**BUỔI 1: MẬT MÃ CỔ ĐIỂN – ĐỀ CƯƠNG**

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

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

4. Tại sao không thể nói mọi khóa của mật mã một bảng thế đều an toàn như nhau

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

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

7. Gọi DES là thuật toán mã hóa DES và DES-1 là thuật toán giải mã DES.

Chứng minh DES-1(DES(X)) = X

8. 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?

**BUỔI 1 – GỢI Ý TRẢ LỜI**

*Chú ý: các gợi ý dưới đây chỉ là các ý chính, không phải là câu trả lời đầy đủ. Sinh viên cần tự mình suy nghĩ để tìm ra câu trả lời hoàn chỉnh, đầy đủ.*

1. Định nghĩa chỉ số trùng lặp: Chỉ số trùng lặp của một tập hợp là xác suất để hai phần tử ngẫu nhiên của tập hợp đấy trùng nhau.

Công thức tính: xem giáo trình trang 39

Gợi ý chứng minh công thức:

Để ý rằng chính là xác xuất để hai phần tử ngẫu nhiên có cùng giá trị là phần tử thứ i trong tập giá trị của các phần tử của tập hợp.

1. Mã bí mật (mã đối xứng):

+ ưu điểm: đơn giản, nhanh

+ nhược điểm: kém an toàn, quản lý khóa phức tạp, không gắn liền với cá nhân nên không sử dụng được trong các ứng dụng xác thực danh tính, …

Mã công khai (mã phi đối xứng):

+ ưu điểm: độ an toàn cao, quản lý khóa đơn giản, dung được tỏng các ứng dụng xác thực danh tính, …

+ nhược điểm: cồng kềnh, xử lý chậm, …

1. Định nghĩa tấn công biết bản rõ: xem sách giáo khoa

Ví dụ: tự tìm hiểu

1. Chỉ ra một ví dụ cụ thể về một khóa mà kẻ tấn công dễ dàng phá nhanh chóng. Để ý rằng mã dịch (shift cipher) cũng là một trường hợp đặc biệt của mã một bảng thế.
2. Để ý rằng độ ngẫu nhiên của các ký tự trong văn bản càng lớn thì IC càng nhỏ (hãy chứng minh cụ thể nhận xét này). Vì vậy, IC của bản mã ngẫu nhiên sẽ nhỏ hơn IC của bản rõ (Hãy suy nghĩ xem tại sao lại như vậy).
3. Xem slide và giáo trình trang 48,49.
4. Xem giáo trình trang 53, 54. Chú ý cần chứng minh tính đối hợp của hàm T và hàm F.
5. Cấu trúc Feistel: xem slide.

Tại sao cần sử dụng nhiều vòng lặp: để đảm bảo tính khuếch tán

Sự thực hiện ở các vòng lặp có hoàn toàn giống nhau không: cấu trúc của các vòng lặp hoàn toàn giống nhau, chỉ khác ở các tham số đầu vào và khóa được sử dụng.