ĐỀ CƯƠNG

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

- Chỉ số trùng lặp là xác suất để 2 thành phần ngẫu nhiên của 1 chuỗi có độ dài n là trùng nhau, thể hiện độ không đồng đều của các tần suất xuất hiện các chữ cái

- Công thức: $IC(x) = \frac{\sum_{i=0}^{25} f_i(f_i - 1)}{n(n-1)}$, trong đó f_i là tần số xuất hiện của kí tự thứ i trong x

- Chứng minh công thức: xác suất để chọn ra 2 thành phần trùng nhau là $[f_i(f_i-1)]/[n(n-1)]$, có 26 chữ cái nên ta có công thức như trên

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	Dễ dàng trao đổi khóa công khai Mỗi người chỉ quản lý 1 bộ khóa	Đơn giản
Nhược điểm	Phức tạp hơn, tốn chi phí hơn	Vấn đề chia sẻ khóa bí mật Mỗi người phải quản lý nhiều khóa khi muốn trao đổi với nhiều người

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: Kẻ tấn công biết một số cặp bản rõ và bản mã tương ứng nào đó, để tìm ra bản rõ khác hoặc khóa

- Ví dụ: Với các hệ mật mã có không gian khóa nhỏ, sau khi thu thập đủ 1 số lượng cặp bản rõ và bản mã tương ứng, do toàn bộ thuật toán mã hóa thường là công khai nên kẻ tấn công có thể vét cạn hay thống kê để tìm ra khóa

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

- $IC(M) \geq IC(R)$, vì tần số xuất hiện các thành phần của R đồng đều hơn M, theo bất đẳng thức Cauchy thì IC đạt giá trị nhỏ nhất khi các tần số có giá trị "gần" bằng nhau. Ngoài ra, khi tần số khác nhau. IC bị ảnh hưởng bởi tần số có giá trị lớn

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 thiết kế:

  Khuếch tán: khuếch tán đặc tính thống kê của bản tin vào bản mã -> thực hiện nhiều lần thao tác hoàn vị + tác động thuật toán

  Hỗn loạn: sự phụ thuộc của bản mã đối với bản tin phải càng phức tạp càng tốt -> dùng 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 $DES^{-1}\big(DES(X)\big) = X$

- $(L_i, R_i) = (R_{i-1}, L_{i-1} + f(R_{i-1}, K_i) = T \,.\, F(L_{i-1}, R_{i-1})$

  -> $DES = IP^{-1}.F_{16}.T.F_{15}.T\ldots F_2.T.F_1.IP$; $DES^{-1}=IP^{-1}.F_1.T.F_2\ldots F_{15}.T.F_{16}.IP$

- Do $IP.IP^{-1}=1$ và $F_i.F_i=(L_{i-1}, R_{i-1})$ nên $DES^{-1}(DES(X)) = X$

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 là 1 cấu trúc bao gồm nhiều vòng lặp, mỗi vòng lặp sẽ thực hiện các thao tác hoán vị và thay thế, đầu vào của vòng lặp là đầu ra của vòng lặp trước đó và 1 khóa con được sinh ra từ khóa đầy đủ bởi thuật toán sinh khóa, giải mã là một quá trình ngược với các khóa on được phát sinh ngược lại

- Cần nhiều vòng lặp để đảm bảo tính khuếch tán và hỗn loạn

- Sự thực hiện ở các vòng lặp không hoàn toàn giống nhau do sử dụng khóa con khác nhau được sinh ra từ khóa đầy đủ bởi thuật toán sinh khóa

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?

- Nên chọn 2 số p, q đều lớn vì để đảm bảo độ an toàn của thuật toán, nếu chọn 1 số lớn và 1 số nhỏ thì kẻ tấn công có thể nhanh chóng vét cạn để tìm ra 2 số này bởi n=p.q là công khai, từ đó sử dụng khóa công khai e để tìm ra các khóa bí mật

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

- Vì các thuật toán liên quan tới e, e đều ở số mũ sau đó lấy đồng dư với n, d phụ thuộc e theo đồng dư với m. Với mỗi e lớn hơn m luôn có một e khác nhỏ hơn m có cùng kết quả khi tính đồng dư m, n. Ngoài ra khi, e lớn thì tính toán lâu hơn

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

- Vì khi ký trực tiếp lên văn bản thì tốc độ chậm, kích thước chữ ký lớn. Ngoài ra khi bản tin quá dài, cần chia nhỏ, khi đó kẻ tấn công thay đổi thứ tự hay thêm bớt các phân mảnh sẽ gây khó khăn, thiệt hại. Trong khi hàm băm là hàm biến đổi 1 chuỗi KT có độ dài bất kỳ thành 1 chuỗi ký tự có độ dài cố định, vì vậy nên ký lên giá trị của hàm băm

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.

- Quá trình tạo và kiểm tra chữ ký số sử dụng 3 thuật toán:

Thuật toán tạo khóa bí mật và công khai.

Thuật toán tạo chữ ký số bằng khóa bí mật.

Thuật toán kiểm tra chữ ký số bằng khóa công khai.

- Ví dụ:

Giả sử Bob muốn gửi một văn bản cho Alice và muốn Alice biết văn bản đó thực sự do chính Bob gửi. Khi đó, Bob gửi cho Alice một văn bản điện tử kèm với chữ ký số. Chữ ký này được tạo ra với khóa bí mật của Bob.

Khi nhận được bản tin, Alice kiểm tra sự thống nhất giữa văn bản và chữ ký bằng thuật toán kiểm tra sử dụng khóa công khai của Bob. Bản chất của thuật toán tạo chữ ký đảm bảo rằng nếu chỉ cho trước văn bản, rất khó (gần như không thể) tạo ra được chữ ký số của Bob nếu không biết khóa bí mật của Bob. Nếu phép thử cho kết quả đúng thì Alice có thể tin tưởng rằng bản tin thực sự do Bob gửi.

Thông thường, để tránh mất thời gian, Bob không mật mã hóa toàn bộ văn bản bằng khóa bí mật của mình, mà chỉ thực hiện với mã băm, hay còn gọi là giá trị băm, đại diện và đặc trưng cho văn bản đó. Điều này khiến việc ký số của Bob trở nên đơn giản hơn và chữ ký số trở nên ngắn hơn. Xác suất xảy ra trường hợp 2 văn bản khác nhau lại cho ra cùng một giá trị băm là cực kỳ thấp.

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

1. Sinh chữ ký: $s=E_{PrA}(H(M))$ -> M||s

2. Xác minh chữ ký: D_{PbA} eq H(M) = true if $D_{PbA}(s)=H(m)$; false if $D_{PbA}(s)\#H(m)$

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: nếu muốn xác suất 100% tồn tại 2 người cùng ngày sinh cần 366 người nhưng nếu muốn xác suất là 50% chỉ cần 23 người.

- Chứng minh: Gọi P: xác xuất để n người trong phòng không trùng ngày sinh

Người 1: 365 cách chọn

Người 2: 364 cách chọn

…

Người n: 366-n cách chọn

-> P = 365 * 364 * … (366 - n) / 365 ^ n

N=23 thì P ~ 50%

- Ứng dụng trong tấn công: lượng văn bản cần đưa ra thử có thể rất nhỏ so với không gian băm mà xác suất đụng độ là khá cao, nguy hiểm khi dùng hàm băm có không gian đầu ra nhỏ

14. Tại sao cần sử dụng khóa phiên

- Vì để hạn chế lượng thông tin được mã hóa với cùng 1 khóa, đảm bảo tính mới của khóa và giảm thời gian tính toán

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 r_1 là yếu tố ngẫu nhiên để chống phát lại

- Khi không có r_1, kẻ tấn công chặn gói tin ở bước 2 mà KDC gửi cho A, sau đó thay thế K_S bằng khóa của kẻ tấn công

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 là để xác minh rằng A và B đang thực sự nói chuyện với nhau, chống kẻ tấn công phát lại

- Nếu không có hai bước này thì Alice và Bob sẽ trao đổi thông tin ngay với nhau bằng khóa K_S từ bước 4. Mặc dù vậy, khi có bước 4, 5 hay không thì kẻ tấn công đều có thể phát lại ở bước 3 khi biết 1 K_S trong quá khứ

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

- Nếu kẻ tấn công biết 1 khóa phiên trong quá khứ thì sẽ phát lại ở bước 3 và xác minh được với Bob

- Khắc phục: thêm timestamp 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 k_s với giao thức như sau:

Alice $\xrightarrow{\{\text{ request for session key to Bob }\}\ k_{AC}}$ Cathy

Alice $\xleftarrow{\{\ k_s\ \}\ k_{AC} \,\|\, \{\ k_s\ \}\ k_{BC}}$ Cathy

Alice $\xrightarrow{\{\ k_s\ \}\ k_{BC}}$ Bob

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

- Điểm yếu: kẻ tấn công phát lại ở bước 3 mà Bob vẫn nghĩ là A do không có cơ chế kiểm tra K_S
- Khắc phục: thêm yếu tố ngẫu nhiên như giao thức Needman-schroeder

19. Tính nhanh

1. 28^{-1} mod 75
2. $17^{-1}\ mod\ 101$
3. $357^{-1}\ mod\ 1234$
4. $3125^{-1}\ mod\ 9987$

Đã làm trên lớp

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

Đã làm trên lớp

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

X = a

Gọi $a_1, a_2, \cdots, a_{\varphi(n)}$ là các số nguyên dương nhỏ hơn n và nguyên tố cùng nhau với n. Với mọi 2 số phân biệt $i, j \in \{1, 2, \cdots, \varphi(n)\}$:
$(a_i, n) = (a_j, n) = 1 \Rightarrow (aa_i, n) = (aa_j, n) = 1; aa_i \not\equiv aa_j \pmod{n}$. Do vậy, $aa_1, aa_2, \cdots, aa_{\varphi(n)}$ là một hoán vị theo mô-đun n của $a_1, a_2, \cdots, a_{\varphi(n)}$.

Suy ra $a_1 a_2 \cdots a_{\varphi(n)} \equiv (aa_1)(aa_2)\cdots(aa_{\varphi(n)}) \equiv a^{\varphi(n)} a_1 a_2 \cdots a_{\varphi(n)} \pmod{n}$.

Giản ước đồng dư thức, $a^{\varphi(n)} \equiv 1 \pmod{n}$.

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

Đã làm trên lớp

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

Đã làm trên lớp

24. Tính nhanh

$$9726^{3533} \ (mod\ 11413)$$

Đã làm trên lớp