MAS 433: Cryptography

Lecture 5

Block Cipher (Part 1, Introduction)

Wu Hongjun

Lecture Outline

- Classical ciphers
- Symmetric key encryption
  - One-time pad & information theory
  - **Block cipher**
    - DES, Double DES, Triple DES
    - AES
    - Mode of Operations
    - Attacks
  - Stream cipher
- Hash function and Message Authentication Code
- Public key encryption
- Digital signature
- Key establishment and management
- Introduction to other cryptographic topics

Lecture Outline (contd.)

- Information theoretical security & computational security
- Practical symmetric key ciphers
- Introduction to block cipher

Recommended Reading

- CTP Section 3.1, 3.2
- HAC Section 7.1, 7.2.1

- Wikipedia:
  - Block cipher
    http://en.wikipedia.org/wiki/Block_cipher

Information-Theoretical Security vs Computational Security

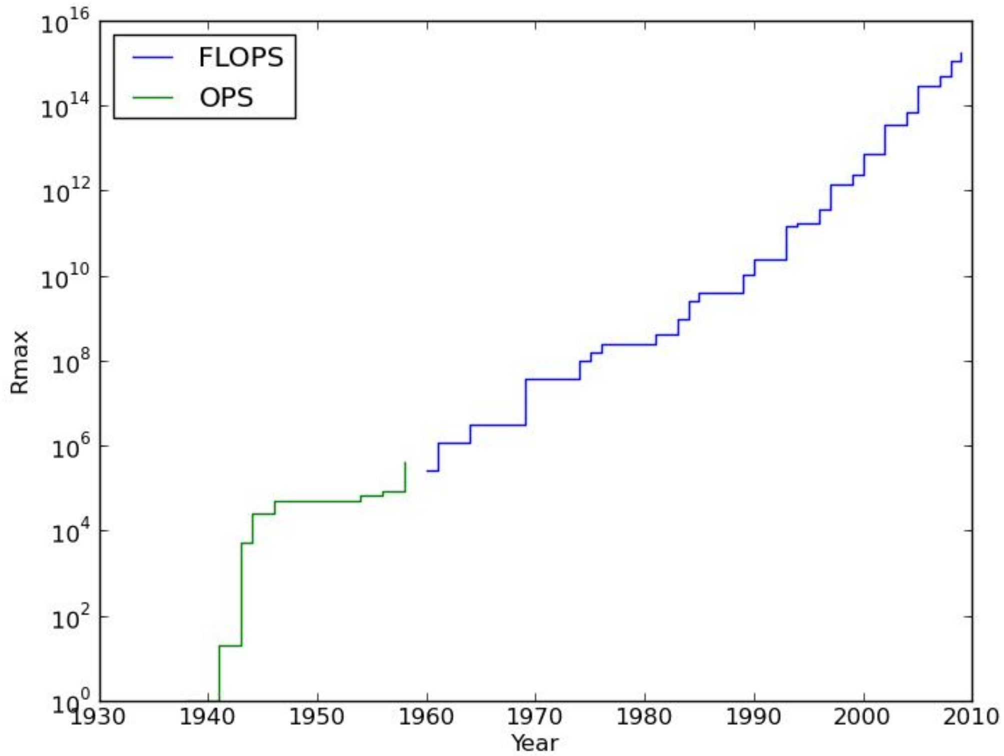
- Information-theoretically secure
  - Also called “unconditionally secure”
  - A cryptosystem is information-theoretically secure if it is secure even when the attacker has **unlimited computing power**
  - One case we have studied
    - One-time pad: perfect secrecy
      - But the one-time key’s length is as long as the message
      - Inconvenient to use for many applications
- Computationally secure
  - A cryptosystem is computationally secure if it cannot be broken with **the current computing technology** within **a given period of time**.

Computing power today

- Intel Core-i5 CPU
  - A widely used CPU in 2010 (notebook, desktop computers)
  - Each costs less than S$400
  - Each has two cores, runs at the speed about 2.5GHz
  - Perform about 2^{32} 64-bit integer additions (or XORs)
- The most powerful supercomputer in the world in 2010
  - Jaguar (Oak Ridge National Laboratory)
  - 224,162 Opteron CPUs
  - Perform 1.76 Pflops (about 2^{51} FLoating Point Operatios Per Second)
- The combined computing power of top 500 supercomputers in 2010
  - Perform 32.4 Pflops (about 2^{55} FLoating Point Operations Per Second) (about 2^{80} operations per year)
- Computer is getting faster and faster (for the same price)
  - 128-bit key is needed today

The Fastest Computers in History

http://en.wikipedia.org/wiki/Supercomputer



1938;: 1 OPS Konrad Zuse, Germany

1943: 5 KOPS Post Office Research Station, Bletchley Park, UK

1961; 1.2 MFLOPS; Los Alamos National Laboratory, USA

1984; 2.4 GFLOPS ; Scientific Research Institute of Computer Complexes, USSR

1997; 1.338 TFLOPS; Sandia National Laboratories, USA

2008; 1.026 PFLOPS; Los Alamos National Laboratory, USA

Ciphertext-only attack & known-plaintext attack

- Ciphertext-only attack
  - The attacker does know the message
  - But the attacker knows the statistical information of the message (such as the distribution of letters, digrams, trigrams …)
- Known-plaintext attack
  - The attacker
    - knows part of the plaintext
    - tries to recover the key and to decrypt other messages being encrypted using that key
  - Known-plaintext attack is practical in many applications
    - Example: NTU webmail (protected using SSL), a lot of contents are identical to all the users (such as the NTU logo, webpage frame, email protocol)

Kerckhoffs' principle

- Kerckhoffs' principle
  - The attacker knows the specifications of the cipher except the secret key
  - A strong cipher should remain secure in the above scenario
- Do we need to publish every cipher following Kerckhoff's principle?
  - Making a cipher public makes sense only if we assume that all the attackers are cooperative (i.e., they will publish their attacks)

Practical Symmetric Key Ciphers

- Practical ciphers are required to be at least
  - Computationally secure
    - Strong even when the attacker knows the cipher specifications (Kerchoffs' principle)
    - Strong against known-plaintext attack
  - Convenient to use
    - A relatively short key (for example: a 128-bit key) can be used to encrypt many messages without compromising security
- Two types of practical symmetric key ciphers
  - Block cipher
  - Stream cipher

Block Cipher

- Substitution cipher
  - The size of the substitution table is small
    - 26 elements (for English)
  - Extremely weak against
    - ciphertext-only attack & known-plaintext attack
  - What will happen if we increase the size of the secret substitution table to 2^{128} elements?
    - The resulting cipher is strong!
      - What is the complexity of known-plaintext attack?
    - But the key (substitution table) size is too large to store

International Data Corporation (IDC) estimates that the amount of data generated in 2009 was 1.2 million Petabytes ($\approx\approx 2^{70}$ bytes $\approx 10^{21}$ bytes)

The internet size is estimated to be 5 million Terabytes($\approx\approx 2^{62}$ bytes) of data. Google indexed roughly 200 terabytes ($\approx\approx 2^{48}$ bytes) of that, or 0.004% of the total size (Eric Schmidt, CEO of Google, 2005).

Block Cipher

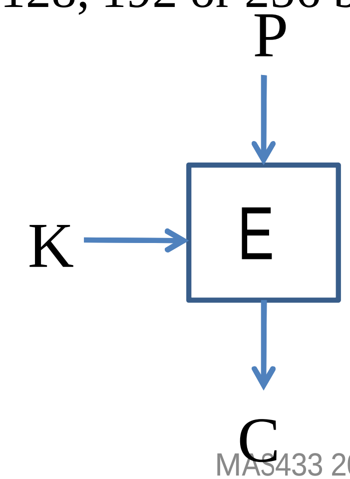
- Block cipher
  - Maybe viewed as a huge “substitution cipher”
    - DES: a “substitution table with 2^{64} elements”
    - AES: a “substitution table with 2^{128} elements”
  - But each element in the huge “table” is computed only when it is needed
    - So there is no need to store the huge table
    - How to compute each element?
      - Equivalent to: how to encrypt a message block?
        how to design a block cipher?

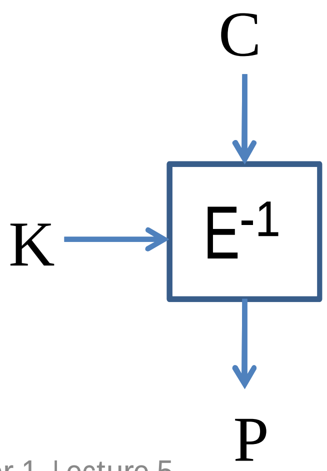
Block Cipher: overall

- an *n*-bit plaintext block is encrypted to an *n*-bit ciphertext block
  - Block size: *n* bits
    - DES: 64 bits
    - AES: 128 bits
  - Key size
    - DES: 56 bits, (insecure today)
    - 3-DES: 112 or 168 bits
    - AES: 128, 192 or 256 bits

Encryption:

$$C = E_K(P)$$





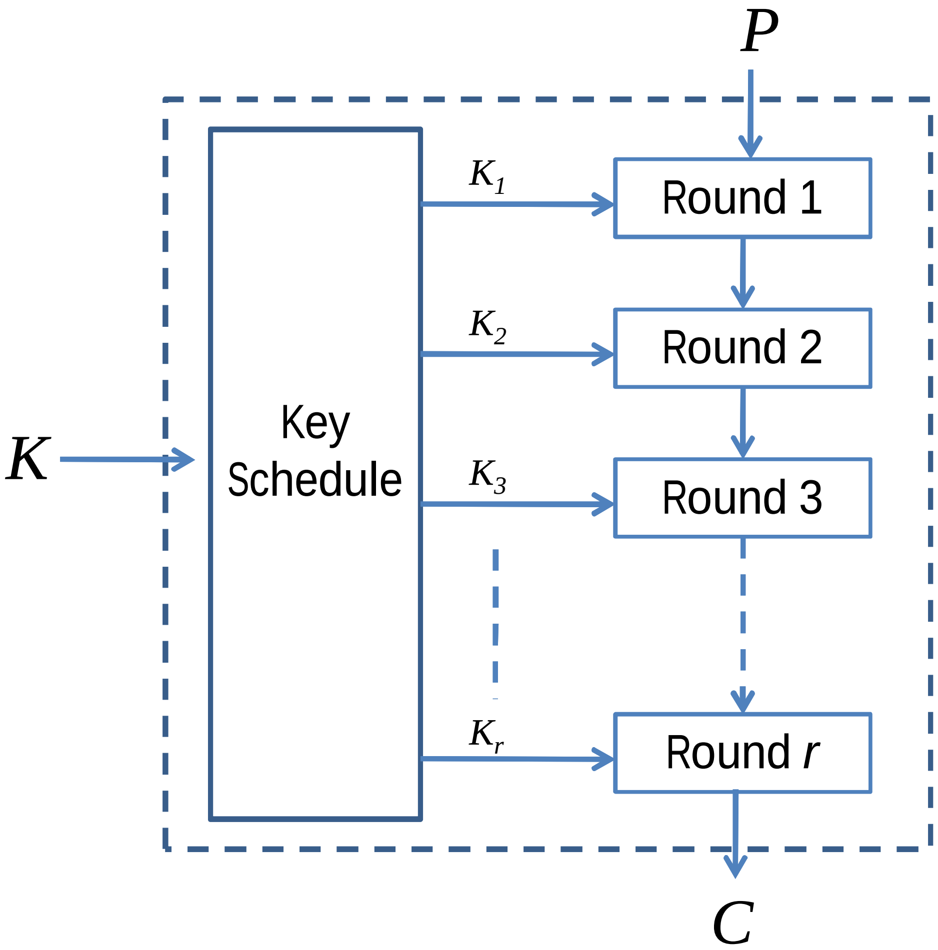
Decryption:

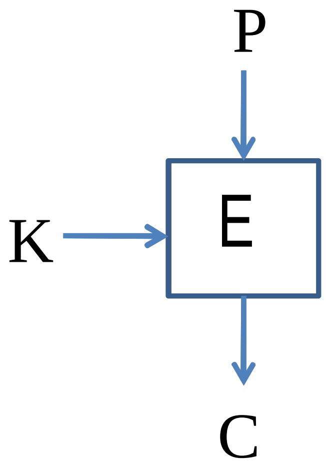
$$P = E_K^{-1}(C)$$

Block Cipher: Iterated Structure

- To simplify the design, security evaluation and implementation, a round function is used repeatedly in a block cipher
  - A typical block cipher consists of
    - r rounds (one ***round function*** for each round)
      - a ***round key*** is used for each round
    - ***key schedule***
      - round keys are generated from the secret key

Block Cipher: Iterated Structure (contd.)





Block Cipher: Round Function

- How to design the round function?
  - Design strategy
    - **Confusion** (non-linear)
      - Combine bits in a nonlinear way
        - » Small substitution table
        - » Multiplication together with XOR
        - » addition together with XOR
        - » ….
    - **Diffusion**
      - Let all the bits affect each other
        - » Permutation
        - » Shift, Rotation
        - » ….

Block Cipher: Round Function (contd.)

- Two main approaches to design round function
  - Substitution-permutation network (SPN)
    - AES …
  - Feistel network
    - DES …

  - To be learned soon …

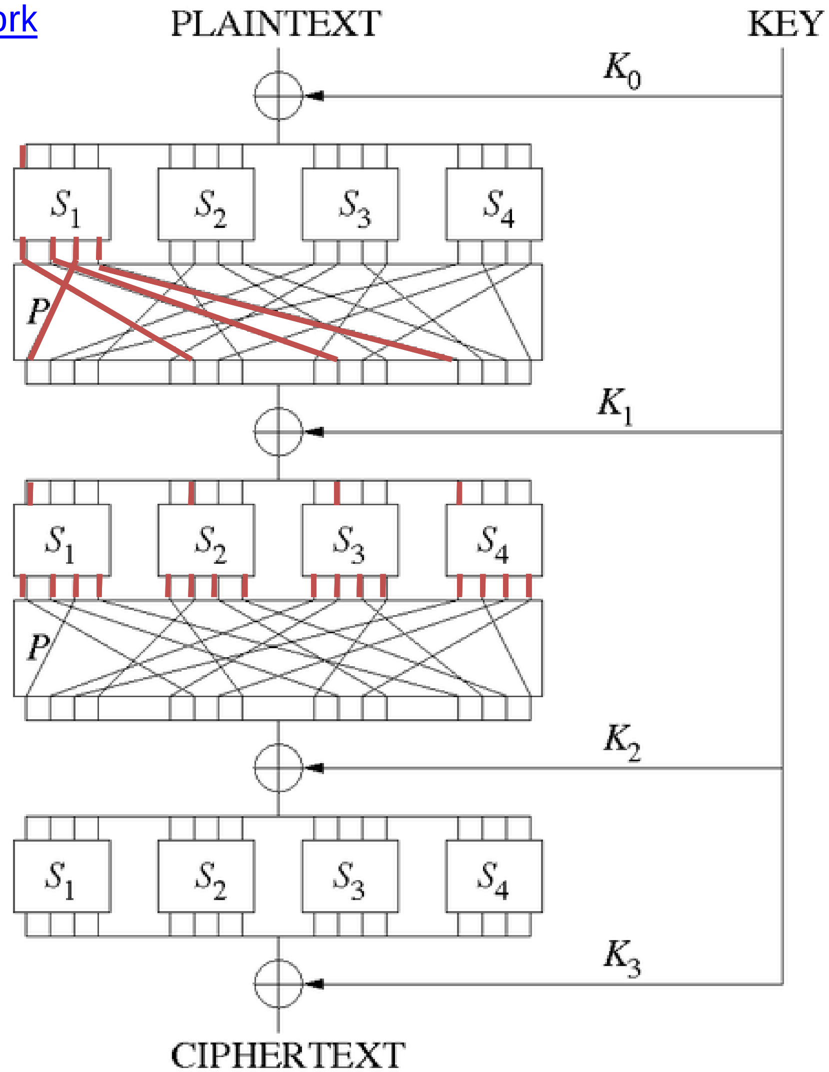
Block Cipher: Key Schedule

- How to design key schedule
  - Many different approaches
  - No perfect guideline so far
  - Basic rule:
    - Each bit of the key should affect a number of round keys at **different** locations (different locations: some round keys near the beginning, some round keys in the middle, some round key near the end)

Example: A Simple Block Cipher

http://en.wikipedia.org/wiki/Substitution-permutation_network

- **Substitution-Permutation network**
  - Confusion: substitution
    - Substitution table: secret or public
  - Diffusion: permutation
    - Permutation: normally public
- Example: A toy cipher
  - Block size: 16 bits
  - 3 rounds
  - Substitution
    - four Sboxes
    - Each Sbox: 4×4-bit
  - Permutation
    - Bit-wise permutation
    - 16 positions being permutated
    - Carefully chosen to ensure quick diffusion
      - Each plaintext bit affects all the 16 bits in the state after 2 rounds.



How to design the substitution table?

Summary

- Information-theoretical security & computational security
- Practical symmetric key ciphers
  - Computational security
  - Kerckhoffs' principle
  - Known-plaintext attack & …
- Block Cipher
  - Iterated structure
    - Round function & round key
    - Key schedule
  - Round function
    - Design strategy: Confusion & diffusion
    - Methods:
      - Substitution-permutation network
      - Feistel network