ĐỀ CƯƠNG

# 1. IC (chỉ số trùng lặp là gì), nêu và chứng minh công thức tính chỉ số trùng lặp.

- IC (Index of Coincidence) là xác suất hai kí tự ngẫu nhiên trong văn bản là giống nhau.

- Công thức cho văn bản x = gồm n kí tự, số lần xuất hiện của mỗi kí tự là

- Chứng mình công thức:

Số cách chọn ra 2 kí tự ngẫu nhiên trong văn bản là:

Số cách chọn ra 2 kí tự mà 2 kí tự đều là là:

Tổng số cách chọn ra 2 kí tự mà 2 kí tự đều giống nhau là

Xác xuất để 2 kí tự được chọn từ văn bản là 2 kí tự giống nhau là:

# 2. Phân tích ưu nhược điểm và so sánh hai hệ mã: công khai và bí mật

Table

Description automatically generated

|  |  |  |
| --- | --- | --- |
|  | Hệ mã khóa bí mật | Hệ mã khóa công khai |
| Ưu điểm | Quá trình mã hóa và giải mã thường diễn ra nhanh | Thường an toàn hơn do phải cần đến hai khóa  Bất kì ai có khóa công khai đều có thể mã hóa thông tin. Thông tin được mã hóa chỉ có thể được giải mã bằng khóa bí mật. Thuận tiện hơn trong việc trao đổi khóa |
| Nhược điểm | Cần phải có 1 phương thức để trao đổi khóa chung | Quá trình giải mã diễn ra chậm  Không thể xác thực người gửi nếu như không biết trước mã công khai của nhau |
| Phân biệt | Hệ mã khóa bí mật chỉ cần 1 khóa cho việc mã hóa và giải mã  Hệ mã khóa công khai cần phải có 2 khóa cho việc mã hóa và giải mã: 1 khóa công khai và 1 khóa bí mật | |

# 3. Giải thích thuật ngữ tấn công biết bản rõ (known plaintext attack) và lấy ví dụ những tình huống tấn công thực tế.

Thuật ngữ tấn công biết bản rõ là một dạng tấn công trong đó kẻ tấn công có thông tin về **một vài** *bản rõ* và *bản mã* tương ứng. Từ thông tin này thì kẻ tấn công có thể dùng để tìm ra các khóa đã được dùng để mã hóa gói tin này hoặc tìm cách để giải mã gói tin dùng cũng khóa với gói tin đã bắt được.

Ví dụ: Kẻ tấn công E tính cờ hoặc có tay trong là một người trong hệ thống mã hóa. E có thể lấy được thông tin về một vài bản rõ X và bản mã Y. Từ thôn tin này kẻ tấn công có thể dùng phép thử loại trừ để vét cạn không gian khóa để tìm ra khóa đúng K sao cho Encrypt(K, X) = Y

# 4. Hãy so sánh IC của một bản rõ M và một mã ngẫu nhiên R có cùng độ dài

Một bản mã ngẫu nhiên R có cũng độ dài sẽ có IC nhỏ hơn bản rõ M. Từ công thức

ta có thể chứng minh được giá trị IC đạt cực tiểu khi giá trị các f[i] bằng nhau theo bất đẳng thức Cauchy Swcharz. Trong bản mã ngẫu nhiên R,tần xuất xuất hiện của các chứ cái sẽ đồng đều hơn (các f[i] bằng nhau), IC do đó sẽ có giá trị gần với giá trị cực tiểu hơn.

# 5. Nêu các nguyên tắc thiết kế mật mã khối an toàn. Nêu các kỹ thuật thiết kế để đảm bảo các nguyên tắc đó.

Nguyên tắc để thiết kế mật mã khối an toàn:

* **Confusion** (Hỗn loạn, rắc rối) Sự phụ thuộc của bản mã đối với bản rõ phải thực phức tạp để gây rắc rối, cảm giác hỗn loạn đối với kẻ thù có ý định phân tích tìm qui luật để phá mã. Quan hệ hàm số của mã-tin là phi tuyến (non-linear).
* **Diffusion** (Khuếch tán) Làm khuếch tán những mẫu văn bản mang đặc tính thống kê (gây ra do dư thừa của ngôn ngữ) lẫn vào toàn bộ văn bản. Nhờ đó tạo ra khó khăn cho kẻ thù trong việc dò phá mã trên cơ sở thống kê các mẫu lặp lại cao. Sự thay đổi của một bit trong một khối bản rõ phải dẫn tới sự thay đối hoàn toàn trong khối mã tạo ra.

Kỹ thuật thiết kế:

* Confusion có thể đƣợc thực hiện bằng phép thay thế (substitution)
* Diffusion được tạo ra bằng các phép chuyển đổi chỗ (transposition/permutation) hay hoán vị.

# 6. Gọi DES là thuật toán mã hóa DES và là thuật toán giải mã DES.

# Chứng minh

Ta có

=> Hàm F là các hàm có tính chất đối hợp

Suy ra

# 7. Cấu trúc feistel là gì, tại sao cần sử dụng nhiều vòng lặp? Sự thực hiện ở các vòng lặp có hoàn toàn giống nhau không?

Cấu trực feistel là một cấu trực gồm nhiều vòng lặp, mỗi vòng lặp thực hiện thao tác hoàn vị và thay thế với đầu vào là đầu ra của vòng lặp trước đó và một khóa con được sinh ra từ khóa đầy đủ với thuật toàn sinh khóa.

Việc sử dụng nhiều vòng lặp sẽ tăng permutation và confusion của cấu trúc, giúp cho mã hóa an toàn hơn

Sự thực hiện ở các vòng lặp gần như giống nhau, chỉ khác nhau ở đầu vào và khóa được sử dụng

# 8. Trong thuật toán RSA, tại sao phải chọn p, q đều lớn, nếu chỉ chọn 1 số lớn, 1 số nhỏ có được không?

Bởi vì cốt lõi của việc phá được mã RSA là việc tìm ra được q và p từ n = p x q. Khả năng tìm được cặp số p q sẽ phụ thuộc vào độ lớn số nhỏ hơn, vì từ 1 số sẽ suy ra được số còn lại. Số càng nhỏ thì việc tìm ra sẽ càng nhanh. Do đó cần cả p và q càng lớn để tăng số khả năng phải thử, giảm khả năng mã RSA bị phá

# 9. Trong thuật toán RSA, tại sao phải chọn e < m

Ta chọn e < m bởi vì giá trị lớn hơn là và không cần thiết sẽ tăng khối lượng tính sử dụng

Giả sử e>φ(n). Khi đó tồn tại e′<φ(n) sao cho: e≡e′(modφ(n))

Khi đó ta có e = e′+ k⋅φ(n)

ae ≡ a^(e′+k⋅φ(n)) ≡ a^e′\* a^(k⋅φ(n))

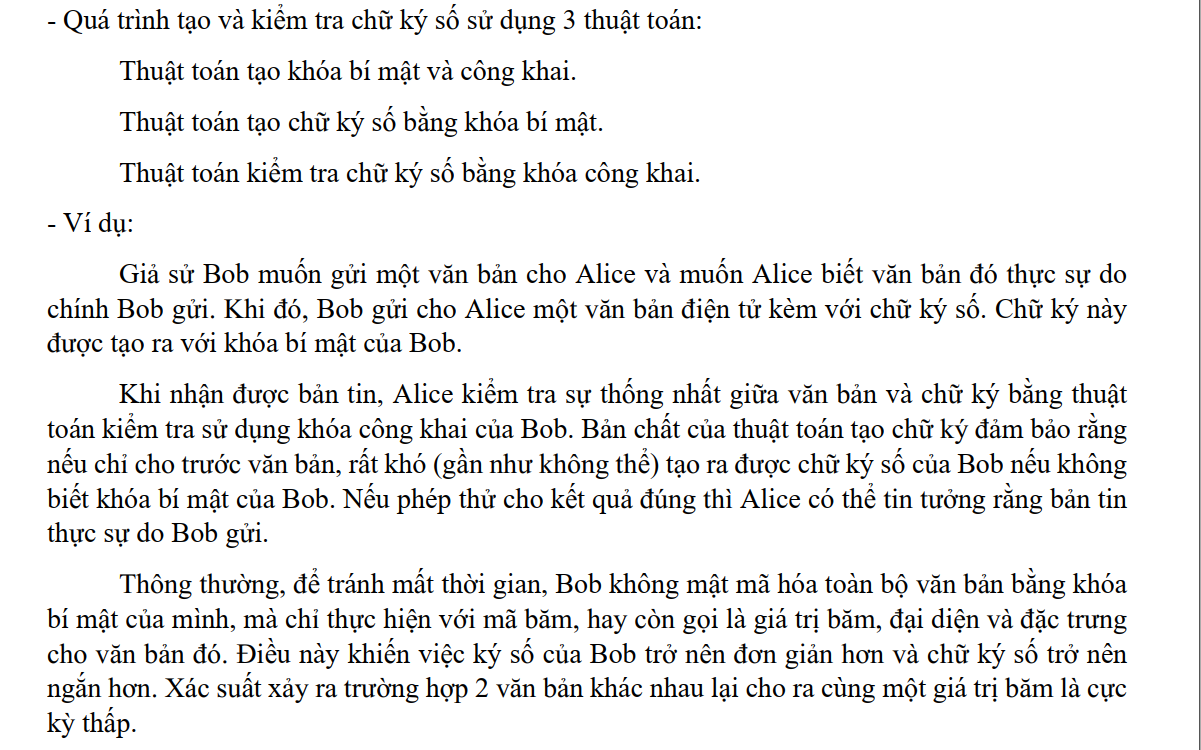
≡ ae′\* (a^φ(n))^k≡ae′(1)^k≡ae′(modn)

→luôn tồn tại e’ nhỏ hơn

# 10. Nêu lý do tại sao cần ký lên giá trị của hàm băm thay vì ký trực tiếp lên văn bản

* Việc kí lên hàm băm sẽ tiết kiệm thời gian hơn, do hàm băm luôn cho ra một xâu độ dài cố định và thông thườngng ngắn hơn rất nhiều so với xâu đầu vào, từ đó giúp sinh chữ kí một cách hiệu quả hơn.
* Đảm bảo tính phi đụng độ cao, không thể tìm được hai văn bản thông tin khác nhau cho cũng một hàm băm. Đồng đảm bảo tính một chiều: từ hàm băm không thể suy ra nội dung văn bản. Từ đó tránh được việc bị giả mạo chữ kí

# 11. Áp dụng các kiến thức về mật mã công khai và chữ ký số, hãy xây dựng một giao thức trao đổi giữa hai người A và B sao cho giao thức này đảm bảo tính mật, tính toàn vẹn và tính xác thực xác thực của gói tin. Giả sử rằng A và B đều biết khóa công khai của đối phương.



Text, letter

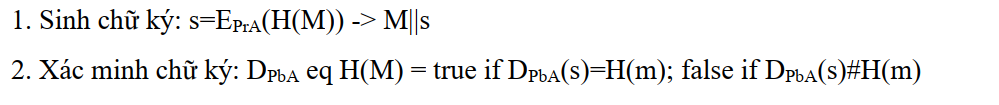
Description automatically generated

# 12. Trình bày giao thức tạo và xác minh chữ ký số sử dụng hệ mật mã khóa công khai

Giao thức tạo: X || Da(H(X)) trong đó H là hàm băm, Da là khóa bí mật, Ea là khóa công khai

Giao thức xác minh kiểm tra Ea(Da(Hx)) eq H(X)

///

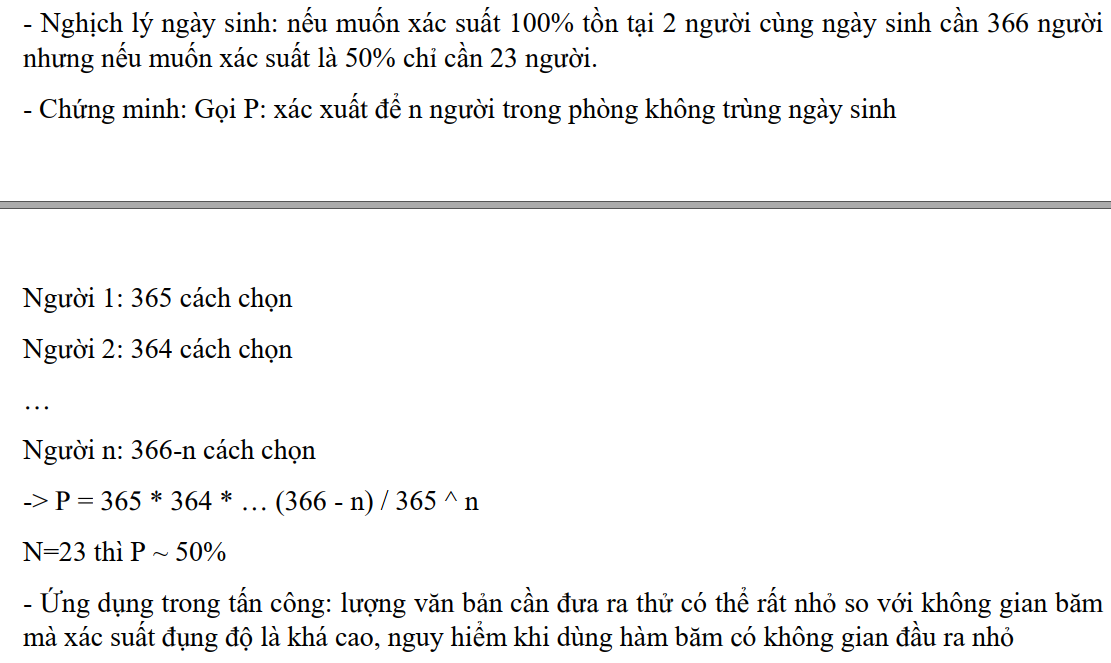


# 13. Trình bày nghịch lý ngày sinh, chứng minh công thức tổng quát của nghịch lý ngày sinh. Trình bày ứng dụng của nghịch lý ngày sinh trong tấn công vào chữ ký số.

Nghịch lý ngày sinh được phát biểu như sau

Trong 1 nhóm người , để có 100% khả năng có 2 người có cũng ngày sinh, ta cần ít nhất 366 người. Nhưng để có 50% khả năng có 2 người có cũng ngày sinh ta chỉ cần 23 người, một con số nhỏ hơn rất nhiều

Chứng minh



Ứng dụng:

* Kẻ tấn công có thể tạo ra các văn bản giả (có nội dung có hại cho bên kí) những vẫn có giá trị hàm băm giống văn bản gốc để lừa bên kí kí vào. Bằng cách thay đổi một số kí tự trong văn bản gốc (có thể là dấu cách, dấu câu, từ đồng nghĩa, …) sau đó tính giá trị băm của các văn bản, kẻ tấn công có thể tìm ra cặp văn bản có giá trị băm giống với văn bản gốc. Và theo nghịch lý ngày sinh thì kẻ tấn công có khả năng cao tìm được đụng độ chỉ với một lượng văn bản nhỏ hơn nhiều so với số văn bản có thể tạo ra.
* Từ công thức tổng quát có thể tính toàn được kích thước cần thiết cho đầu ra của hàm băm để có thể chống lại tấn công sử dụng nghịch lý ngày sinh một cách có hiệu quả

# 14. Tại sao cần sử dụng khóa phiên

* Tránh việc sử dụng một khóa nhiều lần, của khóa ngăn chặn kẻ tấn công sử dụng thống kê để phá khóa (vì sử dụng nhiều khóa ngẫu nhiên, mỗi khóa mã hóa một lượng nhỏ thông tin -→ kẻ tấn công sẽ có ít thông tin để phá khóa một cách hiệu quả).
* Đảm bảo tính mới của khóa. Giả sử như kẻ tấn công có thể phá được khóa, tuy nhiên thời gian phá khóa sẽ lâu hơn session → hết session thì khóa không còn sử dụng được nữa.
* Giảm thời gian tính toán (session key thường là mã đối xứng, nhanh hơn việc mã hóa bằng mã bất đối xứng).

# 15. Ý nghĩa của trong giao thức Needham-Shroeder. Trình bày chi tiết tấn công với giao thức Needham-Shroeder khi không có

- r1 là yếu tố ngẫu nhiên giúp ngăn chặn kiểu tấn công phát lại

- Khi không có r1, kẻ tấn công sẽ chặn gói tin C gửi cho A ở bước 2 và gửi cho A một gói tin trong quá khứ (kẻ tấn công không giải mã được gói tin này, nhưng kẻ tấn công vẫn tìm được k’[s] bằng cách phân tích các gói tin trao đổi bằng khóa phiên này trong quá khứ). A khi nhận được gói tin vẫn không biết đó là khóa phiên cũ nên vẫn sẽ trao đổi với B bằng khóa phiên k’[s].

# 16. Vai trò của bước 4,5 trong giao thức Needham-Shroeder. Trình bày chi tiết tấn công với giao thức Needham-Shroeder khi không hai bước này.

- Bước 4,5 nhầm xác minh A và B thực sự đang nắm khóa phiến k[s], chống tấn công phát lại. Nếu như kẻ tấn công chỉ đơn thuần phát lại từ 3 (kẻ tấn công lúc này không biết khóa k[s]), thì khi đó kẻ đó sẽ không tìm được r2 để đáp lại B.

- Nếu không có bước 4,5, kẻ tấn công có thể phát lại các gói tin cũ từ bước 3 trở đi mà B sẽ không có cách nào để xác thực được đó là A.

# 17. Giao thức Needham-Shroeder có điểm yếu gì, có thể khắc phục như thế nào

- Điểm yếu : Giả sử khóa k’[s] cũ đã bị kẻ tấn công tìm ra hoặc bị lộ, kẻ tấn công có thể phát lại k’[s] cũ ở bước 3, B sẽ không biết đó là khóa phiên cũ, tưởng kẻ tấn công là A muốn nhắn tin, nên sẽ tiếp tục gửi tin nhắn tới kẻ tấn công bằng khóa phiên cũ. Và đường nhiên do đã nắm được khóa k’ là gì rồi nên kẻ tấn công có thể dễ dàng giải mã r2 và xác thực với B mình là A

- Khắc phục: thêm timestamp vào khóa phiên ở bước 2

# 18. Giả sử A và B có cùng một bên tin cậy thứ 3 là C. A và B muốn thông qua C để thiết lập một khóa phiên với giao thức như sau:

* Table

  Description automatically generated

# Hãy cho biết giao thức này có điểm yếu gì, có thể khắc phục như thế nào

**Điểm yếu** của giao thưc này nằm ở bước 2. Kẻ tấn công có thể dùng phương thức replay attack.

* Đầu tiên kẻ tấn công thu thập gói trong quá khứ và các thông tin A và B dùng để trao đổi sử dụng khóa này. Kẻ tấn công sẽ dùng các thông tin thu được để tìm ra .
* Sau đó khi C gửi cho A gói tin chứa mã khóa phiên mới, kẻ tấn công sẽ chặn gói tin C gửi cho A và gửi lại cho A gói .
* A sẽ tưởng gói tin đó là từ C và sẽ tiếp tục gửi cho B khóa .Cả 2 sẽ trao đổi thông tin bằng khóa cũ này. Kẻ tấn công, dù không biết , vẫn có thể phá hoại trao đổi giữa A và B bằng khóa .

**Cách khắc phục**: thêm timestamp khi C gửi khóa phiên cho A như sau: . Như vậy nếu kẻ tấn công có dùng gói tin cũ thì 2 bên có thể phát hiện ra được

# 19. Tính nhanh

* 1. 28-1 mod 75

# A piece of paper with writing Description automatically generated with low confidence

# Text, letter Description automatically generated

# Text, letter Description automatically generated 20. Chứng minh: với nguyên tố

Theo định lý Fermat

Suy ra

Hay

Mà p,q là số nguyên tố, suy ra

Vậy

# 21. Chứng minh với là số nguyên dương bất kỳ và X nguyên tố cùng nhau với

Text, letter

Description automatically generated

# 22. Viết đoạn giả mã của thuật toán tính nghịch đảo đồng dư

Đầu vào n, m ( (n,m) = 1)

Đầu ra a là nghịch đảo đồng dư của n theo modulo m

Thuật toán:

* a1 = 1, b1 = 0, a2 = 0, b2 = 1
* Tính số chia q và số dư r khi chia n2 cho n1
* while r != 0
  + n1 = n2
  + n2 = r
  + t = a2
  + a2 = a1 – q \* a2
  + a1 = t
  + t = b2
  + b2 = b1 – q \*b2
  + b1 = t
  + Tính số chia q và số dư r khi chia n2 cho n1
* a = (a2 + m) % m

# 23. Chứng minh tính đúng đắn của phương pháp bình phương và nhân

# A picture containing text, document Description automatically generated 24. Tính nhanh

Ta có 3533 = 110111001101

