báo m0, m1 M. k
2. Gen, một bit ngẫu nhiên b {0, 1} đư ợc chọn. Sau đó c Enck(mb) đư ợc trao cho A.
3. A xuất ra một bit b '
4. Nếu b'= b, A thành công PrivKeav = 1, ngư ợc lại 0.

A,Π



Tính không thể phân biệt đối nghịch

Định nghĩa 7

Π trên M là hoàn toàn bí mật nếu với mọi A nó thỏa mãn điều đó

$$\Pr[\text{PrivKeav}_{A,\Pi} = 1] = \frac{1}{2}.$$

Những sơ đồ nào dư ới đây là hoàn toàn bí mật?

- Enck,k′(m) = OTPk(m) OTPk ′(m)
- Enck(m) = đảo ngư ợc(OTPk(m))
- Enck(m) = OTPk(m) k
- Enck(m) = OTPk(m) OTPk(m)
- Enck(m) = OTP0n (m)
- Enck(m) = OTPk(m) LSB(m)

Bản tóm tắt

- Tính bí mật hoàn hảo = Tính không thể phân biệt hoàn hảo = Tính không thể phân biệt đối
- nghịch Tính bí mật hoàn hảo có thể đạt đư ợc. Sổ tay dùng một lần (mật mã của Vernam)
- Định lý Shannon