**Họ và tên: Nguyễn Sỹ Lợi**

**MSSV: 20194097**

**GIẢI ĐỀ CƯƠNG**

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

Text

Description automatically generated

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

Table

Description automatically generated

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

Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

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

Text

Description automatically generated

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

Text

Description automatically generated

Text, letter

Description automatically generated

Text, letter

Description automatically generated

A screenshot of a computer

Description automatically generated with medium confidence

Text, letter

Description automatically generated

Text

Description automatically generated

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

Chứng minh

Text, letter

Description automatically generated

Text, letter

Description automatically generated

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?

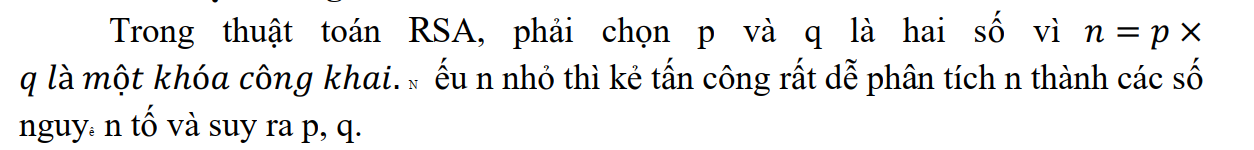
Text, letter

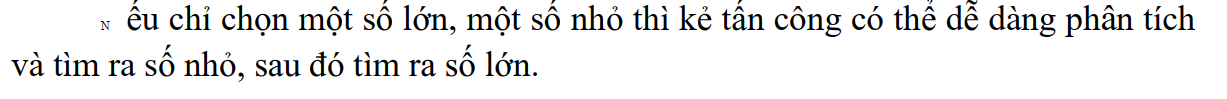
Description automatically generated

Text

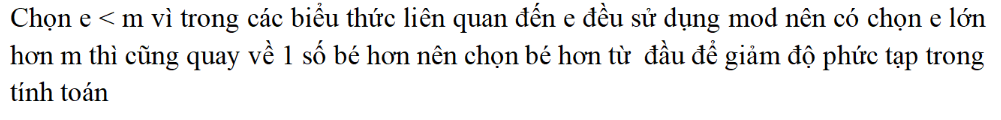
Description automatically generated

**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?**





**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

Text

Description automatically generated

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

Description automatically generated

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

A picture containing text, device

Description automatically generated

Text, letter

Description automatically generated

Text

Description automatically generated

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.

Text

Description automatically generated

Text

Description automatically generated

Text, letter

Description automatically generated

14. Tại sao cần sử dụng khóa phiên

• Để hạn chế lượng thông tin được mã hoá với cùng 1 khoá

• Đảm bảo tính mới của khoá

• Giảm thời gian tính toán, Khóa công khai dùng lũy thừa, đồng dư lâu, Khóa

đối xứng thì tính toán chỉ dùng phép tính đơn giản như hoán vị, ...

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

Table

Description automatically generated

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.

**Text

Description automatically generated**

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

Text

Description automatically generated

Graphical user interface, text, application, table

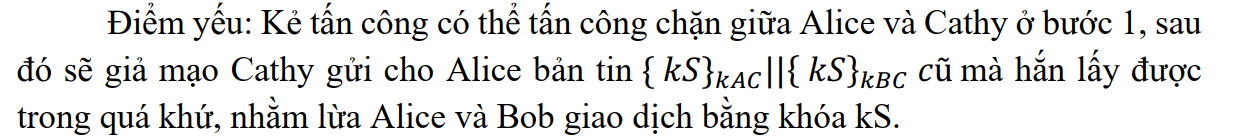
Description automatically generated

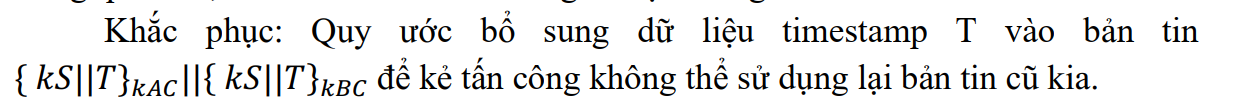
18. Giả sử A và B có cùng một bên tin cậy thứ 3 là C. A và B muốn thông qua C để thiết lập một khóa phiên với giao thức như sau:

Table

Description automatically generated

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





19. Tính nhanh

* 1. 28-1 mod 75

Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

20. Chứng minh: với nguyên tố

Text, letter

Description automatically generated

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

**Graphical user interface, text, application

Description automatically generated**

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

**Text

Description automatically generated**

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

**Graphical user interface, text, application, letter

Description automatically generated**

24. Tính nhanh

**Text, letter

Description automatically generated**

Text, letter

Description automatically generatedCâu 2: a. - A muốn gửi một đoạn tin mA cho B - A băm mA, thu được hA = Hash(mA) - A dùng khóa bí mật dA kí lên hA, thu được chữ kí sA = D(dA, hA) - A ghép mA với sA lại, mã hóa bằng khóa công khai eB của B, thu được cA = E(eB, mAsA) - A gửi cA cho B - B nhận được cA - B dùng khóa bí mật dB giải mã thu được mAsA = D(dB, E(eB, mA||sA)) - B băm mA, thu được hA = Hash(mA) - B kiểm tra hA = E(eA, sA) ?, nếu đúng thì tin của A gửi đảm bảo tính mật, tính toàn vẹn và tính xác thực - B muốn gửi tin cho A, thực hiện tương tự

b. Giải thích:

- Tính toàn vẹn: Do tính chất của hàm Hash, đoạn tin đầu vào dù chỉ bị sai sót, mất mát 1 bit cũng sẽ cho ra kết quả hoàn toàn khác, nên hàm Hash cho ra hA mang tính đảm bảo rằng đoạn tin mA không bị mất mát, sai sót

- Tính mật: Do chỉ có B có khóa bí mật dB mới giải mã được đoạn mã cA mà A gửi cho B, do vậy đoạn mã đó đảm bảo tính mật, không ai ngoài A và B có thể biết được nội dung của mA

- Tính xác thực: do chỉ có A có khóa bí mật dA nên chỉ có A mới tạo ra được chữ kí sA, sau đó B hay tất cả mọi người biết khóa công khai eA của A đều có thể dùng để xác thực 1 văn bản mA có phải do A viết hay không.