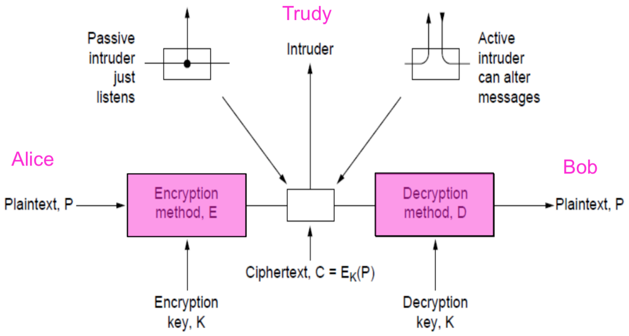
Week 10: Security

Cryptography

Basic Components

- Plaintext: P
- Encryption method: E
- Encryption key: K
- Cipher-text: C
- Decryption method: D
- Decryption key: K



- Passive intruder: just listen massage
- Active intruder: alter message
- We require that $D_{K_2}(E_{K_1}(P)) = P$ if and only if $K_1 = K_2$

Kerckhoff's Principle

Cryptographic algorithms and related functions (E, D) are public, keys (K) are private

Key

- Key is a short string and can be change often
- The size of key space is determined by the number of bits in key string
- The longer key, the more effort needed to break a encryption

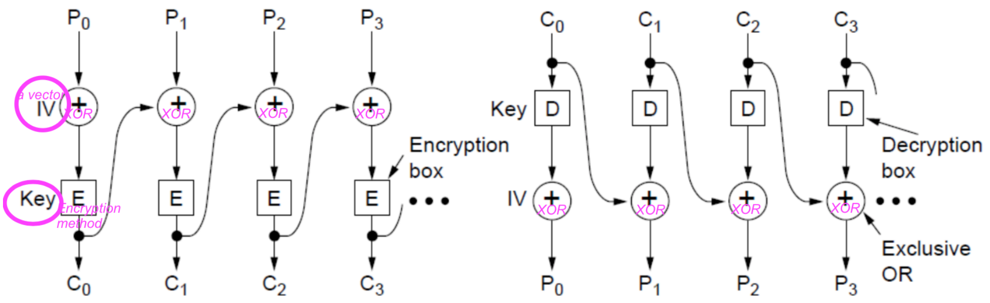
Cipher

- **Substitution cipher**: each letter is replaced by other letters
- **Transposition cipher**: re-order all letters
- **One-time pad**: convert the plaintext into bit-string, choose a random same-length bit-string as key, then XOR them bit by bit
- **Block cipher**: treat fixed length string, the fixed length is called block size. The operated string has same length as before.

Symmetric Key Algorithm

- Use **a same key** for encryption and decryption (better to change the key often)
- Can use permutation, substitution or both of them to encrypt and decrypt
- 2 Example
  - **DES** (Data Encryption Standard)
    - 64-bit block size
    - 56-bit key
    - 2^{56} key space
  - **AES** (Advanced Encryption Standard)
    - 128-bit block size
    - 128-bit key
    - 2^{128} key space

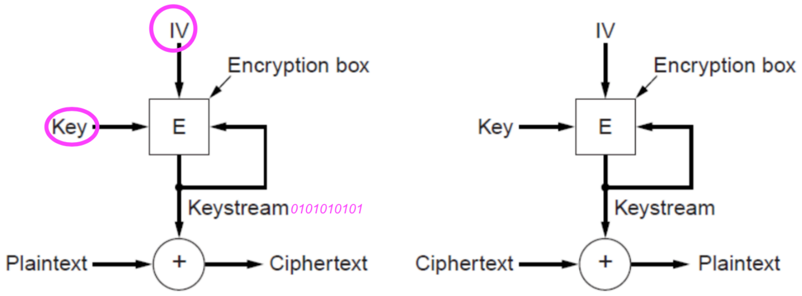
Block Chain Mode



CBC mode encryption CBC mode decryption

Stream Cipher Mode

- Key may be overleaped!



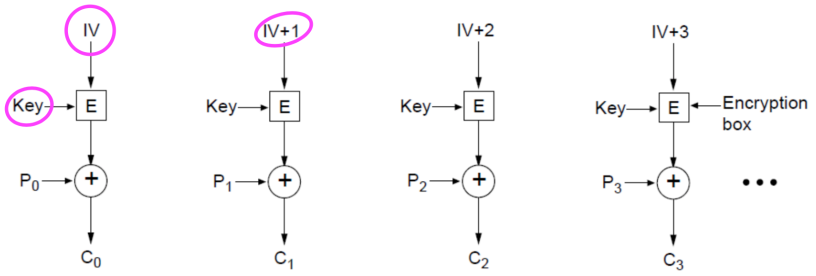
Encryption Decryption

XOR NOTE:

If A XOR B = C,
then A XOR C = B and
B XOR C = A

If P1 XOR K = C1 and
P2 XOR K = C2,
then C1 XOR C2 = P1 XOR P2

Counter Mode



Encryption above; repeat the operation to decrypt

Asymmetric Key Algorithm

- There are **2 different key** to be used in encrypting and decrypting, one is public, one is private

Diffe-Hellman'S 2 Key System

- a owner has 2 keys
  - **public key**: someone want to send message to the owner use public key to encrypt plaintext
  - **private key**: the owner use private key to decrypt received ciphertext

RSA Algorithm

- Very robust, but require 1024-bit-length key
- The security of RSA is based on large computation complexity, but it is slow to encrypt/decrypt large volume of data
- **$C=P^e$ mod n** (public key is e and n)
- **$P=C^d$ mod n** (private key is d and n)

Digital Signature

- Cryptography methods that can be used to ensure authenticity and non-repudiation
- 3 requirements:
  - receiver can verify identity of sender
  - sender cannot reputation the message
  - receiver cannot generate the message by themselves
- 3 approachs:
  - use symmetric key via a intermediary
  - use public key as individual
  - use message digest
    - use a one-way hash function to transfer an arbitrary-length plaintext to s fixed-length bit-string

Message Digest

Message Digest (MD) is a one-way hash function to transfer an arbitrary-length plaintext to a **fixed-length bit-string**. MD transformation is fast.

- given plaintext, MD should quickly compute its output
- given output, there should be no way to derive plaintext
- the output of P can only be derive by P
- if we change plaintext a little, the output should be very different

Public Key Management

- Certification authority (CA) acts as a middleman
- X.509
- PKI (Public Key Infrastructure) establish/store/revoke public key

Netowrk Secury

- 4 relates concepts
  - **Secrecy**: hidden information from unauthorized users 不让看的人不能看
  - **Authentication**: ensure the user your are talking with has access to some resource 让看的人能看
  - **Non-repudiation**: prove a information sent by a user is valid 证明信息真的是某个人发出的
  - **Integrity control**: ensure the information is not be changed in transit 信息不被篡改

Authentication Protocol

Protocol used to **secure authentications.**

- 原则: minimize the use of private ket in the establish of secure connection
- 4 approachs:
  - **shared keys**
  - **key distribution** (third-party)
  - **kerberos**
  - **public key**

IPSec

A **network level protocol** that ensure secure transit of packet

- IPSec is connection-oriented protocol, the connections is like a secure encrypted tunnel, and be called **SA** (security association)

Implementation

- IPSec 2 components:
  - New headers being added to normal IP packets
  - ISAKMP key management
- IPSec 2 modes:
  - **Transport mode**: only add security header to normal IP packet, no encryption
  - **Tunnel mode**: set up a tunnel and encryption the whole IP packet

VPN (Virtual Private Network)

VPN is a virtual layer on top of IP network

- VPN provides a **secure end-to-end tunnel** over public infrastructure.
- Traffic in the tunnel will selectively and securely transited using **IPSec**

Firewall

- Firewall is used in each endpoint to **set up security tunnel** and ensure security at the network boundary
- 3 characteristics:
  - all ingoing and outgoing traffic must transit the firewall
  - only authorized traffic can pass through the firewall
  - firewall should be immune to penetration itself
- Constraints:
  - no protection if intruders can bypass the firewall
  - no protection against internal attacks
  - no protection against application payload attacks

Wireless Security

Wireless network is harder to secure because of omnidirectional signal propagation. Many wireless networks working in an insecure way

- 802.11 has a security protocol **WEP** (Wired Equivalency Protocol), which is a 40-bit-key encryption based on RC4 algorithm
- But WEP is not very reliable because 40-bit key is too short and RC4 method reuse keys

MAC Address Filtering

Let the wifi router block some unwanted devices' MAC address

Non-Broadcast SSID

SSID (service set identifier) is the network name of your wifi. If wifi is set to non-broadcast its SSID, only the devices pre-known the SSID can connect to the wifi.

Additional Encryption (128-bit WEP)

Use longer key in WEP

WPA2 (Wifi Protected Access 2)

Multilayered Security

Use more than one method in more than one layer to ensure security.