Machine Translated by Google

Giới thiệu

Bằng tiến sĩ. Nguyễn Đình Dư ơ ng

FIT - Trư ờng Đại học Giao thông Vận tải

Mật Mã, Mùa Xuân, 2023

Machine Translated by Google

Đề cương

Machine Translated by Google

Nội dung

Machine Translated by Google

Mật mã là gì?

- Mật mã: từ tiếng Hy Lạp kryptós, “ẩn, bí mật”; và graphin, “viết”
- Mật mã học: nghệ thuật viết hoặc giải mã.
  (Từ điển Oxford ngắn gọn 2006)
- Mật mã: một hệ thống các tín hiệu được sắp xếp trước, đặc biệt được sử dụng để đảm bảo bí mật trong việc truyền tải thông điệp.
- (từ mã trong mật mã) Thập niên 1980: từ Cổ điển đến Hiện đại;
- từ Quân đội đến mọi người Mật mã hiện đại: nghiên cứu khoa học về các kỹ thuật toán học để bảo mật thông tin, hệ thống và tính toán phân tán kỹ thuật số chống lại các cuộc tấn công bất lợi

Machine Translated by Google

Mật mã là gì? [xkcd:504]

Machine Translated by Google

Nội dung

Machine Translated by Google

Mã hóa khóa riêng

- Mục tiêu: xây dựng trư ớc các mật mã (sơ đồ mã hóa) để cung cấp thông tin liên lạc bí mật giữa hai bên chia sẻ khóa riêng (khóa đối xứng)
- Giả định ngầm định: ban đầu có một số cách để chia sẻ khóa một cách bí mật
- Mã hóa ổ đĩa: cùng một ngư ời dùng tại các thời điểm khác nhau

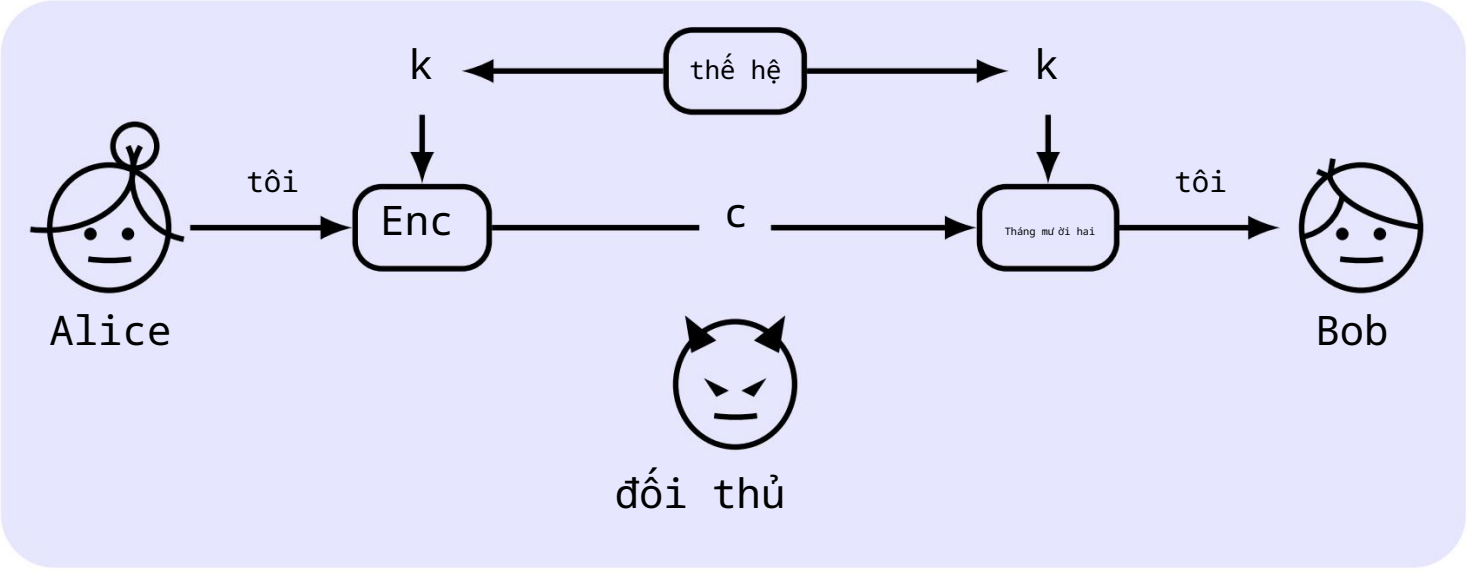
Machine Translated by Google

Alice, Bob [xkcd:1323]

Việc đổi tên sẽ dễ dàng hơ n, như ng nếu bạn không thoải mái khi nói dối, hãy thử chỉ kết bạn với những ngư ời tên Alice, Bob, Carol, v.v.

Machine Translated by Google

Cú pháp mã hóa



- khóa k K, bản rõ (hoặc thông điệp) m M, bản mã c C
- Thuật toán tạo khóa k Gen
- Thuật toán mã hóa c := Enck(m)
- Thuật toán giải mã m := Deck(c)
- Sơ đồ mã hóa: Π = (Gen, Enc, Dec)
- Yêu cầu về độ chính xác cơ bản: Deck(Enck(m)) = m

Machine Translated by Google

Khóa bảo mật và thuật toán che khuất

- Dễ dàng hơn để duy trì bí mật của một khóa ngắn
- Trong trường hợp chìa khóa bị lộ, các bên trung thực dễ dàng thay đổi chìa khóa hơn
- Trường hợp nhiều cặp người thì dễ sử dụng cùng một thuật toán nhưng khác khóa

nguyên lý Kerckhoffs

Phương pháp mật mã không nhất thiết phải bí mật, phải có khả năng rơi vào tay kẻ thù mà không gặp bất tiện.

Châm ngôn của Shannon

Kẻ thù biết hệ thống.

Machine Translated by Google

Tại sao “Thiết kế mật mã mở”

- Các thiết kế được xuất bản trải qua sự giám sát của công chúng sẽ mạnh
- mẽ hơn Tốt hơn để các “tin tặc có đạo đức” tiết lộ các lỗ hổng bảo mật
- Kỹ thuật đảo ngược mã (hoặc rò rỉ do gián điệp công nghiệp) gây ra mối đe dọa nghiêm trọng đối với an ninh Cho phép thiết
- lập các tiêu chuẩn.

EC kép: Cửa sau được tiêu chuẩn hóa

“EC kép đã được tiêu chuẩn hóa bởi NIST, ANSI và ISO cùng với các thuật toán khác để tạo ra số giả ngẫu nhiên.” “Những tiết lộ của Snowden, và đặc biệt là các báo cáo về Dự án Bullrun và Dự án kích hoạt SIGINT, đã chỉ ra rằng Dual EC là một phần trong nỗ lực có hệ thống của NSA nhằm phá hoại các tiêu chuẩn.” “Reuters đưa tin rằng NSA đã trả cho RSA “10 triệu đô la trong một thỏa thuận đặt [EC kép] làm phương pháp ưu tiên hoặc mặc định để tạo số trong phần mềm BSafe.”

Machine Translated by Google

Kịch bản tấn công

- Chỉ bản mã: kẻ tấn công chỉ quan sát bản mã
- Bản rõ đã biết: kẻ tấn công học các cặp bản rõ/bản mã dư ới cùng một khóa
- Bản rõ đư ợc chọn: đối thủ có khả năng lấy đư ợc mã hóa của bản rõ mà nó lựa chọn
- Bản mã đư ợc chọn: kẻ tấn công có khả năng giải mã các bản mã khác mà nó lựa chọn
- Tấn công thụ động: COA KPA vì
  - không phải tất cả bản mã đều bí mật
- Tấn công chủ động: CPA CCA
  - khi nào nên mã hóa/giải mã bất cứ điều gì đối thủ mong muốn?

Machine Translated by Google

Nội dung

Machine Translated by Google

Mật mã của Caesar

> Nếu anh ta có điều gì bí mật muốn nói, anh ta viết nó bằng mật mã, nghĩa là bằng cách thay đổi thứ tự các chữ cái trong bảng chữ cái đến mức không một từ nào có thể đư ợc tạo ra. Nếu bất kỳ ai muốn giải mã những từ này và hiểu đư ợc ý nghĩa của chúng, ngư ời đó phải thay chữ cái thứ tư trong bảng chữ cái, cụ thể là D, cho A, và tư ơ ng tự như vậy bằng những chữ cái khác.
>
> –Suetonius, “Cuộc đời của Julius Caesar”

- Enc(m) = m + 3 mod 26 [1]
- Điểm yếu: ?

Ví dụ

bắt đầu cuộc tấn công ngay bây giờ

[1] Trên thực tế, trích dẫn chỉ ra rằng việc giải mã liên quan đến việc xoay các chữ cái trong bảng chữ cái về phía trư ớc 3 vị trí, Dec(c) = c + 3 mod 26

Machine Translated by Google

Mật mã dịch chuyển

- Enck(m) = m + k mod 26
- Bộ bài(c) = c k mod 26
- Yếu đuối: ?

Ví dụ: Giải mã chuỗi

EHJLQWKHDWWDFNQRZ

Nguyên tắc không gian khóa đủ

Bất kỳ sơ đồ mã hóa an toàn nào cũng phải có một không gian khóa không dễ bị tấn công khi tìm kiếm toàn diện.[2]

[2] Nếu không gian bản rõ lớn hơn không gian khóa.

Machine Translated by Google

Phương pháp chỉ số trùng hợp (IC) (để tìm k)

Làm thế nào để tự động xác định rằng văn bản được giải mã có ý nghĩa?

Chỉ số trùng hợp (IC): xác suất hai chữ cái được chọn ngẫu nhiên (chọn rồi trả lại) sẽ giống hệt nhau.

Gọi pi là xác suất của chữ cái thứ i trong văn bản tiếng Anh.

$$\text{TÔI} \overset{\text{chắc chắn}}{=} \sum_{i=0}^{25} p_i^2$$

Ví dụ

IC của 'quả táo' là gì?

Đối với một văn bản tiếng Anh dài, IC là ≈ 0,065. Với j = 0, 1, . . . , 25, qj là xác suất của chữ cái thứ j trong bản mã.

$$\text{Là} \overset{\text{chắc chắn}}{=} \sum_{\text{tôi}=0}^{25} p_i \cdot q_{i+s}$$

Hỏi: Đối với mật mã dịch chuyển, nếu s = k thì Is ≈ ?

Machine Translated by Google

Thay thế chữ cái đơn

- Ý tưởng: Ánh xạ mỗi ký tự tới một ký tự khác nhau một cách tùy ý thái độ
- Điểm mạnh: Không gian khóa lớn $\approx 2^{88}$. Hỏi: Làm thế nào để đếm?
- Điểm yếu: ?

Ví dụ

abcdefghijklmnopqrstuvwxyz

XEUADNBKVMROCQFSYHWGLZIJPT

Bản rõ: kể cho anh ấy về tôi

Bản mã: ??????????????

Machine Translated by Google

Tấn công bằng các mẫu thống kê

1. Lập bảng tần số của các chữ cái trong bản mã
2. So sánh với văn bản tiếng Anh
3. Đoán chữ cái thường xuyên nhất tương ứng với e, v.v.
4. Chọn bản rõ "có ý nghĩa" (Không tầm thường)

Bảng: Tần suất chữ cái trung bình cho văn bản tiếng Anh

e 12,7%	t 9,1%	a 8,2%	o 7,5%	i 7,0%	n 6,7%
6,4% s	6,3% h	6,1% r	6,0% d	4,3% l	4,0% c
2,8% u	2,8% m	2,4% w	2,4% f	2,2% g	2,0% y
2,0% p	1,9% b	1,5% v	1,0% k	0,8% j	0,2% x
0,2% q	0,1% z	0,1%			

Machine Translated by Google

Ví dụ về Phân tích tần số (Bản mã)

LIVITCSWPIYVEWHEVSRIQMXLEYVEOIEWHRXEXIPFEMVEWHKVS

TYLXZIXLIKIIXPIJVSZEYPERRGERIMWQLMGLMXQERIWGPSRIH

MXQEREKIETXMJTPRGEVEKEITREWHEXXLEXXMZITWAWSQWXSWE

XTVEPMRXRSJGSTVRIEYVIEXCVMUIMWERGMIWXMJMGCSMWXSJO

MIQXLIVIQIVIXQSVSTWHKPEGARCSXRWIEVSWIIBXVIZMXFSJX

THÍ CHGAEWHEPSWYSWIWIEVXLISXLIVXLIRGEPIRQIVIIBGIIHM

WYPFLEVHEWHYPSRRFQMXLEPPXLIECCIEVEWGISJKTVWMRLIHY

SPHXLIQIMYLXSJXLIMWRIGXQEROIVFVIZEVAEKPIEWHXEAMWY

EPPXLMWYRMWXSGSWRMHIVEXMSWMGSTPHLEVHPFKPEZINTCMXI

VJSVLMRSCMWMSWVIRCIGXMWYMX

Machine Translated by Google

Ví dụ về Phân tích tần số (Analysis)

Đếm và đoán, thử và sai.

Bảng: Các bư ớc phân tích

Bản rõ Bản rõ	
I E	
XLI cái	
E a	
trạng thái xếp hạng	
atthattMZe lúc đó	
anh ấy ở đây	
remarMột	nhận xét

Machine Translated by Google

Ví dụ về phân tích tần số (Bản rõ)

Sau đó, Legrand đứng dậy, với vẻ trang nghiêm và trang nghiêm, mang cho tôi con bọ từ chiếc tủ kính đựng nó. Đó là một con bọ hung xinh đẹp, và vào thời điểm đó, các nhà tự nhiên học chưa biết đến nó – tất nhiên là một giải thưởng lớn xét theo quan điểm khoa học. Có hai đốm đen tròn ở gần một đầu của lưng và một cái dài ở gần đầu kia. Những chiếc vảy cực kỳ cứng và bóng, trông như màu vàng bóng. Trọng lượng của con côn trùng rất đáng chú ý, và khi cân nhắc mọi thứ, tôi khó có thể trách Jupiter vì quan điểm của anh ấy tôn trọng nó.

– “Con bọ vàng” của Edgar Allan Poe

Machine Translated by Google

Mật mã Vigenère (dịch chuyển nhiều bảng chữ cái)

- Ý tưởng: Để "làm trơn" sự phân bố trong bản mã bằng cách ánh xạ các trường hợp khác nhau của cùng một chữ cái trong bản rõ sang các trường hợp khác nhau trong bản mã
- Mã hóa: $c_i = m_i + k[i \bmod t]$, t là độ dài (chu kỳ) của k
- Giải mã: Cần tìm t; nếu t được biết, cần biết liệu việc giải mã có hợp lý hay không, nhưng lực lượng vũ phu (26^t) là không khả thi đối với $t > 15$

Ví dụ (Khóa là 'cafe')

Bản rõ cho anh ấy biết về tôi

Chìa khóa cafecafecafeca

Bản mã ???????????

Machine Translated by Google

Phư ơ ng pháp Kasiski (để tìm t)

- Để xác định các mẫu lặp lại có độ dài 2 hoặc 3
- Khoảng cách giữa các lần xuất hiện như vậy là bội số của
- tt là ư ớc chung lớn nhất của tất cả các khoảng cách

Ví dụ (Khóa là 'hạt')

ngư ời đàn ông và ngư ời phụ nữ đã lấy đư ợc lá thư từ bư u điện

VMFQTPFOHMJJXSFCSSIMTNFZXFYISEIYUIKHWPQMJJQSLVTGJKGF

Machine Translated by Google

Phư ơ ng pháp chỉ số trùng hợp (IC) (để tìm t)

Với τ = 1, 2, . . ., qi là xác suất của chữ cái thứ i trong

c1, c1+τ , c1+2τ , . . . , IC là

$$\text{chắc chắn} = \text{tôi} \sum_{\text{tôi}=0}^{25} q_i^2$$

Nếu τ = t thì Iτ ≈? ; ngư ợc lại khí ≈ $\frac{1}{26}$ Và

$$I\tau \approx \sum_{\text{tôi}=0}^{25} \frac{1}{262} \approx 0{,}038$$

Sau đó sử dụng lại phư ơ ng pháp IC để tìm ki .

Nguyên tắc đối thủ tùy tiện

An ninh phải đư ợc đảm bảo cho bất kỳ đối thủ nào trong nhóm đối thủ có sức mạnh đư ợc chỉ định

Machine Translated by Google

Tấn công phân tích mật mã (bài tập về nhà)

- Theo COA, yêu cầu về bản mã liên quan đến kích thư ớc của không gian khóa. Vigènere > phụ chữ cái đơ n. > shift Theo KPA, bị hỏng tầm
- thư ờng.

Bài học kinh nghiệm

- Nguyên tắc không gian khóa đủ
- Thiết kế mật mã an toàn là một nhiệm vụ
- khó khăn Độ phức tạp không hàm ý tính bảo mật (thế thì sao?)
- Nguyên tắc đối địch tùy tiện

Machine Translated by Google

Nội dung

Machine Translated by Google

Ba nguyên tắc chính của mật mã hiện đại

1. Việc xây dựng một định nghĩa nghiêm ngặt về an ninh/mối đe dọa
   ngư ời mẫu
2. Khi tính bảo mật của mật mã dựa vào một kết quả chư a đư ợc chứng minh
   giả định này, giả định này phải đư ợc nêu chính xác và tối thiểu nhất có thể
3. Mật mã phải kèm theo bằng chứng bảo mật nghiêm ngặt với định nghĩa và giả định trên

Machine Translated by Google

Tại sao Nguyên tắc 1 – Xây dựng các định nghĩa chính xác

Câu hỏi: Bạn chính thức hóa việc bảo mật cho mã hóa khóa riêng như thế nào?

1. Không kẻ thù nào có thể tìm ra khóa bí mật khi được cung cấp một bản mã.

   Enck(m) = m

2. Không đối thủ nào có thể tìm thấy bản rõ tương ứng với mật mã.

   Enck(m) = m0 AESk(m)

3. Không đối thủ nào có thể xác định được bất kỳ ký tự nào của bản rõ tương ứng với bản mã. m = 1000, ai đó có thể học 800 < m < 1200

4. Không đối thủ nào có thể lấy được bất kỳ thông tin có ý nghĩa nào về bản rõ từ bản mã.

   Bạn có thể định nghĩa cái gọi là 'có ý nghĩa' không?

Các định nghĩa về bảo mật phải đủ cho tất cả các ứng dụng tiềm năng.

Machine Translated by Google

Tại sao Nguyên tắc 1 – Cách xác định

Cách xác định tính bảo mật – Bài học từ Alan Turing Tính

- toán là gì?3 Lời kêu
  1. gọi trực tiếp đến trực giác
  2. Bằng chứng về sự tư ơ ng đư ơ ng của hai định nghĩa
     (Định nghĩa mới có sức hấp dẫn trực quan hơ n)
  3. Đư a ra ví dụ giải bằng định nghĩa
- Phư ơ ng pháp bổ sung để bảo mật: Kiểm tra thời gian

3Q: Bất kỳ "bằng chứng toán học nào cho thấy tồn tại các vấn đề đư ợc xác định rõ ràng" máy tính không giải đư ợc"? A: Bài toán dừng trong lý thuyết tính toán

Machine Translated by Google

Nguyên tắc 2 – Dựa vào các giả định chính xác

Hầu hết các cấu trúc mật mã không thể đư ợc chứng minh là an toàn vô điều

- kiện Tại sao?
  1. Xác thực giả định So sánh các sơ đồ Tạo điều kiện thuận lợi cho bằng chứng về tính bảo mật

  Việc xây dựng là an toàn nếu giả định là đúng.

- Làm sao?
  1. cũ, đã đư ợc kiểm tra ký lư ỡng đơ n giản và cấp độ thấp hơ n, nên dễ học, bác bỏ & sửa

Machine Translated by Google

Nguyên tắc 3 – Bằng chứng nghiêm ngặt về bảo mật

- Tại sao? Bằng chứng được mong muốn hơn trong lĩnh vực bảo mật máy tính so với các lĩnh vực khác.
- Cách tiếp cận giản lược:

Định lý 1

Cho rằng Giả định X là đúng, Cấu trúc Y là an toàn theo định nghĩa đã cho.

Bằng chứng.

Rút gọn bài toán do X đưa ra thành bài toán phá vỡ Y. □

- Phương pháp tiếp cận đặc biệt: dành cho những người cần một giải pháp "nhanh chóng và bẩn thỉu", hoặc những người chỉ đơn giản là không biết.

Machine Translated by Google

Bản tóm tắt

- Mật mã bảo mật thông tin, giao dịch và tính toán
  Nguyên tắc
- Kerckhoffs & Thiết kế mật mã mở Caesar's, shift,
- Mono-Alphabetic sub., Vigenère Brute Force,
- tần số chữ cái, Kasiski's, IC Nguyên
- tắc không gian khóa vừa đủ
- Nguyên tắc đối thủ tùy ý
- Bảo mật đư ợc chứng minh nghiêm ngặt