Chapter 05: Chữ ký số.

Chữ ký số là một công cụ xác thực để người tạo ra message đính kèm 1 code mà nó hoạt động như 1 chữ ký ngoài đời thật.

Thông thường chữ ký được tạo bằng cách hash of the message and encrypting the message with the creator’s private key.

Chữ ký số đảm bảo nguồn và toàn vẹn của tin nhắn, sử dụng secure hash algorithm(SHA).

Attacks and Forgeries(tấn công và giả mạo chữ ký):

Attacks:key-only attack, known message attack,generic(chung) chosen message attack, directed(hướng) chosen message attack, adaptive(thích nghi) chosen message .attack

Break success levels: total break,selective forgery(giả mạo chọn lựa), existential forgery(giả mạo hiện hữu).

Digital Signature **Requirements**:

phải phụ thuộc vào thông điệp ký.

phải sử dụng thông tin duy nhất cảu người gửi.

• để ngăn chặn cả hai giả mạo và phủ nhận.

phải tương đối dễ dàng để sản xuất

phải tương đối dễ dàng để nhận ra và xác minh

được tính toán để không thể giả mạo(computationally infeasible to forge):

• với message mới trong trường hợp tồn tại chữ ký số.

• với chữ ký số giả mạo cho thông điệp được đưa.

be practical save digital signature in storage.

**Direct** Digital Signatures:

chỉ liên quan đến người gửi và người nhận.

giả định người nhận có khóa công khai của người gửi.

chữ ký số được thực hiện bởi người gửi ký toàn bộ tin nhắn hoặc băm với private key.

có thể mã hóa bằng cách sử dụng khóa công khai người nhận.

quan trọng là dấu hiệu đầu tiên sau đó mã hóa tin nhắn & chữ ký.

security phụ thuộc vào private-key của người gửi.

**Digital Signature Algorithm** (DSA):

tạo ra một chữ ký 320 bit

với 512-1024 bit an ninh

nhỏ hơn và nhanh hơn so với RSA

a digital signature scheme only

an ninh phụ thuộc vào độ khó của máy tính logarit rời rạc

biến thể của ElGamal & Schnorr án