
 THE UNIVERSITY OF BRITISH COLUMBIA

Symmetric Crypto Systems


 EECE 412

Copyright © 2004-2005 Konstantin Beznosov 2/6/07

Module Outline

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

UBC Logo

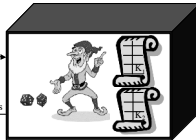

 THE UNIVERSITY OF BRITISH COLUMBIA

Block Ciphers “Under the Hood”

Copyright © 2004-2005 Konstantin Beznosov 2/6/07

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

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

UBC Logo

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

UBC Logo


Advanced Encryption Standard


- Replacement for DES
- AES competition (late 90’s)
 - NSA openly involved
 - Transparent process
 - Many strong algorithms proposed
 - Rijndael Algorithm ultimately selected
 - Pronounced like “Rain Doll” or “Rhine Doll”
- Iterated block cipher (like DES)

UBC Logo

AES Decryption

- To decrypt, process must be invertible
- Inverse of MixAddRoundKey is easy, since \oplus is its own inverse
- MixColumn is invertible (inverse is also implemented as a lookup table)
- Inverse of ShiftRow is easy (cyclic shift the other direction)
- ByteSub is invertible (inverse is also implemented as a lookup table)



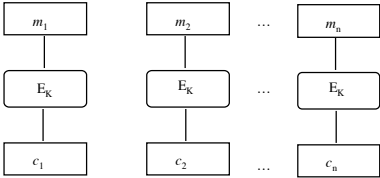
 THE UNIVERSITY OF BRITISH COLUMBIA

Modes of Operation

Copyright © 2004-2005 Konstantin Beznosov 2/6/07

Electronic Code Book (ECB)


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




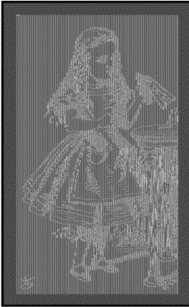
$C = c_1 | c_2 | \dots | c_n$


Drawbacks

- Same message has same ciphertext
- Redundant/repetitive patterns will show through
- Subject to "cut-and-splice" attacks



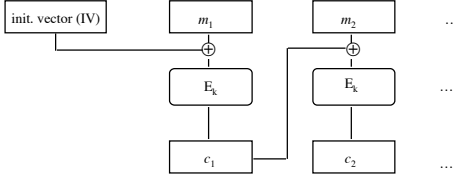
Alice in ECB Mode




Cipher Block Chaining (CBC)


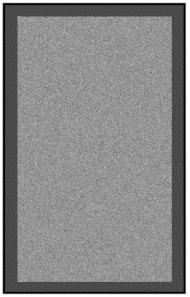
$M = m_1 | m_2 | \dots | m_n$




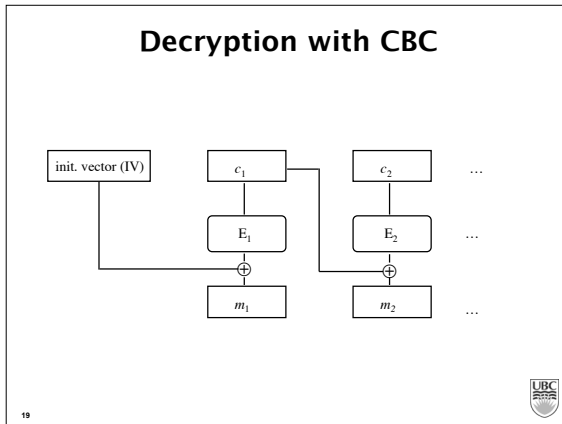
$C = IV | c_1 | c_2 | \dots | c_n$



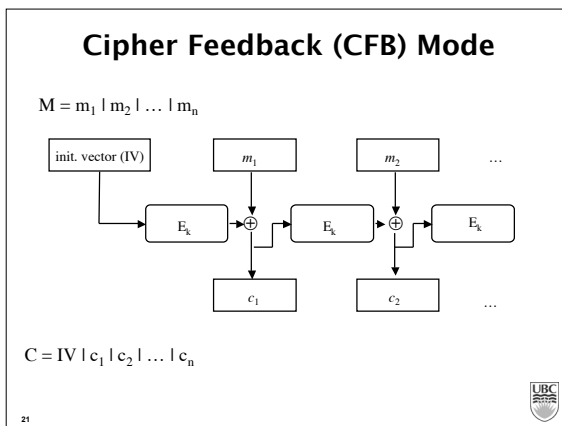
Alice in CBC Mode



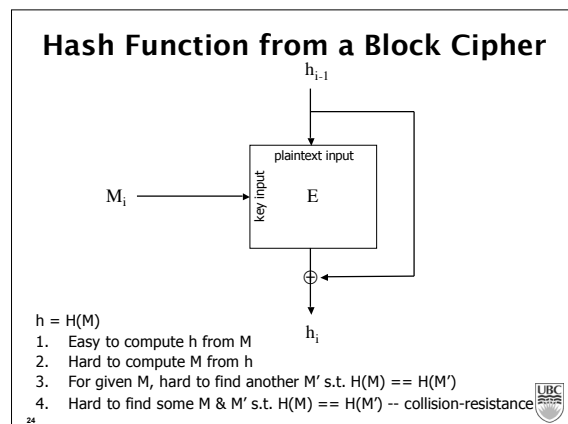


- ### Output Feedback (OFB)
- $K_1 = \{IV\}_K, K_2 = \{K_1\}_K, \dots, K_i = \{K_{i-1}\}_K, \dots$
 - Purpose: use block cipher as a stream cipher
 - $C_i = \{m_i\}_{K_i}$, e.g., $c_i = m_i \oplus K_i$



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

- ### 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?



Common Hash Functions and Applications

- Common hash functions
 - (Message Digest) MD5 value 128b
 - (Secure Hash Algorithm) SHA-1 160b value, SHA-256, SHA-512
- 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
 - $K_{i+1} = H(K_i, M_{i1}, M_{i2}, \dots)$
 - Forward security



25

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,



26