Network Security

Review Questions

Chương 2

1. Các thành phần cơ bản của mã hóa đối xứng (symmetric encryption)?
2. Có bao nhiêu khóa dùng trong mã hóa đối xứng?
3. Sự khác biệt giữa mã hóa khối (block cipher) và mã khóa luồng (stream cipher).
4. CBC mode là gì?
5. Triple Encryption là gì?
6. Liệt kê những cách phân phối khóa bí mật (secret key).
7. Sự khác biệt giữa khóa chính (master key) và khóa giao dịch (session key).
8. Trung tâm phân phối khóa (KDC) là gì?

Chương 3

1. Liệt kê 3 cách thức để chứng thực thông điệp (message authentication)
2. Mã chứng thực thông điệp (message authentication code) là gì?
3. Liệt kê các thuộc tính có ích của một hàm băm đối với chứng thực thông điệp
4. Các thành phần của mã hóa công khai (public key cryptosystem)?
5. Liệt kê 3 cách dùng của mã hóa công khai.
6. Sự khác biệt giữa khóa riêng (private key) và khóa bí mật (secret key)?
7. Chữ kí điện tử (digital signature) là gì?
8. Chứng chỉ khóa công khai (public-key certificate) là gì?
9. Làm thế nào để dùng mã hóa công khai để phân phối khóa bí mật?

Chương 4

1. Kerberos được thiết kế để giải quyết những vấn đề gì?
2. Liệt kê 3 nguy cơ khi xác thực người dùng thông qua mạng hay Internet.
3. Trình bày mô hình xác thực đơn giản (simple authentication dialogue).
4. Chuẩn X.509 là gì?
5. Định dạng của chứng chỉ X.509.

Chương 5

1. Liệt kê 5 dịch vụ được cung cấp bởi PGP.
2. Mô hình bảo mật và xác thực của PGP.
3. Tại sao PGP tạo chữ kí trước khi nén dữ liệu?
4. Radix-64 là gì?
5. Định dạng của thông điệp PGP.
6. 4 chức năng của S/MIME.

Chương 7

1. SSL gồm những giao thức gì?
2. Hoạt động của giao thức mẫu tin SSL (SSL Record Protocol)
3. Giao thức TLS là gì?
4. Các dịch vụ của SET.
5. Các đặc tính của SET.