
 THE UNIVERSITY OF BRITISH COLUMBIA


Symmetric Crypto Systems

 EECE 412
 Session 4

Copyright © 2004 Konstantin Beznosov

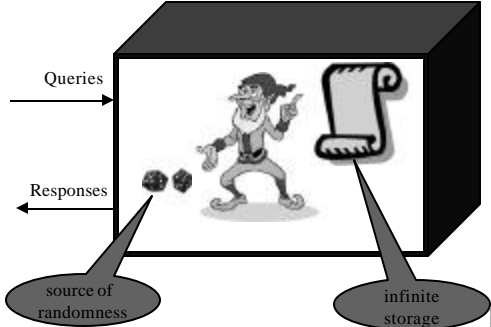
Last Session Recap

- Historical background
 - Caesar and Vigenère ciphers
 - One-time pad
- The Random Oracle model
 - Random functions: hash functions
 - Random generators: stream ciphers
 - Random Permutations: block ciphers



UBC Logo

What is Random Oracle Model?




UBC Logo

Session Outline

- Substitution and transposition ciphers
- Block ciphers “under the hood”
- Modes of operation for block ciphers

UBC Logo


 THE UNIVERSITY OF BRITISH COLUMBIA

Substitution and transposition ciphers

Copyright © 2004 Konstantin Beznosov

Substitution Ciphers

Change characters in plaintext to produce ciphertext

Example: Vigenère Cipher

```

Plain  TO BE OR NOT TO BE TH AT IS THE QUESTION
Key    RE LA TI ONS RE LA TI ON SR ELA TI ONSREL
Cipher KS ME HZ BBL  KS ME MPOG AJ  XSE J CSFLZSY
    
```

UBC Logo

Transposition Cipher

Rearrange letters in plaintext to produce ciphertext

- Example (Rail-Fence Cipher)
 - Plaintext: HELLO WORLD
 - Rearrange as

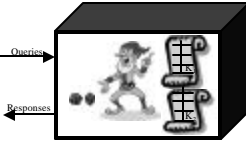
HLOOL
 ELWRD
 - Ciphertext: HLOOLELWRD
- a.k.a. permutation ciphers



Block Ciphers “Under the Hood”

Random Permutation (Block Cipher) as Random Oracle

- In
 - fixed size short string (plaintext) M
 - DES - 64 bits
 - Key K
- Out
 - same fixed size short string (ciphertext) C



Notation

- $C = \{ M \}_K$
- $M = \{ C \}_K$



Related Notes

- Main properties of block ciphers
 - invertible
 - confusing
 - Diffusing
- Main block ciphers
 - Data Encryption Standard (DES)
 - Advanced Encryption Standard (AES) a.k.a., Rijndael



SP-network

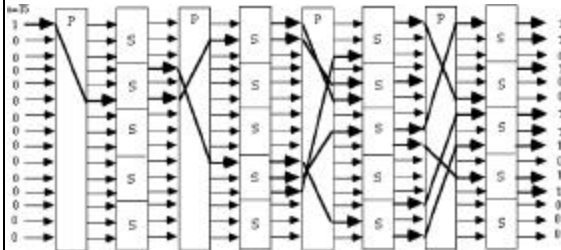


Fig 2.3 - Substitution-Permutation Network, with the Avalanche Characteristic

From Lecture notes on "Cryptography and Computer Security" by Lawrie Brown



S-Boxes

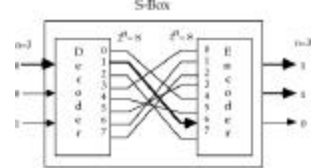


Fig 2.1 Substitution Operation

Main techniques for breaking S-boxes

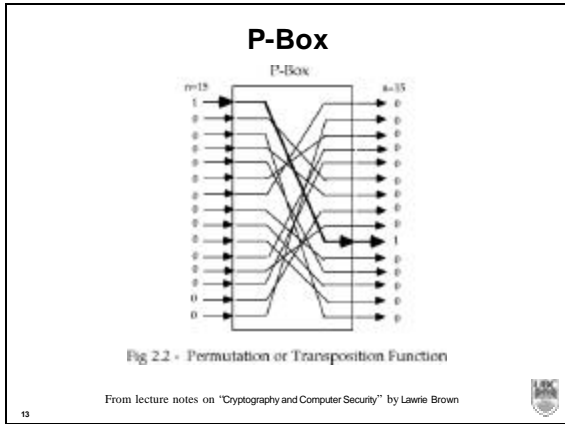
- Linear cryptanalysis
- Differential cryptanalysis

Required properties of S-boxes

- each output bit will depend on every input bit
- changing one input bit will change about half of the output bits

From Lecture notes on "Cryptography and Computer Security" by Lawrie Brown

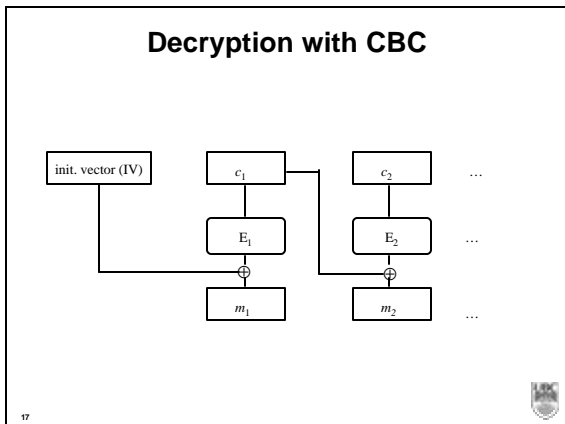
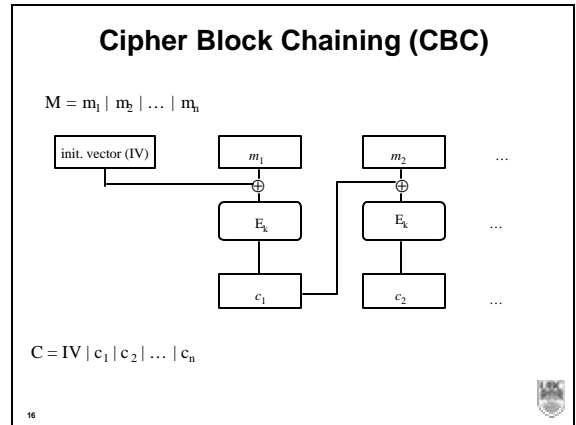
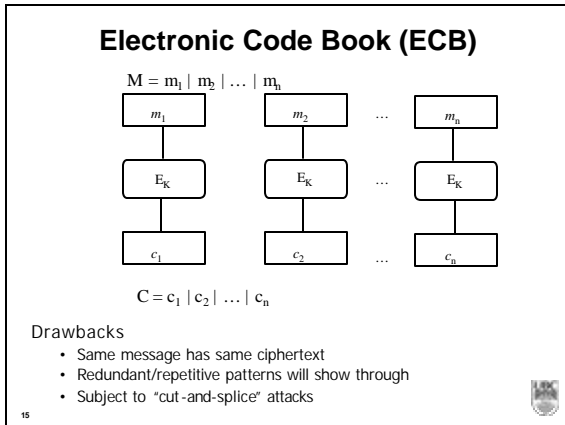




THE UNIVERSITY OF BRITISH COLUMBIA

Modes of Operation

Copyright © 2004 Konstantin Beznosov

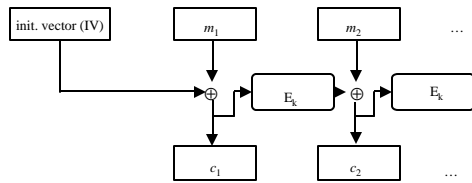


Output Feedback (OFB)

- $K_1 = \{IV\}_K, K_2 = \{K_1\}_K, \dots, K_i = \{K_{i-1}\}_K \dots$
- Purpose: use block cipher as a stream cipher
- $C_i = \{m_i\}_{K_i}, \text{ e.g., } c_i = m_i \oplus K_i$

Cipher Feedback (CFB) Mode

$M = m_1 | m_2 | \dots | m_n$



$C = IV | c_1 | c_2 | \dots | c_n$

19

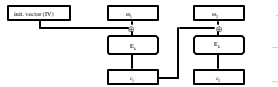
Counter Encryption

- Drawbacks of feedback modes
 - Hard to parallelize
 - CBC -- cannot precompute
 - OFB -- memory requirements
- $K_i = \{IV + i\}_K$

20

Message Authentication Code (MAC)

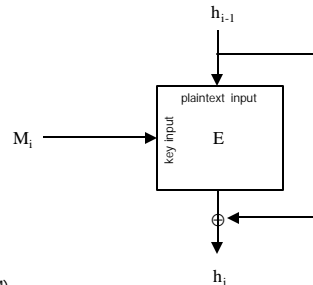
- Purpose
 - protect message integrity and authenticity
- How to do MAC with a block cipher?



- How to do MAC and encryption of a message?

21

Hash Function from a Block Cipher



$h = H(M)$

1. Easy to compute h from M
2. Hard to compute M from h
3. Hard to find another M' s.t. $H(M) == H(M')$

22

Common Hash Functions and Applications

- Common hash functions
 - (Message Digest) MD5 value 128b
 - (Secure Hash Algorithm) SHA -1 160b value
- Applications
 - MACs
 - $MAC_K(M) = H(K, M)$
 - $HMAC_K(M) = H(K \oplus A, H(K \oplus B, M))$
 - Time stamping service
 - key updating
 - $K_i = H(K_{i-1})$
 - Backward security
 - Autokeying
 - $K_{i+1} = H(K_i, M_1, M_2, \dots)$
 - Forward security

23

Key Points

- Ciphers are either substitution, transposition (a.k.a., permutation), or product
- Any block cipher should confuse and defuse
- Block ciphers are implemented in SP-networks
- Stream ciphers and hash functions are commonly implemented with block ciphers
- Hash functions used for fingerprinting data, MAC, key updating, autokeying,

24