Lecture 13

Secure Programming

Reference:

Security in Computing, Charles P. Pfleeger, Shari Lawrence, Jonathan Margulies

1

Security Goals

- Security Goals (CIA Triad)
  - Confidentiality, Integrity, and Availability
- Confidentiality
  - Assets accessed by authorized parties
  - Read type access
    - Read, view, print, or just know existence of object
- Integrity
  - Assets modified by authorized parties or in authorized ways
  - Modification - write, change, delete, or create
- Availability
  - Assets available when users want to access

2

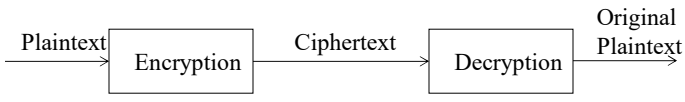
Confidentiality

- Cryptosystem
- Symmetric Cryptosystem
  - DES, AES
- Asymmetric Cryptosystem
  - Diffie Hellman, RSA

3

Cryptosystem

- Encryption
  - Message encoded to not obvious message
  - Encrypt, encipher, encode
- Decryption
  - Encrypted message transformed into normal form
  - Decrypt, decipher, decode



4

Cryptosystem

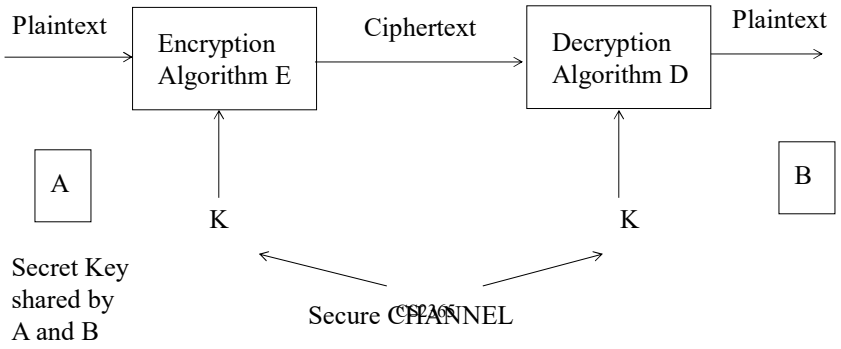
- Cryptosystem
  - System for encryption and decryption
  - Plaintext P = (p1, p2, …., pn): original form of a message
  - Ciphertext C = (c1, c2, …., Cm): encrypted form
  - Transformation between P and C
    - C=E(P) and P = D(C)
  - Cryptosystem: P = D(E(P))

Stream and Block Ciphers

- Stream Cipher
  - Convert one symbol of plaintext to a symbol of ciphertext
  - Advantages
    - Speed of transformation
- Block Cipher
  - Encrypts a group of plaintext symbols as one block
  - Advantages
    - High diffusion

Symmetric Cryptosystem

- Secret Key Cryptosystem (Single Key)
  - Encryption and decryption keys are the same
  - P = D(K, C) where C = E(K, P)
  - P = D(K, E(K, P))



Symmetric Cryptosystem

- Confidentiality depends only on secrecy of the key
- Attacker is assumed to know E and D
- Secret key systems do not scale well
  - With N parties we need to generate and distribute N*(N-1)/2 keys
- A and B can be people and computers

Data Encryption Standard (DES)

- Developed for the U.S. government
  - Accepted as a cryptographic standard in US and abroad (1976)
- DES
  - 56 bits long key; 64-bit block size; E and D are public
  - Has not been broken since 1977, but not secure anymore
  - Different 4 modes
    - Electronic Code Book, Ciphertext Block Chaining, Cipher FeedBack, Output Feedback modes

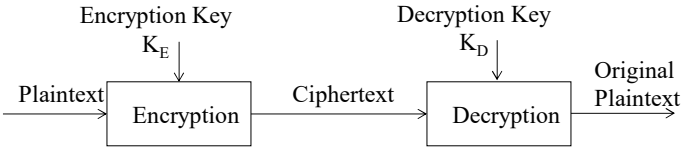
Advanced Encryption Standard (AES)

- NIST selected AES of the Rijndael family in 2001
- Symmetric key cryptography as a block cipher
  - Block sizes of 128 bits
  - Key sizes of 128, 192, and 256 bits

- Program – AESTest.java

Asymmetric Cryptosystem

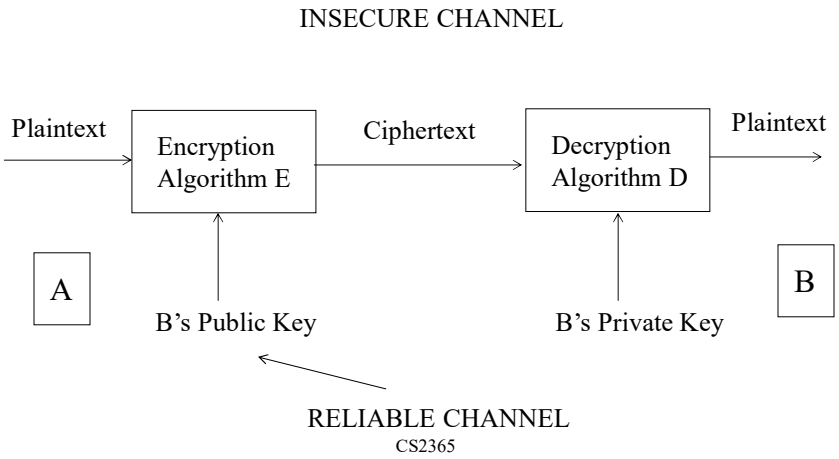
- Asymmetric Encryption (Two Keys)
  - A pair of keys for encryption and decryption
  - $P = D(K_D, E(K_E, P))$



Public Key (Asymmetric) Encryption

- Diffie and Hellman [1976]
  - Proposed a public key encryption system
  - Motivation – n*(n-1)/2 for secret keys among n-users
  - Each user has two keys – a public key and a private key
  - $P = D(K_{PRIV}, E(K_{PUB}, P))$
    - Alice encrypts messages with Bob's public key
    - Bob encrypts a message with a private key

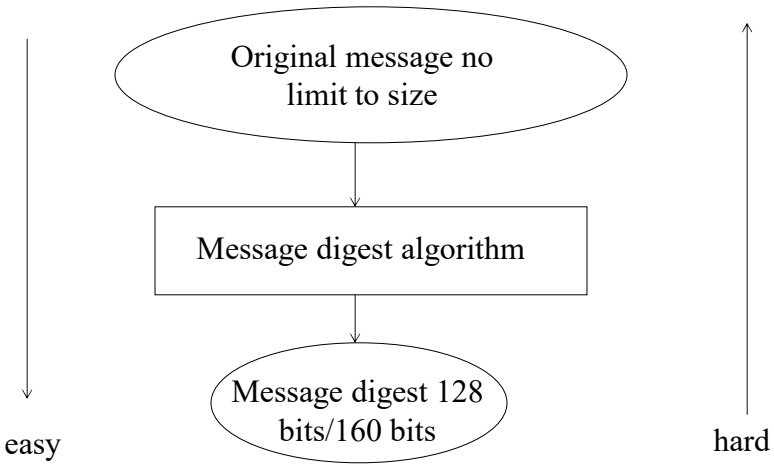
Public Key Encryption



Integrity

- Protect against unauthorized changes to data
- Message digest (MD) or Message Authentication Code (MAC)
- MD with secret-key technology
- MD with pubic-key technology

Message Digest



Message Digest

- One-way function
  - m = H(M) is easy to compute
  - M = H^{-1}(m) is hard to compute

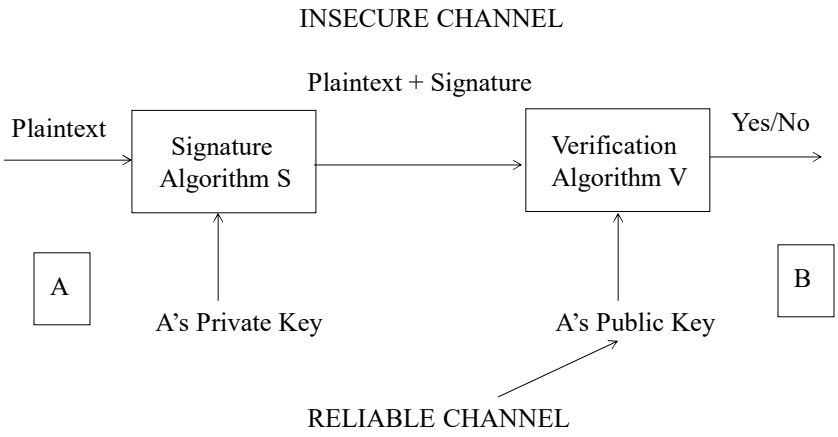
Message Digest

- MD5
  - Proposed by Ron Rivest
  - Improved version of MD4
  - 128 bits digest
- NIST SHA/SHS (Secure Hash Algorithm or Standard)
  - 160 bits digest
  - Similar to MD5
  - SHA-0, SHA-1, SHA-2, SHA-3
- Program – Secure Hash Algorithm (SHA-1)

Digital Signature

- Non-repudiation
  - Protect against one party to a transaction or communication activity
  - later falsely denying that the transaction or activity occurred
- Digital signature
  - A mark that only the sender can make
  - But other people recognize

Digital Signature



19

Digital Signature

- Person P signs message M, generates signature S(P, M), and sends [M, S(P, M)] to R
- Two primary properties
  - It must be unforgeable
  - It must be authentic
- Program: DSATest.java

20