ĐỀ CƯƠNG

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

IC (chỉ số trùng lặp) là xác suất để 2 kí tự lấy ra từ một đoạn văn bản mà 2 kí tự đó trùng nhau. IC của ngôn ngữ tự nhiên là 0.068

Công thức tính chỉ số IC: $IC = \frac{\sum_{i=0}^{25} f_i \times (f_i - 1)}{n(n-1)}$

$$với\ f_i\ là\ tần\ suất\ của\ kí\ tự\ trong\ đoạn\ văn\ bản$$

Chứng minh:

Ta có: Giả sử đoạn văn bản có độ dài n, hay có n kí tự. Kí tự i (i từ 0 đến 25) có tần suất xuất hiện là f_i.

Xác suất để lấy được kí tự thứ nhất là kí tự i trong văn bản ban đầu (n kí tự): $\frac{f_i}{n}$

Xác suất để lấy được kí tự thứ hai là kí tự i trong văn bản là: $\frac{f_i - 1}{n-1}$

$$Vậy, xác\ suất\ để\ hai\ kí\ tự\ được\ chọn\ ngẫu\ nhiên\ là\ kí\ tự\ i\ là:$$

$$P = \frac{f_i}{n} \times \frac{f_i - 1}{n-1} = \frac{f_i \times (f_i - 1)}{n \times (n-1)} = IC$$

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

	Hệ mã công khai	Hệ mã bí mật
Ưu điểm	Tiết kiệm số lượng khóa cần quản lý	Quá trình mã hóa, giải mã diễn ra nhanh chóng, không mất nhiều thời gian
Nhược điểm	Quá trình mã hóa, giải mã mất nhiều thời gian	Số lượng khóa cần quản lý lớn (số lượng khóa tăng khi số lượng giao dịch tăng)

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

Tấn công biết bản rõ (known plaintext attack): khi kẻ tấn công biết một vài cặp bản mã và bản rõ, từ đó có thể dùng để tìm khóa từ hiểu biết về giao thức, kiểu tập tin hay các chuỗi đặc trưng có trong bản rõ.

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

IC (M) = 0.068 (= IC của ngôn ngữ tự nhiên)

IC (R) = IC (M) trong trường hợp bản mã R được mã hóa bằng cách sử dụng mã dịch hoặc mã một bảng thế, vì tần suất các kí tự xuất hiện trong R không đổi, bằng với tần suất xuất hiện trong bản rõ.

IC (R) < IC (M) trong trường hợp bản mã R được mã hóa bằng cách sử dụng đa bảng thế… vì khi đó, tần suất xuất hiện của các kí tự gần bằng nhau.

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.

Các nguyên tắc thiết kế mật mã khối an toàn:

- Khuếch tán: Mỗi một bit bản rõ và khóa phải ảnh hưởng lên nhiều bit của bản mã; mỗi bit của bản mã bị ảnh hưởng bởi nhiều bit của bản rõ. Mục đích nhằm gây khó khăn trong việc phá khóa dựa trên đặc tính thống kê.
- Hỗn loạn: Phức tạp hóa mỗi quan hệ giữa bản tn và bản mã, tốt nhất là dùng "phi tuyến".

Các kĩ thuật thiết kế đảm bảo nguyên tắc được thực hiện bằng các thuật toán thay thế phức tạp

6. Gọi DES là thuật toán mã hóa DES và DES^{-1} là thuật toán giải mã DES. Chứng minh $DES^{-1}(DES(X)) = X$

Ta có:

$DES\ (X) = (IP)^{-1} \times F_{16} \times T \times F_{15} \times T \times \dots T \times F_1 \times (IP) \times X$

$DES^{-1}(DES(X))$

$= (IP)^{-1} \times F_1 \times T \times \dots \dots \times F_{15} \times T \times F_{16} \times (IP).DES(X)$

$\rightarrow DES^{-1}(DES(X))$

$= (IP)^{-1} \times F_1 \times T \times \dots \dots \times F_{15} \times T \times F_{16} \times (IP) \times (IP)^{-1}$

$\times F_{16} \times T \times F_{15} \times T \times \dots T \times F_1 \times (IP) \times X$

Ta lại có:

$(IP) \times (IP)^{-1} = (IP)^{-1} \times IP = 1$

$F_{i\ .}\ F_i = F\ (\ F\ (L_{i-1}; R_{i-1})) =\ F(L_{i-1}\ xor\ f\ (R_{i-1}; K_i);\ R_{i-1})$

$= (L_{i-1}\ xor\ f\ (R_{i-1}; K_i))\ xor\ f(\ (R_{i-1}; K_i);\ R_{i-1})$

$= (\ L_{i-1};\ R_{i-1})$

$\rightarrow DES^{-1}(DES(X)) = X$ (điều phải chứng minh)

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 trúc Feistel bao gồm nhiều vòng lặp, bằng cách thực hiện hoán vị và thay thế. Đầu vòng của vòng lặp này là đầu ra của vòng lặp trước. Quá trình giải mã giống quá trình mã hóa, chỉ khác thứ tự khóa được sử dụng ngược lại.

Cần sử dụng nhiều vòng lặp để phù hợp với nguyên tắc khuếch tán và hỗn loạn.

Sự thực hiện ở các vòng lặp gần như giống nhau, khác nhau ở khóa con được sử dụng trong vòng lặp đó, ví dụ vòng 1 dùng khóa K1 và vòng 2 dùng khóa K2

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?

Trong thuật toán RSA, phải chọn p và q là hai số vì $n = p \times q$ *là một khóa công khai*. Nếu n nhỏ thì kẻ tấn công rất dễ phân tích n thành các số nguyên tố và suy ra p, q.

Nếu chỉ chọn một số lớn, một số nhỏ thì kẻ tấn công có thể dễ dàng phân tích và tìm ra số nhỏ, sau đó tìm ra số lớn.

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

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

Cần ký lên giá trị của hàm băm thay vì ký trực tiếp lên văn bản vì:

- Nếu ký trực tiếp lên văn bản : Vì kích thước chữ kí phụ thuộc vào kích thước văn bản, nên với các văn bản quá dài (dung lượng lớn), thì ta sẽ phải chia nhỏ bản tin trước khi gửi. Điều này sẽ giúp cho kẻ tấn công có thể lợi dụng sơ hở, tấn công bằng cách thay đổi thứ tự bản tin.
- Nếu kí lên giá trị hàm băm: Vì hàm băm là hàm một chiều, và đầu ra output là một chuỗi có độ dài xác định không phụ thuộc vào độ dài của bản mã, nên ta có thể giảm bớt khối lượng gói tin gửi đi. Ngoài ra, hàm băm còn có tính chất kiểm tra lỗi và tính không trùng lặp.

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.

Giả sử A cần phải kí lên văn bản m và gửi cho B. A sử dụng chữ kí số kí lên giá trị hàm băm H(m) và sau đó đóng gói chữ kí và văn bản, mã hóa gói tin bằng khóa công khai của thuật toán RSA gửi đi cho B.

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

Giả sử văn bản cần kí là m và A cần kí văn bản m và gửi cho B.

Giao thức tạo chữ kí số sử dụng mật mã khóa công khai:

- A sử dụng hàm băm H và input là m thu được H (m)
- A sử dụng hàm sinh chữ kí: $s = E_{pr\ A}\big(H(m)\big)$
- A gửi bản tin gồm văn bản m và chữ kí s cho B

Giao thức xác minh chữ kí số sử dụng hệ mật mã khóa công khai:

- B nhận được bản tin A gửi trên

- B lấy chữ kí s, và giải mã s thu được giá trị hàm băm$H(n) = D_{pr\ A}(s)$
- B sử dụng hàm băm H và input là văn bản m thu được H(m)
- So sánh H(n) và H(m), nếu 2 giá trị bằng nhau thì xác minh được chữ kí s chính là chữ kí của A trên văn bản m.

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: trong phòng có n người.

- Để xác suất chọn 2 người ngẫu nhiên trong phòng có cùng ngày sinh là 100% thì $n \geq 366$.
- Để xác suất chọn 2 người ngẫu nhiên trong phòng có cùng ngày sinh lớn hơn 50% thì $n \geq 23$.

Chứng minh công thức tổng quát của nghịch lý ngày sinh:

Ta có: trong phòng có n người, nên không gian mẫu $n(\Omega) = 365^n$

Để mỗi người có một ngày sinh, không ai trùng ai thì có: A_{365}^{n}

Vậy, xác suất để có hai người trong phòng có cùng ngày sinh là: $P = 1 - \frac{A_{365}^{n}}{365^n}$

$$P = 1 \rightarrow n \geq 366 \text{ và } P \geq 0.5 \rightarrow n \geq 23$$

Ứng dụng của nghịch lý ngày sinh trong tấn công chữ kí số là:

A là thư kí và có văn bản X cần B kí, và A là người tấn công. A tạo ra các văn bản đúng $((X1, X2, \dots . Xk)$ và văn bản $(f1, f2, \dots fk)$. A cần tìm 2 văn bản Xi và fj sao cho H(Xi) = H(fj).

A sẽ chọn văn bản Xi để B kí, sau đó, A lấy chữ kí s của B trên H(Xi) ghép vào văn bản H(fi) và gửi đi cho bên xác nhận.

Ứng dụng của nghịch lý: nếu A tạo ra các văn bản trên với $k \approx \sqrt{N}$ (N là khoảng không gian, số giá trị của hàm băm H) thì xác suất A tìm được 2 văn bản Xi và fj sao cho H(Xi) = H(fj) là lớn hơn hoặc bằng 50%.

14. Tại sao cần sử dụng khóa phiên

Cần sử dụng khóa phiên vì khóa phiên có các tính chất:

- Gắn với một phiên giao dịch
- Là khóa bí mật, chỉ dùng để mã hóa thông tin
- Không dùng để xác thực chủ thể
- Đảm bảo tính mới của khóa, dù kẻ tấn công phá được khóa trong quá khứ thì rất khó có thể lợi dụng để tấn công trong tương lai.

15. Ý nghĩa của r_1 trong giao thức Needham-Shroeder. Trình bày chi tiết tấn công với giao thức Needham-Shroeder khi không có r_1.

Ý nghĩa của r1 trong giao thức Needham-Shroeder là: r1 được sử dụng ở bước 1 và 2, với mục đích để kẻ tấn công không thể giả mạo Cathy ở bước 2, gửi cho Alice gói tin cũ mà hắn bắt phá được trong quá khứ.

Giao thức Needham-Shroeder khi không có r1:

Bước	Người gửi	Gói tin	Người nhận
1	Alice	Alice||Bob	Cathy
2	Cathy	{Alice||Bob||kS||$\{Alice\|\|kS\}_{kBC}\}_{kAC}$	Alice
3	Alice	$\{Alice\|\|kS\}_{kBC}$	Bob
4	Bob	$\{r2\}_{kS}$	Alice
5	Alice	$\{r2-1\}_{kS}$	Bob

Kẻ tấn công có thể chặn ở giữa Alice và Cathy, sau khi bắt được gói tin Alice gửi Cathy ở bước 1, hắn sẽ giả mạo Cathy gửi cho Alice gói tin {Alice||Bob||kS||$\{Alice||kS\}_{kBC}\}_{kAC}$ mà hắn bắt được trong quá khứ, nhằm mục đích đánh lừa Alice và Bob giao dịch với nhau bằng khóa phiên kS cũ (khóa mà kẻ tấn công đã phá được)

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.

Vai trò của bước 4, 5 tránh việc kẻ tấn công chặn ở giữa Alice và Bob, sau khi bắt được gói tin Alice gửi Bob ở bước 3, hắn không thể giả mạo Bob để giao dịch với Alice

Giao thức Neefham-Shroeder khi không có 2 bước 4 và 5

Bước	Người gửi	Gói tin	Người nhận
1	Alice	Alice||Bob||r1	Cathy
2	Cathy	{Alice||Bob||r1||kS||$\{Alice\|\|kS\}_{kBC}\}_{kAC}$	Alice
3	Alice	$\{Alice\|\|kS\}_{kBC}$	Bob

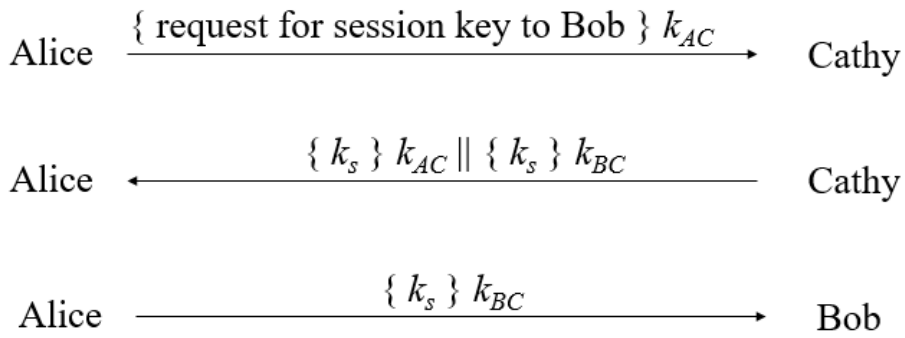
Kẻ tấn công có thể chặn giữa Alice và Bob ở bước 3, và giả mạo Alice gửi gói tin $\{Alice||kS\}_{kBC}$ cũ mà hắn phá được trong quá khứ, nhằm mục đích đánh lừa Bob giao dịch với hắn bằng khóa phiên kS cũ, trong lúc đó Bob vẫn nghĩ kẻ tấn công là Alice.

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

Điểm yếu: Ở giao thức Needham-Shroeder, kẻ tấn công có thể giả mạo Alice ở bước 3, và gửi cho Bob bản tin $\{Alice\ ||\ kS\}_{kBC}$ mà họ thu lấy được từ trong quá khứ. Sau đó, lấy các thông tin mà Bob gửi cho Alice qua khóa kS.

Khắc phục: Thêm dữ liệu timestamp T vào bản tin mà Cathy gửi cho Alice: $\{Alice \,||\, kS\}_{kBC} \rightarrow \{Alice \,||kS||T\}_{kBC}$

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 k_s với giao thức như sau:



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

Điểm yếu: Kẻ tấn công có thể tấn công chặn giữa Alice và Cathy ở bước 1, sau đó sẽ giả mạo Cathy gửi cho Alice bản tin $\{kS\}_{kAC}||\{kS\}_{kBC}$ cũ mà hắn lấy được trong quá khứ, nhằm lừa Alice và Bob giao dịch bằng khóa kS.

Khắc phục: Quy ước bổ sung dữ liệu timestamp T vào bản tin $\{kS||T\}_{kAC}||\{kS||T\}_{kBC}$ để kẻ tấn công không thể sử dụng lại bản tin cũ kia.

19. Tính nhanh

a) 28^{-1} mod 75

Ta có:

$$\begin{cases} 75 = 28.2 + 19 \\ 28 = 19.1 + 9 \\ 19 = 9.2 + 1 \\ 9 = 9.1 \end{cases} \rightarrow \begin{cases} 1 = 19 - 9.2 = (28 - 9) - 9.2 = 28 - 9.3 \\ = 19.1 - 9.2 = 19.1 - (28 - 9.1).2 \\ = 19.3 - 28.2 = 75.3 - 28.8 \end{cases}$$

$$Vậy\ -8 = 67 = 28^{-1} mod\ 75$$

b) $17^{-1}\ mod\ 101$

Ta có:

$$\begin{cases} 101 = 17.5 + 16 \\ 17 = 16.1 + 1 \\ 16 = 1.16 \end{cases} \rightarrow \begin{cases} 1 = 17 - 16.1 \\ = 17 - (101 - 17.5) \\ = 17.6 - 101 \end{cases}$$

$$Vậy\ -6 = 107 = 17^{-1} mod\ 101$$

c) $357^{-1}\ mod\ 1234$

Ta có:

$$\begin{cases} 1234 = 357.3 + 163 \\ 357 = 163.2 + 31 \\ 163 = 31.5 + 8 \\ 31 = 8.3 + 7 \\ 8 = 7.1 + 1 \\ 7 = 1.7 \end{cases} \rightarrow \begin{cases} 1 = 8 - 7.1 = 8 - (31 - 8.3) = 8.4 - 31 \\ = (163 - 31.5).4 - 31 = 163.4 - 31.21 \\ = 163.4 - (357 - 163.2).21 \\ = 163.46 - 357.21 \\ = (1234 - 357.3).46 - 357.21 \\ = 1234.46 - 357.159 \end{cases}$$

$$Vậy\ -159 = 1075 = 357^{-1} mod\ 1234$$

$d)\ 3125^{-1}\ mod\ 9987$

Ta có:

$$\begin{cases} 9987 = 3125.3 + 612 \\ 3125 = 612\ .5 + 65 \\ 612 = 65.9 + 27 \\ 65 = 27.2 + 11 \\ 27 = 11.2 + 5 \\ 11 = 5.2 + 1 \\ 5 = 1.5 \end{cases} \rightarrow \begin{cases} 1 = 11 - 5.2 = 11 - (27 - 11.2).2 \\ = 11.5 - 27.2 = (65 - 27.2).5 - 27.2 \\ = 65.5 - 27.12 = 65.5 - (612 - 65.9).2 \\ = 65.113 - 612.12 \\ = (3125 - 612.5).113 - 612.12 \\ = 3125.113 - 612.577 \\ = 3125.1844 - 9987.577 \end{cases}$$

$$Vậy\ 1184 = 3125^{-1} mod\ 9987$$

20. Chứng minh: $X^{(p-1)(q-1)} \equiv 1\ (mod\ pq)$ với $p,\ q$ nguyên tố

Áp dụng Fermat:

$$\begin{cases} x^{p-1} \equiv 1(mod\ p) \\ x^{q-1} \equiv 1(mod\ q) \end{cases} \rightarrow \begin{cases} x^{(p-1)(q-1)} \equiv 1(mod\ p) \\ x^{(q-1)(p-1)} \equiv 1(mod\ q) \end{cases}$$

$$Vậy, x^{(p-1)(q-1)} - 1\ chia\ hết\ p.q\ hay X^{(p-1)(q-1)} \equiv 1\ (mod\ pq)$$

21. Chứng minh $X^{\varphi(n)} \equiv 1\ (mod\ n)$ với n là số nguyên dương bất kỳ và X nguyên tố cùng nhau với n

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

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

24. Tính nhanh: $9726^{3533}\ (mod\ 11413)$

$3533 = 2^{11} + 2^{10} + 2^8 + 2^7 + 2^6 + 2^3 + 2^2 + 2^0 = (1101\ 1100\ 1101)_2$

$z = 1$

$i = 11; a11 = 1: z \leftarrow z^2.x = 1^2.9726 \equiv 9726(mod\ 11413)$

$i = 10; a10 = 1: z \leftarrow z^2.x = 9726^2.9726 \equiv 4132.9726 \equiv 2659(mod\ 11413)$

$i = 9; a9 = 0: z \leftarrow z^2 = 2659^2 \equiv 5634(mod\ 11413)$

$i = 8; a8 = 1: z \leftarrow z^2.x = 5634^2.9726 \equiv 2403.9726 \equiv 9167(mod\ 11413)$

$i = 7; a7 = 1: z \leftarrow z^2.x = 9167^2.9726 \equiv 11383.9726 \equiv 4958(mod\ 11413)$

$i = 6; a6 = 1: z \leftarrow z^2.x = 4958^2.9726 \equiv 9575.9726 \equiv 7783(mod\ 11413)$

$i = 5; a5 = 0: z \leftarrow z^2 = 7783^2 \equiv 6298(mod\ 11413)$

$i = 4; a4 = 0: z \leftarrow z^2 = 6298^2 \equiv 4629 (mod\ 11413)$

$i = 3; a3 = 1: z \leftarrow z^2 . x = 4629^2 . 9726 \equiv 5440.9726 \equiv 10185 (mod\ 11413)$

$i = 2; a2 = 1: z \leftarrow z^2 . x = 10185^2 . 9726 \equiv 1486.9726 \equiv 105 (mod\ 11413)$

$i = 1; a1 = 0: z \leftarrow z^2 = 105^2 \equiv 11025 (mod\ 11413)$

$i = 0; a0 = 1: z \leftarrow z^2 . x = 11025^2 . 9726 \equiv 2175.9726 \equiv 5761 (mod\ 11413)$

$$V\hat{a}y\ 5761 = 9726^{3533} (mod\ 11413)$$