**BUỔI 3: CHỮ KÝ SỐ VÀ HÀM BĂM – ĐỀ CƯƠNG**

1. Nêu lý do tại sao cần ký lên giá trị của hàm băm thay vì ký trực tiếp lên văn bản
2. 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.
3. Trình bày giao thức tạo và xác minh chữ ký số sử dụng hệ mật mã khóa công khai
4. 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.

**BUỔI 3 – 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. Xem giáo trình trang 86
2. Để ý rằng để đảm bảo tính mật thì ta thường dùng các kỹ thuật để mã hóa gói tin nhằm đảm bảo chỉ người nào có khóa mới có thể giải mã và đọc được nội dung bản rõ.

Để đảm bảo tính xác thực, ta cần thêm chữ ký điện tử vào văn bản cần xác thực.

Để đảm bảo tính toàn vẹn của gói tin, ta thường gửi kèm giá trị hàm băm của gói tin.

Như vậy, giao thức thỏa mãn các yêu cầu của đề bài là giao thức vừa sử dụng kỹ thuật mã hóa để mã hóa gói tin, vừa có thêm chữ ký điện tử để xác thực gói tin, vừa truyền thêm giá trị hàm băm của gói tin.

Sau đây là một ví dụ đơn giản

Giả sử A cần gửi cho B 1 bản tin với nội dung là *m*, A sẽ gia cố gói tin *m* như sau trước khi gửi: )

Trong đó lần lượt là khóa công khai của B và khóa bí mật của A. E là hàm mã hóa, H là hàm băm.

Sau khi B nhận được gói tin, B sẽ dùng khóa bí mật của mình để giả mã , dùng khóa công khai của A để tìm ra H(m). B cũng tự mình tính giá trị băm của m và so sánh với giá trị H(m) vừa giải mã để kiểm tra chữ ký điện tử của A cũng như tính toàn vẹn của gói tin.

Chú ý: trên đây chỉ nêu gợi ý, sinh viên cần trình bày tường minh, mạch lạc và chứng minh tính đúng đắn của giao thức do mình đề xuất. Khuyến khích sinh viên tự nghĩ ra các giao thức khác.

1. Xem slide
2. + Nghịch lý ngày sinh: xem sách giáo trình trang 89

+ Nghịch lý ngày sinh tổng quát: xem sách giáo trình trang 90

+ Gợi ý chứng minh: xác suất để tồn tại hai phần tử có cùng giá trị băm = 1 – xác suất để tất cả các phần tử đều có giá trị băm khác nhau.

xác suất để tất cả các phần tử đều có giá trị băm khác nhau có thể tính được dễ dàng.

+ Ứng dụng nghịch lý ngày sinh tấn công chữ ký điện tử:

Xét kịch bản như sau: có một ông giám đốc, ông giám đốc này có một cô thư ký. Mọi văn bản của công ty đều được thực hiện theo quy trình như sau:

Cô thư ký soạn văn bản 🡪 cô thư ký gửi văn bản qua mail cho ông giám đốc 🡪 ông giám đốc gửi lại cho cô thư ký văn bản có gắn chữ ký điện tử của ông ta 🡪 cô thư ký gửi văn bản với chữ ký của giám đốc đến địa chỉ cần gửi.

Nếu cô thư ký là một người xấu, cô ta có thể giả mạo chữ ký của ông giám đốc như sau:

* giả sử cô ta cần soạn văn bản với nội dung X và đưa cho ông giám đốc ký.

Vậy thì, cô ta sẽ soạn *n* biến thể của X. Gọi tập biến thể này là tập A.

* Cô ta cũng đồng thời soạn *n* biến thể của văn bản với nội dung mà cô ta mong muốn. Gọi tập biến thể này là tập B.

Sau đó, cô ta chọn ra trong tập A và tập B, mỗi tập 1 biến thể sao cho 2 biến thể này có cùng giá trị hàm băm. Sau đó cô ta đưa biến thể được chọn ở tập A cho ông giám đốc ký và lấy chữ ký đó để gắn vào biến thể được chọn ở tập B.

Hãy chứng minh rằng, nghịch lý ngày sinh cho thấy rằng cách làm của cô thư ký này sẽ có khả năng thành công cao.