HỌ TÊN: LÊ HUỲNH QUANG VŨ

MSSV: 21522797

BÀI 2: Tấn công vào chứng thực với chuỗi băm

A screenshot of a computer

Description automatically generated

*16 bits, printable*

A screenshot of a computer

Description automatically generated

*16 bits, unprintable*

*A screenshot of a computer

Description automatically generated*

*32 bits, printable*

*A screenshot of a computer

Description automatically generated*

*32 bits, unprintable*

*A screenshot of a computer error message

Description automatically generated*

*64 bits, printable*

*A screenshot of a computer error message

Description automatically generated*

*64 bits, unprintable*

*A screenshot of a computer error message

Description automatically generated*

*128 bits, printable*

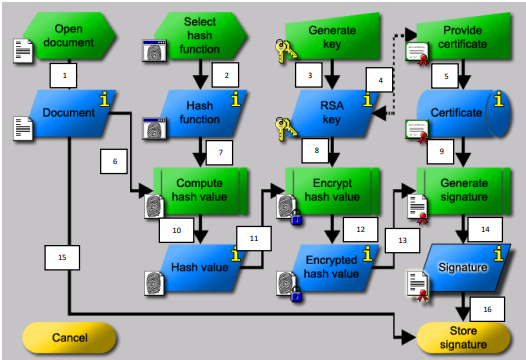
*A screenshot of a computer error message

Description automatically generated*

*128 bits, unprintable*

* Nhận xét:
  + Đối với printable character, số bước nhiều hơn, có chuỗi băm kiểm tra.
  + Đối với unprintable, số bước ít hơn, không có chuỗi băm kiểm tra.
  + Số bits càng nhiều, thời gian tính toán càng dài.

BÀI 3: Chứng thực thông điệp và chữ ký số



1. Mở thông điệp.
2. Chọn hàm băm.
3. Tạo khóa.
4. Cung cấp chứng chỉ cho khóa RSA.
5. Chứng chỉ được cung cấp.
6. Tính toán giá trị băm cho thông điệp theo hàm băm đã chọn.
7. Dùng hàm băm để tính giá trị băm.
8. Dùng khóa RSA mã hóa giá trị băm.
9. Dùng chứng chỉ đã chọn để tạo chữ ký.
10. Giá trị băm đã được tính toán.
11. Đưa giá trị băm vào mã hóa với khóa RSA.
12. Giá trị mã hóa từ giá trị băm đã được tính toán.
13. Đưa giá trị mã hóa vào để tạo chữ ký với chứng chỉ đã chọn.
14. Chữ ký được tạo.
15. Đưa thông điệp chưa mã hóa vào lưu trữ.
16. Đưa chữ ký vào lưu trữ cùng với thông điệp.

BÀI 4: Giao thức bảo mật mạng

|  |  |  |  |
| --- | --- | --- | --- |
| **Tên gọi** | **Tầng hoạt động** | **Đặc điểm** | **Công dụng** |
| Ipsec | - Tầng 3 (OSI): network  - Tầng 2 (TCP/IP): internet | - Gồm: giao thức chứng thực, mã hóa, trao đổi khóa.  - AH  - ESP  - IKE | - Xây dựng mạng riêng ảo (VPN). |
| SSL/TLS | - Tầng 4 (OSI): transport  - Tầng 3 (TCP/IP): transport | 2 thành phần: - Record protocol: được đặt trên đỉnh của các giao thức lớp vận chuyển.  - Gồm các giao thức: handshake, change-cipher-spec, alert. Được đặt giữa các giao thức tầng ứng dụng (như HTTP) và record protocol. | - SSL được sử dụng để bảo vệ những ứng dụng World-Wide-Web và các giao dịch điện tử.  - TLS tương tự. |
| - PGP (pretty good protocol)  - S/MIME (Secure/Multipurpose Internet Mail Extensions) | - Tầng 7 (OSI): application  - Tầng 4 (TCP/IP): application | - Trong hệ thống này mỗi người sẽ có một public key và một private key (khóa riêng tư).  - Dùng public key để mã hóa, private key giải mã. | - PGP có thể được sử dụng để chứng thực một thông điệp, mã hoá thông điệp, hoặc cả chứng thực lẫn mã hoá.  - S/MIME là một chuẩn Internet về định dạng cho email. |
| Kerberos | - Tầng 7 (OSI): application  - Tầng 4 (TCP/IP): application | - Chứng thực 2 chiều.  - Mã hóa khóa đối xứng. | - Dùng để xác thực trong các mạng máy tính hoạt động trên những đường truyền không an toàn.  - Chống lại việc nghe lén hay gửi lại các gói tin cũ và đảm bảo tính toàn vẹn của dữ liệu. |
| SSH | - Tầng 7 (OSI): application  - Tầng 4 (TCP/IP): application | SSH được chia thành 3 lớp trong lớp ứng dụng của mô hình mạng TCP/IP:  – Connection Layer  – User Authentication Layer  – Transport Layer | Có khả năng nén dữ liệu, bảo mật cho dữ liệu truyền (SFTP) và sao chép file (SCP). |