Lecture 7: Block Ciphers

COSC362 Data and Network Security

Book 1: Chapters 4 and 6 – Book 2: Chapters 2 and 20

Spring Semester, 2021

Motivation

- Block ciphers are the main bulk encryption algorithms used in commercial applications.
- Standardised block cipher AES and legacy cipher DES are widely deployed in real applications.
- AES algorithm validation list (by NIST) includes over 5000 implementations:
  - USB drives
  - door controllers
  - media server encryption
  - disk encryption
  - Bluetooth devices

Outline

- Block Cipher Principles
  - Product Cipher and Iterated Cipher
  - Substitution-Permutation Network
  - Feistel Cipher
  - Standard Security Properties
- DES
  - History
  - Algorithm
  - Brute Force Attack
  - Double and Triple DES
- AES
  - History
  - Algorithm
  - Comparisons between AES and DES
- Conclusion

Outline

- Block Cipher Principles
  - Product Cipher and Iterated Cipher
  - Substitution-Permutation Network
  - Feistel Cipher
  - Standard Security Properties
- DES
  - History
  - Algorithm
  - Brute Force Attack
  - Double and Triple DES
- AES
  - History
  - Algorithm
  - Comparisons between AES and DES
- Conclusion

Block Ciphers

- Symmetric key ciphers where each block of plaintext is encrypted with the SAME key.
- A *block* is a set of plaintext symbols of a fixed size:
  - Typical block sizes for modern block ciphers between 64 and 256 bits.
- Used in certain configurations called *modes of operation* (next lecture).

Notations

- Plaintext block P (length is n bits)
- Ciphertext block C (length is n bits)
- Key K (length is k bits)
- *Encryption:* $C = E(P, K)$
- *Decryption:* $P = D(C, K)$

Criteria for Block Cipher Design

Claude Shannon discussed 2 important encryption techniques in 1940:

- *Confusion:* involving substitution to make the relationship between K and C as complex as possible.
- *Diffusion:* involving transformations to dissipate the statistical properties of P across C.

Shannon proposed to use these techniques repeatedly using the concept of *product cipher*.

Product Cipher

- Cryptosystem where encryption is formed by applying (also *composing*) several sub-encryption functions.
- Most block ciphers are composition of simple functions f_i, for $1 \leq i \leq r$, s.t. each f_i has its own key K_i:

$$C = E(P, K) = f_r(\cdots(f_2(f_1(P, K_1), K_2)\cdots), K_r)$$

Iterated Cipher

Most modern block ciphers are special product ciphers, called *iterated ciphers*:

- Encryption is divided into r similar *rounds*.
- Sub-encryption functions are all the same function g, called the *round function*.
- Key K_i is derived from the overall master key K:
  - K_i is called the *round key* or *subkey*
  - K_i is derived from K using a process called *key schedule*

Encryption in Iterated Ciphers

Given a plaintext block P, a round function g and round keys $K_1, K_2, \cdots, K_r$, the ciphertext block C is derived through r rounds as follows:

$$
\begin{aligned}
W_0 &= P \\
W_1 &= g(W_0, K_1) = g(P, K_1) \\
W_2 &= g(W_1, K_2) \\
&\cdots \\
W_r &= g(W_{r-1}, K_r) = C
\end{aligned}
$$

Decryption in Iterated Ciphers

There must be an inverse function g^{-1} s.t. $g^{-1}(g(W, K_i), K_i) = W$ for all keys K_i and blocks W:

$$\begin{aligned}
W_r &= C \\
W_{r-1} &= g^{-1}(W_r, K_r) = g^{-1}(C, K_r) \\
W_{r-2} &= g^{-1}(W_{r-1}, K_{r-1}) \\
&\ldots \\
W_0 &= g^{-1}(W_1, K_1) = P
\end{aligned}$$

Decryption is thus the reverse of encryption.

Types of Iterated Cipher

- *Substitution-Permutation Network (SPN)*
  - Example: Advanced Encryption Standard (AES)
- *Feistel Cipher*
  - Example: Data Encryption Standard (DES)

Substitution-Permutation Network

- Block length n must allow each block to be split into m sub-blocks of length l:
  - $n = l \times m$
- 2 operations:
  - Substitution π_S (called substitution box or simply S-box) operates on sub-blocks of length l bits:

$$\pi_S : \{0, 1\}^l \to \{0, 1\}^l$$

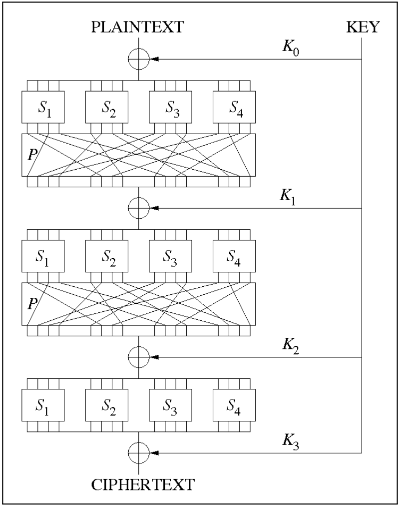
  - Permutation π_P (called permutation box or simply P-box) swaps the inputs from $\{1, \cdots, n\}$, similarly to transposition ciphers:

$$\pi_P : \{1, \cdots, n\} \to \{1, \cdots, n\}$$

Steps in the SPN Round Function

1. Round key K_i is XORed with the current state block W_i:
   - $K_i \oplus W_i$
2. Each sub-block is substituted by applying π_S
3. The whole block is permuted using π_P

Illustration with 3 Rounds

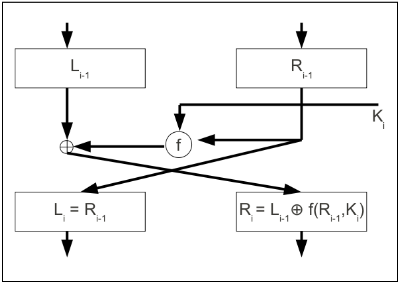


- Encrypting a plaintext block of n bits into a ciphertext block of n bits.
- 4 S-boxes S_i ($m = 4$)
- 1 P-box P
- 4 Round keys K_i

Feistel Cipher

- From Horst Feistel, a cryptographer at IBM who influenced the design of DES.
- Round function swaps the 2 halves of the block and forms a new right hand half.
- Process sometimes called *Feistel network*:
  - It can be seen as a network where the 2 halves of plaintext block travel through.

Encryption



1. Split plaintext block $P = W_0$ into 2 halves (L_0, R_0)
2. For each round, perform:
   - $L_i = R_{i-1}$
   - $R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$
3. Output ciphertext block $C = W_r = (L_r, R_r)$

Decryption

1. Split ciphertext block C into 2 halves (L_r, R_r)
2. For each round, perform:
   - $L_{i-1} = R_i \oplus f(L_i, K_i)$
   - $R_{i-1} = L_i$
3. Output plaintext block $P = (L_0, R_0)$

- No need to invert f:
  - Decrypt for ANY function f
- Choice of f is critical for security:
  - f is the only non-linear part of the encryption

Differential and Linear Cryptanalysis

Differential cryptanalysis:

- First published in 1992.
- Chosen plaintext attack.
- Based on the idea that the difference between 2 input plaintexts can be correlated to the difference between 2 output ciphertexts.

Linear cryptanalysis:

- First published in 1993.
- Known plaintext attack.
- Theoretically used to break DES.

Modern block ciphers normally designed to be immune to both differential and linear cryptanalysis.

Avalanche Effects

Key avalanche:

- A SMALL change in the key (with the same plaintext) should result in a LARGE change in the ciphertext.
- Related to Shannon's notion of confusion.

Plaintext avalanche:

- A SMALL change in the plaintext should result in a LARGE change in the ciphertext.
- Changing 1 bit of plaintext should change each of the bits in the ciphertext with probability $1/2$.
- Related to Shannon's notion of diffusion.

Outline

- Block Cipher Principles
  - Product Cipher and Iterated Cipher
  - Substitution-Permutation Network
  - Feistel Cipher
  - Standard Security Properties
- DES
  - History
  - Algorithm
  - Brute Force Attack
  - Double and Triple DES
- AES
  - History
  - Algorithm
  - Comparisons between AES and DES
- Conclusion

Data Encryption Standard (DES)

- Designed by researchers from IBM.
- Submitted to the National Bureau of Standards (NBS) in US in a call for publicly available ciphers.
- Approved in 1977 as the US standard for encryption.
- Encryption and decryption definitions are public property.
- Security resides in difficulty of decryption without knowledge of key.
- 16-round Feistel cipher with key length of 56 bits and data block length of 64 bits.

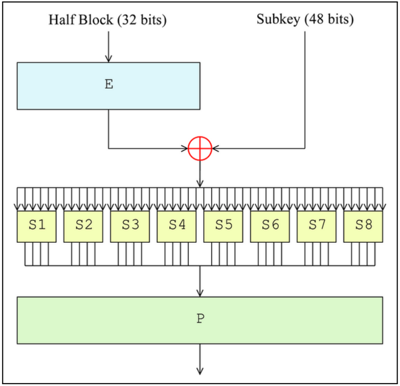
Encryption Steps

P is an input plaintext block of 64 bits:

1. ALL bits of P are permuted using an initial fixed permutation IP.
2. 16 rounds of Feistel operation are applied, denoted by function f:
   - A different 48-bit subkey is used for each round
3. A final fixed inverse permutation IP^{-1} is applied.

Output the ciphertext block C of 64 bits.

Feistel Operation



For each round:

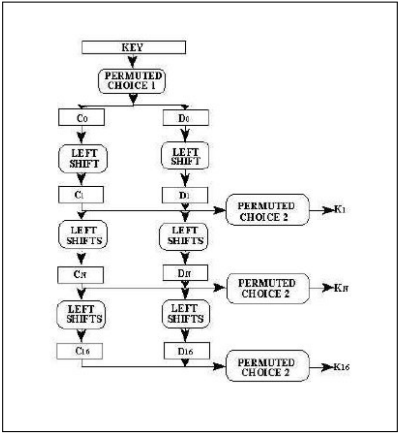
1. Expand 32 bits to 48 bits
2. XOR 48 bits to 48-bit subkey
3. Break 48 bits into 8 blocks of 6 bits
4. Put each block W_i into its substitution table S_i, resulting into blocks of length 4
5. Apply permutation to result into 32 (= 4×8) bits.

S-box Example

Row No.	Column No. 0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

- Let input block W be $x_1x_2x_3x_4x_5x_6$
- Digits x_1 and x_6 define row number between 0 and 3
- Digits x_2, x_3, x_4, x_5 define column number between 0 and 15
- Example: $W = 100101$
  - $x_1 = 1$ and $x_6 = 1$, thus 11, that is 3
  - $x_2 = 0, x_3 = 0, x_4 = 1, x_5 = 0$, thus 0010, that is 2

Key Schedule



- Each of the 16 rounds involves 48 bits of the 56-bit key
- Each 48-bit subkey is defined by a series of permutations and shifts on the full 56-bit key

Brute Force Attack

- Testing all possible 2^k keys in order to find the key K:
  - k is the size of K
- Key identified by using a small number of ciphertext blocks or by looking for low entropy in decrypted plaintext.
- 2^{56} DES keys to test:
  - On average, it would take $2^{56}/2 = 2^{55}$ trial samples to find the key:
    - Trying all keys with last bit equal to 0
- Short DES key size was criticised from the start.

Real World Attacks – Part 1

- 1997:
  - $\$10,000$ DES challenge in February (RSA)
  - Solved in June
  - Linked together thousands of computers over the Internet (parallel processing)
- 1998:
  - EFF DES cracker built, costing less than $\$25,000$
  - Less than 3 days to find 56-bit DES key
  - Searched 88 billion keys per second
- 1999:
  - EFF DES cracker plus distributed search
  - 22 hours and 15 minutes to find 56-bit DES key
  - Searched 245 billion keys per second
- 2007:
  - Parallel FGPA-based machine Copacobana built, costing $\$10,000$
  - Less than 1 week to find 56-bit DES key

Real World Attacks – Part 2

- 2016:
  - Open source password cracking software *hashcat* added in DES brute force searching on general purpose GPUs
  - Systems with 8 GTX 1080 Ti GPUs (each costing $\$1,000$) recover a key under 2 days
- 2017:
  - Chosen plaintext attacks utilizing rainbow tables (precomputed tables for caching the output of cryptographic hash functions)
  - Recovering the DES key for a single specific chosen plaintext 1122334455667788 in 25 seconds.

Double Encryption

- Let K_1 and K_2 be 2 block cipher keys.
- Encryption: $C = E(E(P, K_1), K_2)$.
- If both keys have length k, then exhaustive attacks require 2^{2k-1} trials on average. Why? (cf slide 27)
- Time-memory trade-off which reduces it using Meet-In-The-Middle (MITM) method.

MITM Attack Steps

Let (P, C) be a single plaintext-ciphertext pair:

1. For each key K, store $C' = E(P, K)$ in memory.
2. Check if $D(C, K') = C'$ for any key K':
   - K from 1. is K_1 and K' from 2. is K_2
3. Check if key values in 2. work for other (P, C) pairs.

MITM Attack Applied to Double DES

It requires:

- Storage of 1 plaintext block for every key:
  - Storage of 2^{56} 64-bit blocks
- A single encryption for every key:
  - 2^{56} encryption operations
- A single decryption for every key:
  - 2^{56} decryption operations

Expensive but much easier than brute force search through $2^{2 \cdot 56 - 1} = 2^{111}$ keys.

Triple Encryption

- Much better security
- 3 keys K_1, K_2, K_3
- Encryption: $C = E(D(E(P, K_1), K_2), K_3)$.
- Secure against MITM attack. Why?

Standardised Options

Options for 1999 DES version:

- 3 independent keys K_1, K_2, K_3
  - the most secure
- 2 keys $K_1 = K_3$ and K_2
  - still secure enough
- 1 key $K_1 = K_2 = K_3$
  - backward compatible with single key DES (hence vulnerable to brute force search)

NIST SP 800-131A (2015):

- 2-key triple DES allowed ONLY for legacy use (decryption only).
- 3-key triple DES remains approved.

Current Usage

- OpenSSL does not include Triple DES by default since V1.1.0 (August 2016), considering it as "weak cipher".
- In December 2018, Microsoft announced the retirement of Triple DES throughout their Office 365 service.

Outline

- Block Cipher Principles
  - Product Cipher and Iterated Cipher
  - Substitution-Permutation Network
  - Feistel Cipher
  - Standard Security Properties
- DES
  - History
  - Algorithm
  - Brute Force Attack
  - Double and Triple DES
- AES
  - History
  - Algorithm
  - Comparisons between AES and DES
- Conclusion

Advanced Encryption Standard (AES)

- AES was designed in an open competition due to controversy over DES.
- Process over several years with much public debate.
- 15 original submissions.
- 5 finalists widely believed secure.
- Winner is “Rijndael” by Belgian cryptographers Vincent Rijmen and Joan Daeman.

Overview

- 128-bit data block
- 128-, 192- or 256-bit master key
- 10, 12 or 14 rounds (for 128-, 192- or 256-bit master key respectively)
- Byte-based design
- Substitution-permutation network (SPN):
  - Initial round key addition
  - 10, 12 or 14 (encryption/decryption) rounds w.r.t. to the length of the master key
  - Final round

State Matrix (byte-based)

16-byte data block size:

a_{00}	a_{01}	a_{02}	a_{03}
a_{10}	a_{11}	a_{12}	a_{13}
a_{20}	a_{21}	a_{22}	a_{23}
a_{30}	a_{31}	a_{32}	a_{33}

Mixture of finite field operations in $GF(2^8)$ and bit string operations.

Round Transformation

4 basic operations:

1. ByteSub (non-linear sustitution)
2. ShiftRow (permutation)
3. MixColumn (diffusion)
4. AddRoundKey

- Substitution-permutation network with block length $n = 128$ and sub-block length $l = 8$.
- S-box is a look-up table, mathematically defined in $GF(2^8)$.
- Cryptool has a nice animation of the encryption process.

Key Schedule

- Master key is 128 bits (resp. 192 and 256).
- Each of the 10 (resp. 12 and 14) rounds uses a 128-bit subkey.
- 1 subkey per round + 1 initial subkey:
  - 11 subkeys in total (resp. 13 and 15)
- Deriving the 128-bit subkeys from the master key.

Security

- Some cracks have appeared but no significant breaks.
- Attacks exist on reduced-round versions.
- Related key attack: requiring the attacker to obtain a ciphertext encrypted with a key related to the actual key in a specified way.
- Most serious real attacks so far reduce effective key size by around 2 bits.

Comparison

Data block size:

- DES: 64 bits
- AES: 128 bits

Key size:

- DES: 56 bits
- AES: 128, 192 or 256 bits

Design structure:

- Both are iterated ciphers
- DES has a Feistel structure while AES is SPN
- DES is bit-based and AES is byte-based
- AES is substantially faster in both hardware and software

Outline

Block Cipher Principles
- Product Cipher and Iterated Cipher
- Substitution-Permutation Network
- Feistel Cipher
- Standard Security Properties

DES
- History
- Algorithm
- Brute Force Attack
- Double and Triple DES

AES
- History
- Algorithm
- Comparisons between AES and DES

Conclusion

Conclusion

- Block ciphers are the workhorses of secure communications.
- AES is the current choice, and Triple DES is still important.
- Designing good block ciphers is difficult and time-consuming.
- Block ciphers are used as building blocks for confidentiality and authentication.