Block Cipher Operation

Raj Jain
Washington University in Saint Louis
Saint Louis, MO 63130
Jain@cse.wustl.edu

Audio/Video recordings of this lecture are available at:
http://www.cse.wustl.edu/~jain/cse571-11/
Overview

1. Double DES, Triple DES, DES-X
2. Encryption Modes for long messages:
   1. Electronic Code Book (ECB)
   2. Cipher Block Chaining (CBC)
   3. Cipher Feedback (CFB)
   4. Output Feedback (OFB)
   5. Counter (CTR) Mode
   6. XTS-AES Mode for Block-oriented Storage Devices

Double-DES

- \[ C = E_{K2}(E_{K1}(P)) \]

- **Meet-in-the-middle attack**
  - Developed by Diffie and Hellman in 1977
  - Can be used to attack any composition of 2 functions
    \[ X = E_{K1}(P) = D_{K2}(C) \]
    - Attack by encrypting P with all \(2^{56}\) keys and storing
    - Then decrypt C with keys and match X value
    - Verify with one more pair
    - Takes max of \(\mathcal{O}(2^{56})\) steps \(\Rightarrow\) Total \(2^{57}\) operations

- Only twice as secure as single DES
Triple-DES

- Use DES 3 times: $C = E_{K3}(D_{K2}(E_{K1}(P)))$
- E-D-E provides the same level of security as E-E-E
- E-D-E sequence is used for compatibility with legacy
  - $K1=K2=K3 \Rightarrow DES$
- PGP and S/MIME use this 3 key version
- Provides 112 bits of security
- Two keys with E-D-E sequence
  - $C = E_{K1}(D_{K2}(E_{K1}(P)))$
  - Standardized in ANSI X9.17 & ISO8732
  - No current known practical attacks
  - Several proposed impractical attacks might become basis of future attacks
**DES-X**

- Proposed by Ron Rivest in May 1984
- XOR 64-bit key $K_1$ before DES encryption and xor another 64-bit key $K_2$ after encryption
  \[ C = K_2 \oplus E_K(P \oplus K_1) \]
- Total Key size = 56+64+64 = 184 bits
  But increases security by 88 to 119 bits

Electronic Codebook Book (ECB)

- How to encode multiple blocks of a long message?
- Each block is encoded independently of the others
  \[ C_i = E_K(P_i) \]
- Each block is substituted like a codebook, hence name.

Diagram:

- \( P_1 \) to \( C_1 \) through Encrypt
- \( P_2 \) to \( C_2 \) through Encrypt
- \( P_N \) to \( C_N \) through Encrypt

K is the key for encryption.
ECB Limitations

- Using the same key on multiple blocks makes it easier to break
- Identical Plaintext Identical Ciphertext
  Does not change pattern:

  ![Original](image1.png) ![ECB](image2.png) ![Better](image3.png)

- NIST SP 800-38A defines 5 modes that can be used with any block cipher

Cipher Block Chaining (CBC)

- Add random numbers before encrypting
- Previous cipher blocks is chained with current plaintext block
- Use an Initial Vector (IV) to start process

\[ C_i = E_K(P_i \oplus C_{i-1}) \]

\[ C_0 = IV \]
Advantages and Limitations of CBC

- Any change to a block affects all following ciphertext blocks
- Need Initialization Vector (IV)
  - Must be known to sender & receiver
  - If sent in clear, attacker can change bits of first block, and change IV to compensate
  - Hence IV must either be a fixed value, e.g., in Electronic Funds Transfers at Point of Sale (EFTPOS)
  - Or must be sent encrypted in ECB mode before rest of message
- Sequential implementation Cannot be parallelized
Message Padding

- Last block may be shorter than others ⇒ Pad
- Pad with count of pad size [ANSI X.923]
  1. E.g., [ b1 b2 b3 0 0 0 0 5] = 3 data, 5 pad w 1 count byte
  1. A 1 bit followed by 0 bits [ISO/IEC 9797-1]
  2. Any known byte value followed by zeros, e.g., 80-00…
  3. Random data followed by count [ISO 10126]
  1. E.g., [b1 b2 b3 84 67 87 56 05]
- Each byte indicates the number of padded bytes [PKCS]
  1. E.g., [b1 b2 b3 05 05 05 05 05]
- Self-Describing Padding [RFC1570]
  - Each pad octet contains its index starting with 1
  - E.g., [b1 b2 b3 1 2 3 4 5]

Ref: [http://en.wikipedia.org/wiki/Padding_%28cryptography%29](http://en.wikipedia.org/wiki/Padding_%28cryptography%29)
Cipher Text Stealing (CTS)

- Alternative to padding
- Last 2 blocks are specially coded
- Tail bits of (n-1)st encoded block are added to nth block and order of transmission of the two blocks is interchanged.
Stream Modes of Operation

- Use block cipher as some form of **pseudo-random number generator**
- The random number bits are then XOR’ed with the message (as in stream cipher)
- Convert block cipher into stream cipher
  1. Cipher feedback (CFB) mode
  2. Output feedback (OFB) mode
  3. Counter (CTR) mode
Cipher Feedback (CFB)

- Message is added to the output of the block cipher
- Result is feed back for next stage (hence name)
- Standard allows any number of bit (1, 8, 64 or 128 etc) to be feed back, denoted CFB-1, CFB-8, CFB-64, CFB-128 etc
- Most efficient to use all bits in block (64 or 128)

\[ C_i = \text{P} \oplus \text{E}(C_{i-1}) \]

- Errors propagate for several blocks after the error

\[ C_i = P \oplus E(C_{i-1}) \]
Output Feedback (OFB)

- Output of the cipher is feedback (hence name)
- Feedback is independent of message
- Can be computed in advance

\[ O_i = E_K(O_{i-1}) \]
\[ C_i = P_i \oplus O_i \]
\[ O_{-1} = IV \]
Advantages and Limitations of OFB

- Needs an IV which is unique for each use
  - if ever reuse attacker can recover outputs
- Bit errors do not propagate
- More vulnerable to message stream modification
- Sender & receiver must remain in sync
- Only use with full block feedback
  - Subsequent research has shown that only full block feedback (i.e., CFB-64 or CFB-128) should ever be used
Counter (CTR)

- Encrypt counter value rather than any feedback value
- Different key & counter value for every plaintext block (never reused)

\[ O_i = E_K(i) \]

\[ C_i = P_i \oplus O_i \]

Diagram:

- Counter 1
  - Counter 2
  - Counter N
  - Key (K)
  - Encrypt
  - Plaintext (P_1, P_2, P_N)
  - Ciphertext (C_1, C_2, C_N)
Advantages and Limitations of CTR

- Efficiency
  - Can do parallel encryptions in h/w or s/w
  - Can preprocess in advance of need
  - Good for bursty high speed links
- Random access to encrypted data blocks
- Provable security (good as other modes)
- But must never reuse key/counter values, otherwise could break
Storage Encryption

- File encryption:
  - Different keys for different files
  - May not protect metadata, e.g., filename, creation date,
  - Individual files can be backed up
  - Encrypting File System (EFS) in NTFS provides this service

- Disk encryption:
  - Single key for whole disk or separate keys for each partition
  - Master boot record (MBR) may or may not be encrypted
  - Boot partition may or may not be encrypted.
  - Operating system stores the key in the memory
    Can be read by an attacker by cold boot

- Trusted Platform Module (TPM): A secure coprocessor chip on the motherboard that can authenticate a device
  ⇒ Disk can be read only on that system.
  Recovery is possible with a decryption password or token
Storage Encryption (Cont)

- If IV is predictable, CBC is not usable in storage because the plain text is chosen by the writer.
- Ciphertext is easily available to other users of the same disk.
- Two messages with the first blocks $b \oplus IV_1$ and $b \oplus IV_2$ will both encrypt to the same ciphertext.
- Need to be able to read/write blocks without reading/writing other blocks.
XTS-AES Mode

- XTS = **XEX**-based Tweaked Codebook mode with Ciphertext Stealing (XEX = Xor-Encrypt-xor)

- Creates a unique IV for each block using AES and 2 keys

\[
T_j = E_{K2}(i) \odot \alpha^j \quad \text{Size of } K2 = \text{size of block}
\]

\[
C_j = E_{K1}(P_j \oplus T_j) \oplus T_j \quad K1 \text{ 256 bit for AES-256}
\]

where \(i\) is logical sector # & \(j\) is block # (sector = \(n\) blocks)

\[\alpha = \text{primitive element in } GF(2^{128}) \text{ defined by polynomial } x\]
Advantages and Limitations of XTS-AES

- Multiplication is modulo $x^{128}+x^7+x^2+x+1$ in GF($2^{128}$)
- Efficiency
  - Can do parallel encryptions in h/w or s/w
  - Random access to encrypted data blocks
- Has both nonce & counter
- Defined in IEEE Std 1619-2007 for block oriented storage use
- Implemented in numerous packages and operating systems including TrueCrypt, FreeBSD, and OpenBSD softraid disk encryption software (also native in Mac OS X Lion’s FileVault), in hardware-based media encryption devices by the SPYRUS Hydra PC Digital Attaché and the Kingston DataTraveler 5000.

Summary

- 3DES generally uses E-D-E with 2 keys $\Rightarrow$ 112b protection
- ECB: Same ciphertext for the same plaintext $\Rightarrow$ Easier to break
Homework 6

6.4 For each of the modes ECB, CBC and CTR:

a. Identify whether decrypted plaintext block $P_3$ will be corrupted if there is an error in block $C_1$ of the transmitted cipher text.

b. Assuming that the ciphertext contains $N$ blocks, and that there was a bit error in the source version of $P_1$, identify through how many ciphertext blocks this error is propagated.