Faculty of Computer Science and Engineering
Ho Chi Minh City University of Technology

CRYPTOGRAPHY AND NETWORK SECURITY

Lab 6

Nguyen Phuong Vuong - 1614186

Questions.

1. List two disputes that can arise in the context of message authentication.

- Alice có thể giả mạo một thông điệp khác và cho rằng nó đến từ Bob bằng cách Alice chỉ cần tạo một tin nhắn khác và gán thêm mã xác thực bằng khóa mà Bob và Alice đã chia sẻ cho nhau.
- Bob có thể từ chối rằng mình đã gửi tin nhắn. Bởi vì Alice có thể giả mạo một tin nhắn, không có cách nào để chứng minh rằng Bob thực tế đã gửi tin nhắn.

2. What are the properties a digital signature should have?

- Có thể xác minh tác giả, ngày và giờ của chữ ký.
- Có khả năng xác thực nội dung tại thời điểm ký.
- Chữ ký phải được bên thứ ba kiểm chứng để có thể giải quyết tranh chấp.

3. What requirements should a digital signature scheme satisfy?

- Chữ ký phải là một mẫu bit phụ thuộc vào thông điệp được ký.
- Chữ ký phải sử dụng một số thông tin duy nhất cho người gửi, để ngăn chặn cả giả mạo và từ chối.
- Nó phải tương đối dễ dàng để tạo chữ ký số.
- Nó phải tương đối dễ dàng để nhận ra và xác minh chữ ký số.
- Phải giả mạo không thể giả mạo chữ ký số, bằng cách xây dựng một tin nhắn mới cho chữ ký số hiện có hoặc bằng cách xây dựng chữ ký số lừa đảo cho một tin nhắn cụ thể.
- Phải giữ lại một bản sao chữ ký số trong bộ lưu trữ.

4. What is the difference between direct and arbitrated digital signature(chữ ký kỹ thuật số phân xử)?

- Chữ ký số trực tiếp chỉ liên quan đến các bên giao tiếp (tức bên gửi và bên nhận). Giả định rằng người nhận biết khóa công khai của người gửi. Chữ ký số có thể được hình thành bằng cách mã hóa toàn bộ tin nhắn bằng khóa riêng của người gửi hoặc bằng cách mã hóa mã băm của tin nhắn bằng khóa riêng của người gửi.
- Một chữ ký kỹ thuật số phân xử hoạt động như sau:
    + Mỗi tin nhắn được ký từ người gửi X đến người nhận Y trước tiên đến một bên thứ 3 là Z, Z có nhiệm vụ kiểm tra nguồn gốc và nội dung của tin nhắn.
    + Tin nhắn sau đó được thêm ngày và gửi đến Y với một dấu hiệu cho thấy nó đã được xác minh bởi bên thứ 3 là Z.

5. In what order should the signature function and the confidentiality function be applied to a message, and why?

Điều quan trọng là phải thực hiện chức năng chữ ký trước và sau đó là chức năng bảo mật.
- Trong chức năng Chữ ký, nó sử dụng khóa riêng của người gửi để ký (mã hóa băm) vào tin nhắn và người nhận sử dụng khóa chung của người gửi để giải mã tin nhắn.

- Trong chức năng Bảo mật, người gửi sử dụng khóa riêng của người nhận để mã hóa tin nhắn và sử dụng khóa chung của người nhận để giải mã tin nhắn.
- Trong trường hợp tranh chấp, một số bên thứ ba phải xem tin nhắn và chữ ký để xác minh. Nếu chữ ký được tính trên tin nhắn được mã hóa, thì bên thứ ba cũng cần truy cập vào khóa giải mã để đọc tin nhắn gốc. Tuy nhiên, nếu chữ ký là hoạt động bên trong, thì người nhận có thể lưu trữ thông điệp văn bản gốc và chữ ký của nó để sử dụng sau này trong giải quyết tranh chấp.

6. What are some threats associated with a direct digital signature scheme?

- Tính hợp lệ của chương trình phụ thuộc vào tính bảo mật khóa riêng của người gửi. Nếu người gửi sau đó muốn từ chối gửi một tin nhắn cụ thể, người gửi có thể cho khóa riêng bị mất hoặc bị đánh cắp và người khác giả mạo chữ ký của họ.
- Một số khóa riêng thực sự có thể bị đánh cắp từ X tại thời điểm T. Đối thủ sau đó có thể gửi tin nhắn được ký bằng chữ ký của X và được xác nhận tại T hoặc thời điểm trước khác.

7. DSA specifies that if the signature generation process results in a value of s = 0, a new value of k should be generated and the signature should be recalculated. Why?

- Người dùng tạo chữ ký có s = 0 vô tình tiết lộ khóa riêng x của mình thông qua mối quan hệ:
s = 0 = k–1[H(m) + xr) mod q

$$x = \frac{-H(m)}{r} \bmod q$$

8. With DSA, because the value of k is generated for each signature, even if the same message is signed twice on different occasions, the signatures will differ. This is not true of RSA signatures. What is the practical implication of this difference?

Người ký phải cẩn thận để tạo ra các giá trị của k theo cách không thể đoán trước, để không bị xâm phạm.