Cryptology Basics

Zhang Tianyu

School of Physical and Mathematical Science,
Nanyang Technological University

December 2, 2021

Outline

Outline

Cryptology

Cryptology is the practice and study of secret communication.

Cryptology

Cryptology is the practice and study of secret communication.

Two branches:

- Cryptography: The "design" of cryptosystems
- Cryptanalysis: The "break" of cryptosystems

Act as mutual restraints and push mutual growths

Cryptosystem

Cryptosystem: a suite of cryptographic algorithms to implement a particular security service.

Five components:

- P: plaintext space
- C: ciphertext space
- K: key space
- E: encryption rule set
- D: decryption rule set

Cryptosystem

Cryptosystems could be categorised from different perspectives.

Cryptosystem

Cryptosystems could be categorised from different perspectives.

From different uses of keys:
- Symmetric/Secret Key Algorithms (e.g. DES, AES)
- Asymmetric/Public Key Algorithms (e.g. RSA)

Cryptosystem

Cryptosystems could be categorised from different perspectives.

From different uses of keys:
- Symmetric/Secret Key Algorithms (e.g. DES, AES)
- Asymmetric/Public Key Algorithms (e.g. RSA)

From different operating units on messages:
- Block Cipher (e.g. Blowfish)
- Stream Cipher (e.g. RC4)

Cryptography

Security Services $\rightarrow$ *"Guidelines"*
The security goals that is intended to fulfill.

- Confidentiality
- Data Integrity
- Authentication
- Non-repudiation

Cryptography Primitives $\rightarrow$ *"Basic Components"*
The tools and techniques that could be used to achieve security goals.

- Encryption
- Hash functions
- Message Authentication Codes (MAC)
- Digital Signature

Outline

Characteristics of block ciphers:

- The plaintext is divided into fixed-sized chunks called blocks
- A block is specified to be a bitstring (string of 0's and 1's) of a fixed length, namely block length
- Encrypt/decrypt one block at a time

Block ciphers

Characteristics of block ciphers:

- The plaintext is divided into fixed-sized chunks called blocks
- A block is specified to be a bitstring (string of 0's and 1's) of a fixed length, namely block length
- Encrypt/decrypt one block at a time

Iterated ciphers:

- Most modern-day block ciphers are designed to be iterated ciphers
- Contained multiple rounds to enhance security.
- Repeated encryption process with expanded subkeys

Substitution-Permutation Network (SPN)

Commonly used structure in block cipher

Let the block length equals lm, where l and m are positive integers. A block is thus regarded as the concatenation of m l-bit substrings:

$$x = x_1||x_2||...||x_i||...||x_m$$

, where $|x_i| = m$, $i = 1, 2, ..., m$

- S-Box (Substitution): substitute each substring with another l-bit string.

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

- P-Box (Permutation): reorders the whole lm bits.

$$\pi_P : \{1, 2, ..., lm\} \to \{1, 2, ..., lm\}$$

SPN Structure

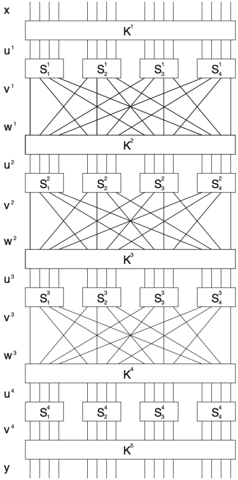

Figure: A 4-Round SPN

SPN Structure

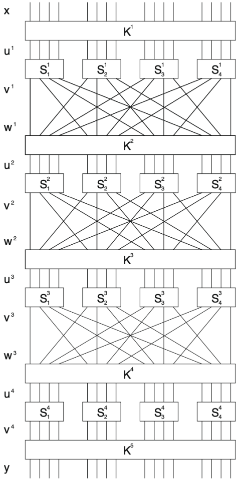

Figure: A 4-Round SPN

- Whitening process
- Symmetric in structure
- Simple and efficient implementation in hardware and software (look-up table)
- Easy improvement by using larger key size (more rounds) and longer block length (larger S-Boxes)
- Multiple variations

AES Background

- Proposed by Vincent Rijmen and Joan Daemen
- Established in 2001 by NIST
- A symmetric-keyed SPN-based block cipher algorithm
- Fixed block length 128 bits
- Three different key lengths: 128/196/256 bits (10/12/14 rounds)

AES Structure

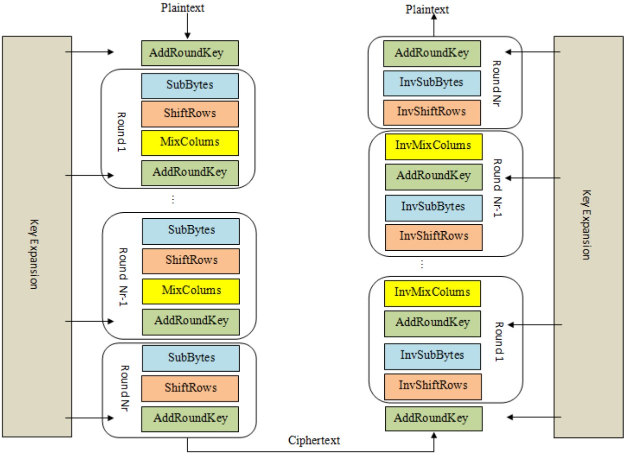

Figure: AES Algorithm Illustration

Block $\rightarrow 4 * 4$ grid, containing 8-bit substrings (i.e. l=8, m=16)

AES Algorithm Explained

Block $\rightarrow 4 * 4$ grid, containing 8-bit substrings (i.e. l=8, m=16)

Operations:

- *AddRoundKey*: XOR-ing the round key
- *SubBytes*: Permutation on $GF(2^8)$ (S-Box)
- *ShiftRows*: Circular left shift (linear transformation)
- *MixColumns*: Matrix multiplication on $GF(2^8)$ (P-Box)

AES Features

Shannon's theory on confusion and diffusion:

- Confusion: Adopting complex transformations (both nonlinear and linear)
  $\rightarrow$ One bit ciphertext depend on multiple parts of the key
- Diffusion: Ensuring Avalanche effect
  $\rightarrow$ One bit change in plaintext result in significantly different ciphertext

AES Features

Shannon's theory on confusion and diffusion:

- Confusion: Adopting complex transformations (both nonlinear and linear)
  $\rightarrow$ One bit ciphertext depend on multiple parts of the key
- Diffusion: Ensuring Avalanche effect
  $\rightarrow$ One bit change in plaintext result in significantly different ciphertext

Purpose for AES operations:

- *SubBytes*: Add non-linearity
- *ShiftRows*: Add linearity
- *MixColumns*: MDS matrix reaching Singleton Bound

AES Actualization

`github.com/zty-cn/AES128`

Outline

Hash Functions

Hash function: a deterministic construction of a fixed-length message digest for plaintext of arbitrary length, usually 160/256 bits.
$\rightarrow$ "compression"

Hash Functions

Hash function: a deterministic construction of a fixed-length message digest for plaintext of arbitrary length, usually 160/256 bits.
$\rightarrow$ "compression"

Four components:

- X: the set of possible messages
- Y: finite set of possible message digests or authentication tags
- K: key space
- H: hash function space, for each $k \in K$, $\exists h_K \in H : X \rightarrow Y$

Message Authentication Code (MAC): keyed hash function

Security of Hash Functions

If a hash function is considered secure, then the following three problems should be difficult to solve (resistance):

- Preimage
  Given $h : X \to Y$ and $y \in Y$, find $x \in X \implies h(x) = y$
- Second Preimage
  Given $h : X \to Y$ and $x \in X$, find $x' \in X \implies h(x) = h(x')$
- Collision
  Given $h : X \to Y$, find $x, x' \in X \implies h(x) = h(x')$

Security of Hash Functions

If a hash function is considered secure, then the following three problems should be difficult to solve (resistance):

- Preimage
  Given $h : X \to Y$ and $y \in Y$, find $x \in X \implies h(x) = y$
- Second Preimage
  Given $h : X \to Y$ and $x \in X$, find $x' \in X \implies h(x) = h(x')$
- Collision
  Given $h : X \to Y$, find $x, x' \in X \implies h(x) = h(x')$

By using the reduction technique, collision is proved to be the easiest among the three fundamental problems.

Find Collision

Example for finding collision $\rightarrow$ *Birthday Paradox*: In a group of only 23 people, there is 50% chance that two people share the same birthday.

Find Collision

Example for finding collision $\rightarrow$ *Birthday Paradox*: In a group of only 23 people, there is 50% chance that two people share the same birthday.

Let $M = |Y|$, finding collision is an $O(\sqrt{M})$ algorithm. Preimage and Second preimage are $O(M)$ algorithms.

Using proper (ε, Q) notation: given average-case success probability ε, the number of queries for collision: $Q \approx \sqrt{-2\ln(1-\varepsilon)}\sqrt{M}$. when $\varepsilon = 1/2$, $Q \approx 1.17\sqrt{M}$.

Merkle-Damgard Construction

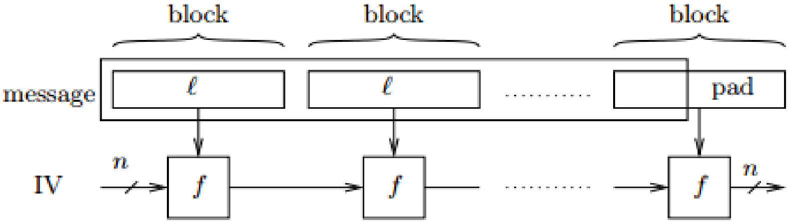

Figure: Merkle-Damgard Algorithm Illustration

- Compressing function $f : \{0,1\}^n * \{0,1\}^l \rightarrow \{0,1\}^n$
- Right pad the message to a multiple of l
- Iterated process of compression

Outline

Optimal senario: no bias (i.e. each bit in ciphertext has equal probability of being 0 or 1, independent from plaintext)

Cryptanalysis on block ciphers

Optimal senario: no bias (i.e. each bit in ciphertext has equal probability of being 0 or 1, independent from plaintext)

Linear Cryptanalysis:
How are input bits and output bits related.
$\rightarrow$ Find biased subsets of input bits and output bits (masks).

Differential Cryptanalysis:
How will the output bits change if input bits change.
$\rightarrow$ Find biased pairs of input XOR and output XOR (differentials).

Algorithmetic Structure

- Tabulate the distribution table
- Start from the most biased pairs
- Find propagation trails in consecutive rounds
- Accelerate on finding the key

Cryptanalysis Actualization

`github.com/zty-cn/TAK-toy-cipher-cryptanalysis`

Thank you for listening!