An Overview of Block Cipher Cryptanalysis

Muhammad Reza Z’aba

MIMOS Berhad, Malaysia
reza [dot] zaba [at] mimos [dot] my

Venue: Universiti Putra Malaysia
Outline

1. Introduction
   - Objectives of this Presentation

2. Overview of Block Ciphers
   - Basic Components of Block Ciphers
   - Evaluating a Cipher

3. What is Cryptanalysis?
   - The Basics of Cryptanalysis
   - Example: Differential Cryptanalysis
   - Other Cryptanalysis Techniques
   - Breaking a Cipher
   - Why Cryptanalysis is Important?

4. Resources
Introduction

Objectives of this Presentation

Outline

1. Introduction
   - Objectives of this Presentation

2. Overview of Block Ciphers
   - Basic Components of Block Ciphers
   - Evaluating a Cipher

3. What is Cryptanalysis?
   - The Basics of Cryptanalysis
   - Example: Differential Cryptanalysis
   - Other Cryptanalysis Techniques
   - Breaking a Cipher
   - Why Cryptanalysis is Important?

4. Resources
Introduction

Objectives of this Presentation

At the end of presentation, it is hoped that the audience is able to

1. understand the basic components of a block cipher
2. understand the basic concepts of cryptanalysis
3. know the importance of cryptanalysis
At the end of presentation, it is hoped that the audience is able to

1. understand the basic components of a block cipher
2. understand the basic concepts of cryptanalysis
3. know the importance of cryptanalysis
At the end of presentation, it is hoped that the audience is able to

1. understand the basic components of a block cipher
2. understand the basic concepts of cryptanalysis
3. know the importance of cryptanalysis
Introduction

Objectives of this Presentation

At the end of presentation, it is hoped that the audience is able to

1. understand the basic components of a block cipher
2. understand the basic concepts of cryptanalysis
3. know the importance of cryptanalysis
Overview of Block Ciphers

Basic Components of Block Ciphers

Outline

1. Introduction
   - Objectives of this Presentation

2. Overview of Block Ciphers
   - Basic Components of Block Ciphers
   - Evaluating a Cipher

3. What is Cryptanalysis?
   - The Basics of Cryptanalysis
   - Example: Differential Cryptanalysis
   - Other Cryptanalysis Techniques
   - Breaking a Cipher
   - Why Cryptanalysis is Important?

4. Resources
Overview of Block Ciphers

Basic Components of Block Ciphers

Block ciphers are mainly used to provide confidentiality

- **The Advanced Encryption Standard (AES)** – used by the US government to protect sensitive but unclassified information → SECRET → TOP SECRET [Committee on National Security Systems, 2003]

- **IDEA** – used in Pretty Good Privacy (PGP) and Secure Shell (SSH) [Lai et al., 1991]

- **Kasumi** – used for securing mobile communications within the 3rd Generation Partnership Project (3GPP) [3rd Generation Partnership Project, 2007]

- **CLEFIA** – designed by Sony for use in copyright protection and authentication [Shirai et al., 2007]

- **KeeLoq** – used in remote control device to lock/unlock cars [Courtois et al., 2008]
Block ciphers are mainly used to provide confidentiality

- **The Advanced Encryption Standard (AES)** – used by the US government to protect sensitive but unclassified information → SECRET → TOP SECRET [Committee on National Security Systems, 2003]
- **IDEA** – used in Pretty Good Privacy (PGP) and Secure Shell (SSH) [Lai et al., 1991]
- **Kasumi** – used for securing mobile communications within the 3rd Generation Partnership Project (3GPP) [3rd Generation Partnership Project, 2007]
- **CLEFIA** – designed by Sony for use in copyright protection and authentication [Shirai et al., 2007]
- **KeeLoq** – used in remote control device to lock/unlock cars [Courtois et al., 2008]
Block ciphers are mainly used to provide confidentiality

- **The Advanced Encryption Standard (AES)** – used by the US government to protect sensitive but unclassified information → SECRET → TOP SECRET [Committee on National Security Systems, 2003]
- **IDEA** – used in Pretty Good Privacy (PGP) and Secure Shell (SSH) [Lai et al., 1991]
- **Kasumi** – used for securing mobile communications within the 3rd Generation Partnership Project (3GPP) [3rd Generation Partnership Project, 2007]
- **CLEFIA** – designed by Sony for use in copyright protection and authentication [Shirai et al., 2007]
- **KeeLoq** – used in remote control device to lock/unlock cars [Courtois et al., 2008]
Overview of Block Ciphers
Basic Components of Block Ciphers

- **SMS4** – used by the Chinese government as a national standard [Office of State Commercial Cryptography Administration, P.R. China, Diffie and Ledin, 2008]
- **SEED** and **ARIA** – used by the Korean government as a national standard [National Security Research Institute, 2005]
- **Cryptomeria (C2)** – used for digital rights management and jointly developed by IBM, Intel, Panasonic and Toshiba
- **MULTI2** – used to encrypt high definition television broadcast in Japan and proposed by Hitachi
What is a Block Cipher?

An algorithm capable of transforming a message block (plaintext) into unreadable form (ciphertext) and vice-versa via a secret master key.
What is a Block Cipher?

An algorithm capable of transforming a message block (plaintext) into unreadable form (ciphertext) and vice-versa via a secret master key.

Example

\[ \text{mybirthday123456} \]

\[ E \hspace{1cm} K \hspace{1cm} E^{-1} \]

secure channel

insecure channel
What is a Block Cipher?

An algorithm capable of transforming a message block (plaintext) into unreadable form (ciphertext) and vice-versa via a secret master key.

Example

DO NOT invite Reza to our party.

mybirthday123456

$\text{secure channel}$

$\text{insecure channel}$

$E^{-1}$
What is a Block Cipher?

An algorithm capable of transforming a message block (plaintext) into unreadable form (ciphertext) and vice-versa via a secret master key.

Example

DO NOT invite Reza to our party.

mybirthday123456

$K$

secure channel

insecure channel

$E^{-1}$

$*/8V\ &a@? [M#!3== \\
|"R$]e%(z?2A`+0:
What is a Block Cipher?

An algorithm capable of transforming a message block (plaintext) into unreadable form (ciphertext) and vice-versa via a secret master key.

Example

\[
\text{DO NOT invite Reza to our party.}
\]

\[\begin{align*}
\text{mybirthday123456} & \quad \text{secure channel} \\
K & \quad \text{insecure channel} \\
\text{DO NOT invite Reza to our party.} & \quad E^{-1}
\end{align*}\]
What is a Block Cipher?

An algorithm capable of transforming a message block (plaintext) into unreadable form (ciphertext) and vice-versa via a secret master key.

Example

- **mybirthday123456**
  - **K**
  - **C**
  - **E**
  - **Encrypt**
  - **E**⁻¹
  - **P**

DO NOT invite Reza to our party.
What is a Block Cipher?

An algorithm capable of transforming a message block (plaintext) into unreadable form (ciphertext) and vice-versa via a secret master key.

Example

DO NOT invite Reza to our party.

mybirthday123456

K

secure channel

insecure channel

Encrypt

Decrypt

*/8V &a@? [M#!3==

|"R$] e%(z?2A‘+0:
Overview of Block Ciphers

Basic Components of Block Ciphers

Anatomy of an $R$-round Block Cipher

Diffusion*
- Key Mixing – adding secrecy into current words
- Linear Trans. $L_1$ – adding inter-word relationship

Confusion*
Nonlinear $S$ – adding nonlinearity

*Shannon (1949)

Note: $K^r$ denote round subkey in round $r$
Overview of Block Ciphers
Basic Components of Block Ciphers

Anatomy of an $R$-round Block Cipher

Diffusion*
- Key Mixing – adding secrecy into current words
- Linear Trans. $L_{1}$ – adding inter-word relationship

Confusion*
Nonlinear $S$ – adding nonlinearity

*Shannon (1949)

Note: $K^{r}$ denote round subkey in round $r$
Overview of Block Ciphers
Basic Components of Block Ciphers

Anatomy of an $R$-round Block Cipher

**Diffusion***
- Key Mixing – adding secrecy into current words
- Linear Trans. $L_1$ – adding inter-word relationship

**Confusion***
Nonlinear $S$ – adding nonlinearity

*Shannon (1949)

Note: $K^r$ denote round subkey in round $r$
Sample Toy Cipher

- 16-bit message and key block size
- 4 rounds
- Plaintext block $P = X^1 = (X_1^1, X_2^1, \ldots, X_{16}^1)$ where $X_i^1 \in \{0, 1\}$
- Ciphertext block $C = X^5 = (X_1^5, X_2^5, \ldots, X_{16}^5)$
- Round subkeys $K^1, K^2, K^3, K^4, K^5$

Encryption

$$X^{r+1} = \theta(\gamma(\sigma_{K^r}(X^r))), \quad r = 1, 2, 3$$
$$C = \sigma_{K^5}(\gamma(\sigma_{K^4}(X^4)))$$
Overview of Block Ciphers
Basic Components of Block Ciphers

Round Function $F$ in round $r$

\[
\begin{align*}
X^r &
\rightarrow Y^r \\
Y^r &
\rightarrow \sigma_{K^r}(X^r) = X^r \oplus K^r \\
Z^r &
\rightarrow \gamma(Y^r) \\
X^{r+1} &
\rightarrow \theta(Z^r)
\end{align*}
\]

S-box $S_i^r(X)$

<table>
<thead>
<tr>
<th>$X$</th>
<th>$S_i^r(X)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>F</td>
</tr>
<tr>
<td>1</td>
<td>D</td>
</tr>
<tr>
<td>2</td>
<td>8</td>
</tr>
<tr>
<td>3</td>
<td>A</td>
</tr>
<tr>
<td>4</td>
<td>7</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>6</td>
<td>1</td>
</tr>
<tr>
<td>7</td>
<td>3</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$X$</th>
<th>$S_i^r(X)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>B</td>
</tr>
<tr>
<td>9</td>
<td>9</td>
</tr>
<tr>
<td>A</td>
<td>0</td>
</tr>
<tr>
<td>B</td>
<td>2</td>
</tr>
<tr>
<td>C</td>
<td>E</td>
</tr>
<tr>
<td>D</td>
<td>C</td>
</tr>
<tr>
<td>E</td>
<td>4</td>
</tr>
<tr>
<td>F</td>
<td>6</td>
</tr>
</tbody>
</table>

Transformations

- $Y^r = \sigma_{K^r}(X^r) = X^r \oplus K^r$
- $Z^r = \gamma(Y^r)$
- $X^{r+1} = \theta(Z^r)$
Overview of Block Ciphers

Basic Components of Block Ciphers

**Round Function** \( F \) in round \( r \)

- \( X^r \)
- \( Y^r \)
- \( Z^r \)
- \( X^{r+1} \)

\[
Y^r = \sigma_{K^r}(X^r) = X^r \oplus K^r
\]

\[
Z^r = \gamma(Y^r)
\]

\[
X^{r+1} = \theta(Z^r)
\]

**S-box** \( S_i^r(X) \)

<table>
<thead>
<tr>
<th>X</th>
<th>( S_i^r(X) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>F</td>
</tr>
<tr>
<td>1</td>
<td>D</td>
</tr>
<tr>
<td>2</td>
<td>8</td>
</tr>
<tr>
<td>3</td>
<td>A</td>
</tr>
<tr>
<td>4</td>
<td>7</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>6</td>
<td>1</td>
</tr>
<tr>
<td>7</td>
<td>3</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>X</th>
<th>( S_i^r(X) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>B</td>
</tr>
<tr>
<td>9</td>
<td>9</td>
</tr>
<tr>
<td>A</td>
<td>0</td>
</tr>
<tr>
<td>B</td>
<td>2</td>
</tr>
<tr>
<td>C</td>
<td>E</td>
</tr>
<tr>
<td>D</td>
<td>C</td>
</tr>
<tr>
<td>E</td>
<td>4</td>
</tr>
<tr>
<td>F</td>
<td>6</td>
</tr>
</tbody>
</table>
Overview of Block Ciphers

Basic Components of Block Ciphers

Round Function $F$ in round $r$

$$F^r(x, y, z) = \sigma_{K^r}(x) \oplus K^r$$

$$z^r = \gamma(y^r)$$

$$x^{r+1} = \theta(z^r)$$

S-box $S_i^r(x)$

<table>
<thead>
<tr>
<th>$X$</th>
<th>$S_i^r(X)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>F</td>
</tr>
<tr>
<td>1</td>
<td>D</td>
</tr>
<tr>
<td>2</td>
<td>8</td>
</tr>
<tr>
<td>3</td>
<td>A</td>
</tr>
<tr>
<td>4</td>
<td>7</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>6</td>
<td>1</td>
</tr>
<tr>
<td>7</td>
<td>3</td>
</tr>
</tbody>
</table>

$X$ | $S_i^r(X)$ |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>B</td>
</tr>
<tr>
<td>9</td>
<td>9</td>
</tr>
<tr>
<td>A</td>
<td>0</td>
</tr>
<tr>
<td>B</td>
<td>2</td>
</tr>
<tr>
<td>C</td>
<td>E</td>
</tr>
<tr>
<td>D</td>
<td>C</td>
</tr>
<tr>
<td>E</td>
<td>4</td>
</tr>
<tr>
<td>F</td>
<td>6</td>
</tr>
</tbody>
</table>
### Example

Let $X^1 = 0000$ and $K^1 = 1234$ (in hexadecimal)

- Then $Y^1 = \sigma_{K^1}(X^1) = \sigma_{1234}(0000) = 1234$
- $Z^1 = \gamma(Y^1) = \gamma(1234) = D8A7$
- $X^2 = \theta(Z^1) = E939$
Example

Let $X^1 = 0000$ and $K^1 = 1234$ (in hexadecimal)

Then $Y^1 = \sigma_{K^1}(X^1) = \sigma_{1234}(0000) = 1234$

$Z^1 = \gamma(Y^1) = \gamma(1234) = \text{D8A7}$

$X^2 = \theta(Z^1) = \text{E939}$
Example

Let $X^1 = 0000$ and $K^1 = 1234$ (in hexadecimal)

Then $Y^1 = \sigma_{K^1}(X^1) = \sigma_{1234}(0000) = 1234$

$Z^1 = \gamma(Y^1) = \gamma(1234) = D8A7$

$X^2 = \theta(Z^1) = E939$
Example

Let \( X^1 = 0000 \) and \( K^1 = 1234 \) (in hexadecimal)

Then \( Y^1 = \sigma_{K^1}(X^1) = \sigma_{1234}(0000) = 1234 \)

\( Z^1 = \gamma(Y^1) = \gamma(1234) = D8A7 \)

\( X^2 = \theta(Z^1) = E939 \)
Overview of Block Ciphers

Basic Components of Block Ciphers

Full 4 Rounds of the Toy Cipher
Outline

1. Introduction
   - Objectives of this Presentation

2. Overview of Block Ciphers
   - Basic Components of Block Ciphers
   - Evaluating a Cipher

3. What is Cryptanalysis?
   - The Basics of Cryptanalysis
   - Example: Differential Cryptanalysis
   - Other Cryptanalysis Techniques
   - Breaking a Cipher
   - Why Cryptanalysis is Important?

4. Resources
In the selection for the AES, three major evaluation criteria were used by the National Institute of Standards and Technology (NIST) [Daemen and Rijmen, 2002]

1. **Security**: resistance to cryptanalysis
2. **Cost**: computational efficiency, program size, working memory, chip area
3. **Algorithm and Implementation Characteristics**: versatility, key agility, simplicity
In the selection for the AES, three major evaluation criteria were used by the National Institute of Standards and Technology (NIST) [Daemen and Rijmen, 2002]

1. Security: resistance to cryptanalysis
2. Cost: computational efficiency, program size, working memory, chip area
3. Algorithm and Implementation Characteristics: versatility, key agility, simplicity
Outline

1. Introduction
   - Objectives of this Presentation

2. Overview of Block Ciphers
   - Basic Components of Block Ciphers
   - Evaluating a Cipher

3. What is Cryptanalysis?
   - The Basics of Cryptanalysis
   - Example: Differential Cryptanalysis
   - Other Cryptanalysis Techniques
   - Breaking a Cipher
   - Why Cryptanalysis is Important?

4. Resources
What is Cryptanalysis?

The Basics of Cryptanalysis

What?

Cryptanalysis?
The study of breaking cryptosystems

Kerckhoffs’ Assumption

- The cipher’s algorithm used in the encryption is known
- The secret key is not known

Why not assume the cipher’s algorithm as a black box?

A cipher’s algorithm can possibly be reverse engineered
What is Cryptanalysis?

The Basics of Cryptanalysis

**What?**

Cryptanalysis?

The study of breaking cryptosystems

Kerckhoffs’ Assumption

- The **cipher’s algorithm** used in the encryption is **known**
- The **secret key** is **not known**

Why not assume the cipher’s algorithm as a black box?

A cipher’s algorithm can possibly be reverse engineered
What is Cryptanalysis?

The Basics of Cryptanalysis

What?

Cryptanalysis?

The study of breaking cryptosystems

Kerckhoffs’ Assumption

- The cipher’s algorithm used in the encryption is known
- The secret key is not known

Why not assume the cipher’s algorithm as a black box?

A cipher’s algorithm can possibly be reverse engineered
What is Cryptanalysis?

The Basics of Cryptanalysis

What?

Where to start? Nonlinear transformation. E.g. S-box

Then what? Expand the analysis done on the nonlinear transformation to the round function and further expand to as many rounds as possible

Muhammad Reza Z’aba (MIMOS)
What is Cryptanalysis?
The Basics of Cryptanalysis

What?

Where to start? Nonlinear transformation. E.g. S-box

Then what? Expand the analysis done on the nonlinear transformation to the round function and further expand to as many rounds as possible
What is Cryptanalysis?

The Basics of Cryptanalysis

What?

Where to start? Nonlinear transformation. E.g. S-box

Then what? Expand the analysis done on the nonlinear transformation to the round function and further expand to as many rounds as possible
What is Cryptanalysis?

The Basics of Cryptanalysis

What?

Where to start? **Nonlinear transformation. E.g. S-box**

Then what? Expand the analysis done on the nonlinear transformation to the round function and further expand to as many rounds as possible.
What is Cryptanalysis?
The Basics of Cryptanalysis

What?

Where to start? **Nonlinear transformation. E.g. S-box**

Then what? Expand the analysis done on the nonlinear transformation to the round function and further expand to as many rounds as possible.
What is Cryptanalysis?

The Basics of Cryptanalysis

Threat Model

Attack Scenarios

- Ciphertext-only
- Known-plaintext
- Chosen-plaintext
- Chosen-ciphertext
- Adaptive chosen-plaintext
- Adaptive chosen-ciphertext
- Related-key

Illustration

\[ P \rightarrow E \rightarrow C \]

\[ K \]
What is Cryptanalysis?

The Basics of Cryptanalysis

Threat Model

Attack Scenarios

- Ciphertext-only
- Known-plaintext
- Chosen-plaintext
- Chosen-ciphertext
- Adaptive chosen-plaintext
- Adaptive chosen-ciphertext
- Related-key

Illustration

\[ K \]

\[ P \rightarrow E \rightarrow C \]
What is Cryptanalysis?

The Basics of Cryptanalysis

Threat Model

Attack Scenarios
- Ciphertext-only
- Known-plaintext
- **Chosen-plaintext**
- Chosen-ciphertext
- Adaptive chosen-plaintext
- Adaptive chosen-ciphertext
- Related-key

Illustration

\[ P \rightarrow E \rightarrow C \]

\[ K \]
What is Cryptanalysis?
The Basics of Cryptanalysis

Threat Model

Attack Scenarios
- Ciphertext-only
- Known-plaintext
- Chosen-plaintext
- **Chosen-ciphertext**
- Adaptive chosen-plaintext
- Adaptive chosen-ciphertext
- Related-key

Illustration

\[ P \rightarrow E \rightarrow C \]

\( K \)
What is Cryptanalysis?
The Basics of Cryptanalysis

**Threat Model**

**Attack Scenarios**
- Ciphertext-only
- Known-plaintext
- Chosen-plaintext
- Chosen-ciphertext
- **Adaptive chosen-plaintext**
- Adaptive chosen-ciphertext
- Related-key

---

**Illustration**

\[ K \]

\[ E \]

\[ P_1 \rightarrow P_2 \]

\[ C_1 \rightarrow C_2 \]
What is Cryptanalysis?

The Basics of Cryptanalysis

Threat Model

Attack Scenarios
- Ciphertext-only
- Known-plaintext
- Chosen-plaintext
- Chosen-ciphertext
- Adaptive chosen-plaintext
- Adaptive chosen-ciphertext
- Related-key

Illustration

\[
\begin{align*}
E &: P_1 \to C_1 \\
P_2 &: E \to C_2
\end{align*}
\]
What is Cryptanalysis?

The Basics of Cryptanalysis

Threat Model

Attack Scenarios

- Ciphertext-only
- Known-plaintext
- Chosen-plaintext
- Chosen-ciphertext
- Adaptive chosen-plaintext
- Adaptive chosen-ciphertext
- Related-key

Illustration

\[ K_1, K_2 = K_1 \oplus \Delta K \]

\[ P \xrightarrow{E} C \]
What is Cryptanalysis?

The Basics of Cryptanalysis

Threat Model: Example

- **Cipher**: Simple Substitution
- **Plaintext, ciphertext and key space**: \{A, B, \ldots, Z\} = \{0, 1, \ldots, 25\}
- **Encryption**: \( C_i = P_i + K \mod 26 \)
- **Decryption**: \( P_i = C_i - K \mod 26 \)

<table>
<thead>
<tr>
<th></th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
<th>G</th>
<th>H</th>
<th>I</th>
<th>J</th>
<th>K</th>
<th>L</th>
<th>M</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>10</td>
<td>11</td>
<td>12</td>
<td></td>
</tr>
<tr>
<td></td>
<td>N</td>
<td>O</td>
<td>P</td>
<td>Q</td>
<td>R</td>
<td>S</td>
<td>T</td>
<td>U</td>
<td>V</td>
<td>W</td>
<td>X</td>
<td>Y</td>
<td>Z</td>
</tr>
<tr>
<td>13</td>
<td>14</td>
<td>15</td>
<td>16</td>
<td>17</td>
<td>18</td>
<td>19</td>
<td>20</td>
<td>21</td>
<td>22</td>
<td>23</td>
<td>24</td>
<td>25</td>
<td></td>
</tr>
</tbody>
</table>
Threat Model: Example

- Cipher: Simple Substitution
- Plaintext, ciphertext and key space: \( \{A, B, \ldots, Z\} = \{0, 1, \ldots, 25\} \)
- Encryption: \( C_i = P_i + K \mod 26 \).
- Decryption: \( P_i = C_i - K \mod 26 \).

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
<th>G</th>
<th>H</th>
<th>I</th>
<th>J</th>
<th>K</th>
<th>L</th>
<th>M</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>10</td>
<td>11</td>
<td>12</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>N</th>
<th>O</th>
<th>P</th>
<th>Q</th>
<th>R</th>
<th>S</th>
<th>T</th>
<th>U</th>
<th>V</th>
<th>W</th>
<th>X</th>
<th>Y</th>
<th>Z</th>
</tr>
</thead>
<tbody>
<tr>
<td>13</td>
<td>14</td>
<td>15</td>
<td>16</td>
<td>17</td>
<td>18</td>
<td>19</td>
<td>20</td>
<td>21</td>
<td>22</td>
<td>23</td>
<td>24</td>
<td>25</td>
</tr>
</tbody>
</table>
### Ciphertext-Only

<table>
<thead>
<tr>
<th>Plaintext</th>
<th>Ciphertext</th>
</tr>
</thead>
<tbody>
<tr>
<td>SFAB UJQV</td>
<td>18, 5, 0, 1, , 20, 9, 16, 21</td>
</tr>
<tr>
<td>DSZQUP</td>
<td>3, 18, 25, 16, 20, 15</td>
</tr>
</tbody>
</table>

What is the key? |
## Threat Model: Example

### Ciphertext-Only

<table>
<thead>
<tr>
<th>Plaintext</th>
<th>Ciphertext</th>
</tr>
</thead>
<tbody>
<tr>
<td>-</td>
<td>SFAB UJQV  $= 18, 5, 0, 1, 20, 9, 16, 21$</td>
</tr>
<tr>
<td>-</td>
<td>DSZQUP    $= 3, 18, 25, 16, 20, 15$</td>
</tr>
</tbody>
</table>

What is the key? $B = 1$
**What is Cryptanalysis?**
The Basics of Cryptanalysis

**Threat Model: Example**

### Ciphertext-Only

<table>
<thead>
<tr>
<th>Plaintext</th>
<th>Ciphertext</th>
</tr>
</thead>
<tbody>
<tr>
<td>SFAB UJQV</td>
<td>18, 5, 0, 1, , 20, 9, 16, 21</td>
</tr>
<tr>
<td>DSZQUP</td>
<td>3, 18, 25, 16, 20, 15</td>
</tr>
</tbody>
</table>

What is the key? \( B = 1 \)

\[
18 - 1 \mod 26 = 17 = R
\]
### Threat Model: Example

#### Ciphertext-Only

<table>
<thead>
<tr>
<th>Plaintext</th>
<th>Ciphertext</th>
</tr>
</thead>
<tbody>
<tr>
<td>SFAB UJQV</td>
<td>$18, 5, 0, 1, 20, 9, 16, 21$</td>
</tr>
<tr>
<td>DSZQUP</td>
<td>$3, 18, 25, 16, 20, 15$</td>
</tr>
</tbody>
</table>

**What is the key?** $B = 1$

$18 - 1 \mod 26 = 17 = R$

Decrypt(SFAB UJQV) = |
What is Cryptanalysis?

The Basics of Cryptanalysis

Threat Model: Example

**Ciphertext-Only**

<table>
<thead>
<tr>
<th>Plaintext</th>
<th>Ciphertext</th>
</tr>
</thead>
<tbody>
<tr>
<td>SFAB UJQV</td>
<td>18, 5, 0, 1, 20, 9, 16, 21</td>
</tr>
<tr>
<td>DSZQUP</td>
<td>3, 18, 25, 16, 20, 15</td>
</tr>
</tbody>
</table>

What is the key?  

\[ B = 1 \]

\[ 18 - 1 \mod 26 = 17 = R \]

\[ \text{Decrypt(SFAB UJQV)} = \text{REZA TIPU} \]
What is Cryptanalysis?

The Basics of Cryptanalysis

Threat Model: Example

<table>
<thead>
<tr>
<th>Plaintext</th>
<th>Ciphertext</th>
</tr>
</thead>
<tbody>
<tr>
<td>SFAB UJQV</td>
<td>18, 5, 0, 1, , 20, 9, 16, 21</td>
</tr>
<tr>
<td>DSZQUP</td>
<td>3, 18, 25, 16, 20, 15</td>
</tr>
</tbody>
</table>

What is the key?  $B = 1$

$18 - 1 \mod 26 = 17 = R$

Decrypt(SFAB UJQV) = REZA TIPU

Decrypt(DSZQUP) = 
What is Cryptanalysis?

The Basics of Cryptanalysis

**Threat Model: Example**

**Ciphertext-Only**

<table>
<thead>
<tr>
<th>Plaintext</th>
<th>Ciphertext</th>
</tr>
</thead>
<tbody>
<tr>
<td>SFAB UJQV</td>
<td>18, 5, 0, 1, 20, 9, 16, 21</td>
</tr>
<tr>
<td>DSZQUP</td>
<td>3, 18, 25, 16, 20, 15</td>
</tr>
</tbody>
</table>

What is the key? \( B = 1 \)

\[ 18 - 1 \mod 26 = 17 = R \]

Decrypt(SFAB UJQV) = REZA TIPU

Decrypt(DSZQUP) = CRYPTO
What is Cryptanalysis?

The Basics of Cryptanalysis

**Threat Model: Example**

<table>
<thead>
<tr>
<th>Plaintext</th>
<th>Ciphertext</th>
</tr>
</thead>
<tbody>
<tr>
<td>SERANG</td>
<td>RDQZMF</td>
</tr>
<tr>
<td>LAPAR</td>
<td>KZOZQ</td>
</tr>
</tbody>
</table>

What is the key? |
**Threat Model: Example**

<table>
<thead>
<tr>
<th>Plaintext</th>
<th>Ciphertext</th>
</tr>
</thead>
<tbody>
<tr>
<td>SERANG</td>
<td>RDQZMF</td>
</tr>
<tr>
<td>LAPAR</td>
<td>KZOZQ</td>
</tr>
</tbody>
</table>

What is the key? $z = 25$
### Threat Model: Example

#### Known-Plaintext

<table>
<thead>
<tr>
<th>Plaintext</th>
<th>Ciphertext</th>
</tr>
</thead>
<tbody>
<tr>
<td>SERANG</td>
<td>RDQZMF</td>
</tr>
<tr>
<td>LAPAR</td>
<td>KZOZQ</td>
</tr>
</tbody>
</table>

What is the key? \( Z = 25 \)

\[
17 - 25 \mod 26 = -8 \mod 26 = 18 = S
\]
### Known-Plaintext

<table>
<thead>
<tr>
<th>Plaintext</th>
<th>Ciphertext</th>
</tr>
</thead>
<tbody>
<tr>
<td>SERANG</td>
<td>RDQZMF</td>
</tr>
<tr>
<td>LAPAR</td>
<td>KZOZQ</td>
</tr>
</tbody>
</table>

What is the key? $Z = 25$

$$17 - 25 \mod 26 = -8 \mod 26 = 18 = S$$

Decrypt(RDQZMF) = SERANG

Decrypt(KZOZQ) = LAPAR
## Threat Model: Example

### Chosen-Plaintext

<table>
<thead>
<tr>
<th>Plaintext</th>
<th>Ciphertext</th>
</tr>
</thead>
<tbody>
<tr>
<td>JOM PERANG</td>
<td>LQO RGTCPI</td>
</tr>
<tr>
<td>KONSPIRASI</td>
<td>MQPURKTCUK</td>
</tr>
</tbody>
</table>

What is the key?
**Threat Model: Example**

<table>
<thead>
<tr>
<th>Plaintext</th>
<th>Ciphertext</th>
</tr>
</thead>
<tbody>
<tr>
<td>JOM PERANG</td>
<td>LQO RGTCPI</td>
</tr>
<tr>
<td>KONSPIRASI</td>
<td>MQPURKTCUK</td>
</tr>
</tbody>
</table>

What is the key? |
<table>
<thead>
<tr>
<th>Plaintext</th>
<th>Ciphertext</th>
</tr>
</thead>
<tbody>
<tr>
<td>JOM PERANG</td>
<td>LQO RGTCPI</td>
</tr>
<tr>
<td>KONSPIRASI</td>
<td>MQPURKTCUK</td>
</tr>
</tbody>
</table>

What is the key?
What is Cryptanalysis?

The Basics of Cryptanalysis

Threat Model: Example

### Chosen-Plaintext

<table>
<thead>
<tr>
<th>Plaintext</th>
<th>Ciphertext</th>
</tr>
</thead>
<tbody>
<tr>
<td>JOM PERANG</td>
<td>LQO RGTCPI</td>
</tr>
<tr>
<td>KONSPIRASI</td>
<td>MQPURKTCUK</td>
</tr>
</tbody>
</table>

What is the key? \( C = 2 \)

\[
11 - 2 \mod 26 = 9 \mod 26 = 9 = J
\]

Decrypt(LQO RGTCPI) = JOM PERANG

Decrypt(MQPURKTCUK) = MQPURKTCUK
What is Cryptanalysis?

The Basics of Cryptanalysis

**Attack Parameters**

**Complexities**

- **Data**: Amount of plaintext/ciphertext
- **Time**: Number of operations
- **Memory**: Amount of space for storing information
- **Number of Rounds**: Number of cipher rounds penetrated by attack
What is Cryptanalysis?

The Basics of Cryptanalysis

**Two Phases of an Attack**

**Distinguisher**
- An algorithm that can distinguish the cipher from a random permutation

**Key Recovery Attack**
- Adding one or more rounds at the end or/and at the beginning of the distinguisher
- Utilizes the distinguisher to verify key bit guesses
- Actual key bit values are obtained once guesses have been verified
What is Cryptanalysis?
The Basics of Cryptanalysis

Two Phases of an Attack

Distinguisher
- An algorithm that can distinguish the cipher from a random permutation

Key Recovery Attack
- Adding one or more rounds at the end or/and at the beginning of the distinguisher
- Utilizes the distinguisher to verify key bit guesses
- Actual key bit values are obtained once guesses have been verified
What is Cryptanalysis?
The Basics of Cryptanalysis

List of Cryptanalytic Techniques

- Differential
- Linear
- Integral
- Truncated Differential
- Impossible Differential
- Boomerang
- Rectangle
- Related-key
- Slide
- Combined Attack
- Algebraic
List of Cryptanalytic Techniques

- Differential
  - Linear
  - Integral
  - Truncated Differential
  - Impossible Differential
  - Boomerang
  - Rectangle
  - Related-key
  - Slide
  - Combined Attack
  - Algebraic
Outline

1. Introduction
   - Objectives of this Presentation

2. Overview of Block Ciphers
   - Basic Components of Block Ciphers
   - Evaluating a Cipher

3. What is Cryptanalysis?
   - The Basics of Cryptanalysis
   - Example: Differential Cryptanalysis
   - Other Cryptanalysis Techniques
   - Breaking a Cipher
   - Why Cryptanalysis is Important?

4. Resources
What is Cryptanalysis?

Example: Differential Cryptanalysis
**Introduction**

- Introduced by Eli Biham and Adi Shamir in CRYPTO 1990
- A *chosen plaintext* attack
- Manipulate the existence of input difference that can produce a predetermined output difference (after a certain number of rounds) with high probability

**Two Phases of the Attack**

- Construct a differential characteristic (distinguisher)
- Launch a key recovery attack
What is Cryptanalysis?

Example: Differential Cryptanalysis

Introduction

- Introduced by Eli Biham and Adi Shamir in CRYPTO 1990
- A *chosen plaintext* attack
- Manipulate the existence of input difference that can produce a predetermined output difference (after a certain number of rounds) with high probability

Two Phases of the Attack

- Construct a differential characteristic (distinguisher)
- Launch a key recovery attack
What is Cryptanalysis?
Example: Differential Cryptanalysis

Where to start? **Nonlinear transformation. E.g. S-box**

Then what? Expand the analysis done on the nonlinear transformation to the round function and further expand to as many rounds as possible
What is Cryptanalysis?

Example: Differential Cryptanalysis

\[
X(1) \oplus L(X(1)) = X(2) \oplus L(X(2)) = \Delta \alpha
\]

\[
L(X(1) \oplus X(2)) = \Delta \beta
\]

\[
\operatorname{Prob}(\Delta \alpha \rightarrow \Delta \beta) = 1
\]
What is Cryptanalysis?

Example: Differential Cryptanalysis

\[ X^{(1)} \rightarrow L \rightarrow X^{(2)} \]

\[ \text{Prob}(\Delta \alpha \rightarrow L(\Delta \alpha) = \Delta \beta) = 1 \]
What is Cryptanalysis?

Example: Differential Cryptanalysis

\[ X^{(1)} \xrightarrow{L} L(X^{(1)}) \]
\[ X^{(2)} \xrightarrow{L} L(X^{(2)}) \]
What is Cryptanalysis?

Example: Differential Cryptanalysis

\[ X^{(1)} \oplus L(X^{(1)}) = X^{(1)} \oplus X^{(2)} = X^{(1)} \oplus X^{(2)} \]

\[ L(X^{(2)}) \]

Muhammad Reza Z’aba (MIMOS)
What is Cryptanalysis?
Example: Differential Cryptanalysis

\[ X^{(1)} \oplus L(X^{(1)}) = X^{(1)} \oplus X^{(2)} = X^{(1)} \oplus L(X^{(1)}) \oplus X^{(2)} = L(X^{(1)} \oplus X^{(2)}) \]

\[ \text{Prob}(\Delta \alpha \rightarrow L(\Delta \alpha) = \Delta \beta) = 1 \]
What is Cryptanalysis?
Example: Differential Cryptanalysis

\[ X^{(1)} \oplus L(X^{(1)}) = L(X^{(1)} \oplus X^{(2)}) = \Delta_\alpha \]

\[ X^{(2)} = X^{(1)} \oplus X^{(2)} = \Delta_\alpha \]

\[ L(X^{(1)}) \oplus L(X^{(2)}) = L(X^{(1)} \oplus X^{(2)}) = \Delta_\beta \]

\[
\text{Prob}(\Delta_\alpha \rightarrow \Delta_\beta) = 1
\]
What is Cryptanalysis?

Example: Differential Cryptanalysis

\[
X(1) \oplus L(X(1)) = X(1) \oplus X(2) = \Delta_\alpha
\]

\[
X(2) \oplus L(X(2)) = L(X(1) \oplus X(2)) = \Delta_\beta
\]
What is Cryptanalysis?

Example: Differential Cryptanalysis

\[
\begin{align*}
X^{(1)} & \oplus \quad L \quad \longrightarrow \\
L(X^{(1)}) & \oplus \\
L(X^{(1)}) & = \Delta_\alpha \\
\\
X^{(2)} & \oplus \quad L \\
L(X^{(2)}) & \oplus \\
L(X^{(2)}) & = L(X^{(1)} \oplus X^{(2)}) = \Delta_\beta \\
\\
\text{Prob}(\Delta_\alpha \xrightarrow{L} L(\Delta_\alpha) = \Delta_\beta) & = 1
\end{align*}
\]

Muhammad Reza Z’aba (MIMOS)
7 April 2011 31 / 64
What is Cryptanalysis?

Example: Differential Cryptanalysis

\[
\begin{align*}
X^{(1)} \oplus X^{(2)} &= \Delta_{\alpha} \\
S(X^{(1)}) \oplus S(X^{(2)}) &= \Delta_{\beta} \\
\text{Prob}(\Delta_{\alpha} \xrightarrow{S} \Delta_{\beta}) &= ?
\end{align*}
\]
What is Cryptanalysis?
Example: Differential Cryptanalysis

**Difference Distribution Table (DDT)**

A table that displays how many times a particular input difference to a $m \times n$ S-box causes a particular output difference to happen.

**Properties of the DDT**

- Contains $2^m \times 2^n$ entries
- Entries in each row add up to $2^m$
- $\Delta_\alpha \xrightarrow{S} \Delta_\beta$ - The event that the input difference $\Delta_\alpha$ causes the output difference $\Delta_\beta$ to happen
- Probability of $\Delta_\alpha \xrightarrow{S} \Delta_\beta$ is $p = \frac{DDT[\Delta_\alpha][\Delta_\beta]}{2^m}$
What is Cryptanalysis?
Example: Differential Cryptanalysis

**Difference Distribution Table (DDT)**

A table that displays how many times a particular input difference to a $m \times n$ S-box causes a particular output difference to happen.

**Properties of the DDT**

- Contains $2^m \times 2^n$ entries
- Entries in each row add up to $2^m$
- $\Delta_\alpha \xrightarrow{S} \Delta_\beta$ - The event that the input difference $\Delta_\alpha$ causes the output difference $\Delta_\beta$ to happen
- Probability of $\Delta_\alpha \xrightarrow{S} \Delta_\beta$ is $p = \frac{DDT[\Delta_\alpha][\Delta_\beta]}{2^m}$
What is Cryptanalysis?
Example: Differential Cryptanalysis

Algorithm to Calculate DDT

- For $\Delta_\alpha = 0$ to $2^m - 1$ do
  - For $x = 0$ to $2^m - 1$ do
    - $\Delta_\beta = S[x] \oplus S[x \oplus \Delta_\alpha]$
    - Increment $DDT[\Delta_\alpha][\Delta_\beta]$
  - end for
- end for

S-box

<table>
<thead>
<tr>
<th>$X$</th>
<th>$S'_i(X)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>F</td>
</tr>
<tr>
<td>1</td>
<td>D</td>
</tr>
<tr>
<td>2</td>
<td>8</td>
</tr>
<tr>
<td>3</td>
<td>A</td>
</tr>
<tr>
<td>4</td>
<td>7</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>6</td>
<td>1</td>
</tr>
<tr>
<td>7</td>
<td>3</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$X$</th>
<th>$S'_i(X)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>B</td>
</tr>
<tr>
<td>9</td>
<td>9</td>
</tr>
<tr>
<td>A</td>
<td>0</td>
</tr>
<tr>
<td>B</td>
<td>2</td>
</tr>
<tr>
<td>C</td>
<td>E</td>
</tr>
<tr>
<td>D</td>
<td>C</td>
</tr>
<tr>
<td>E</td>
<td>4</td>
</tr>
<tr>
<td>F</td>
<td>6</td>
</tr>
</tbody>
</table>
### What is Cryptanalysis?

**Example: Differential Cryptanalysis**

DDT calculation for the S-box of TC1 when $\Delta_\alpha = 1$

<table>
<thead>
<tr>
<th>X</th>
<th>$X \oplus \Delta_\alpha$</th>
<th>$S'_i(X)$</th>
<th>$S'<em>i(X \oplus \Delta</em>\alpha)$</th>
<th>$\Delta_\beta$</th>
<th>$DDT[\Delta_\alpha][\Delta_\beta]$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>F</td>
<td>D</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>D</td>
<td>F</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>8</td>
<td>A</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>A</td>
<td>8</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>4</td>
<td>5</td>
<td>7</td>
<td>5</td>
<td>2</td>
<td>5</td>
</tr>
<tr>
<td>5</td>
<td>4</td>
<td>5</td>
<td>7</td>
<td>2</td>
<td>6</td>
</tr>
<tr>
<td>6</td>
<td>7</td>
<td>3</td>
<td>1</td>
<td>2</td>
<td>7</td>
</tr>
<tr>
<td>7</td>
<td>6</td>
<td>3</td>
<td>1</td>
<td>2</td>
<td>8</td>
</tr>
<tr>
<td>8</td>
<td>9</td>
<td>B</td>
<td>9</td>
<td>2</td>
<td>9</td>
</tr>
<tr>
<td>9</td>
<td>8</td>
<td>9</td>
<td>B</td>
<td>2</td>
<td>10</td>
</tr>
<tr>
<td>A</td>
<td>B</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>11</td>
</tr>
<tr>
<td>B</td>
<td>A</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>12</td>
</tr>
<tr>
<td>C</td>
<td>D</td>
<td>E</td>
<td>C</td>
<td>2</td>
<td>13</td>
</tr>
<tr>
<td>D</td>
<td>C</td>
<td>C</td>
<td>E</td>
<td>2</td>
<td>14</td>
</tr>
<tr>
<td>E</td>
<td>F</td>
<td>4</td>
<td>6</td>
<td>2</td>
<td>15</td>
</tr>
<tr>
<td>F</td>
<td>E</td>
<td>6</td>
<td>4</td>
<td>2</td>
<td>16</td>
</tr>
</tbody>
</table>
# What is Cryptanalysis?

Example: Differential Cryptanalysis

<table>
<thead>
<tr>
<th>$\Delta \alpha$</th>
<th>$\Delta \beta$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>16</td>
</tr>
<tr>
<td>1</td>
<td>16</td>
</tr>
<tr>
<td>2</td>
<td>4 4 4 4</td>
</tr>
<tr>
<td>3</td>
<td>4 4 4 4</td>
</tr>
<tr>
<td>4</td>
<td>4 4 4 4</td>
</tr>
<tr>
<td>5</td>
<td>4 4 4 4</td>
</tr>
<tr>
<td>6</td>
<td>4 4 4 8</td>
</tr>
<tr>
<td>7</td>
<td>4 4 4 8</td>
</tr>
<tr>
<td>8</td>
<td>4 4 4 8</td>
</tr>
<tr>
<td>9</td>
<td>4 4 4 8</td>
</tr>
<tr>
<td>A</td>
<td>8 8 8 8</td>
</tr>
<tr>
<td>B</td>
<td>8 8 8 8</td>
</tr>
<tr>
<td>C</td>
<td>8 8 8 8</td>
</tr>
<tr>
<td>D</td>
<td>8 8 8 8</td>
</tr>
<tr>
<td>E</td>
<td>8 8 8 8</td>
</tr>
<tr>
<td>F</td>
<td>8 8 8 8</td>
</tr>
</tbody>
</table>

Examples

- $\text{Prob}(0 \xrightarrow{S} 0) = \frac{16}{16}$
- $\text{Prob}(1 \xrightarrow{S} 2) = \frac{16}{16}$
- $\text{Prob}(2 \xrightarrow{S} 6) = \frac{4}{16}$

Muhammad Reza Z’aba (MIMOS)
What is Cryptanalysis?
Example: Differential Cryptanalysis

What is the use of the DDT?
Help in building differential characteristics (distinguishers)
What is the use of the DDT?
Help in building differential characteristics (distinguishers)
**n-round Differential Characteristic**

A set of input and output differences that approximates \( n \) rounds of a cipher

- \( \text{Prob}(\Delta I_1 \xrightarrow{F} \Delta O_1) = p_1, \)
- \( \text{Prob}(\Delta I_2 \xrightarrow{F} \Delta O_2) = p_2, \)
- \( \ldots \)
- \( \text{Prob}(\Delta I_n \xrightarrow{F} \Delta O_n) = p_n \)

**Total probability**

\[ p = \prod_{i}^{n} p_i = \prod_{i}^{m} \hat{p}_i \]

---

**m Active S-boxes**

Involves \( m \) active S-boxes

- \( \text{Prob}(\Delta_{\alpha_1} \xrightarrow{S_i^r} \Delta_{\beta_1}) = \hat{p}_1, \)
- \( \text{Prob}(\Delta_{\alpha_2} \xrightarrow{S_i^r} \Delta_{\beta_2}) = \hat{p}_2, \)
- \( \ldots \)
- \( \text{Prob}(\Delta_{\alpha_m} \xrightarrow{S_i^r} \Delta_{\beta_m}) = \hat{p}_m \)

**Active S-box**

S-box involved in characteristic which has non-zero input difference (and hence, non-zero output difference)
**$n$-round Differential Characteristic**

A set of input and output differences that approximates $n$ rounds of a cipher

- $\text{Prob}(\Delta_{I_1} \xrightarrow{F} \Delta_{O_1}) = p_1$,
- $\text{Prob}(\Delta_{I_2} \xrightarrow{F} \Delta_{O_2}) = p_2$,
- \ldots
- $\text{Prob}(\Delta_{I_n} \xrightarrow{F} \Delta_{O_n}) = p_n$

**$m$ Active S-boxes**

Involves $m$ active S-boxes

- \(\text{Prob}(\Delta_{\alpha_1} \xrightarrow{s_i^r} \Delta_{\beta_1}) = \hat{p}_1,\)
- \(\text{Prob}(\Delta_{\alpha_2} \xrightarrow{s_i^r} \Delta_{\beta_2}) = \hat{p}_2,\)
- \ldots
- \(\text{Prob}(\Delta_{\alpha_m} \xrightarrow{s_i^r} \Delta_{\beta_m}) = \hat{p}_m\)

**Active S-box**

S-box involved in characteristic which has non-zero input difference (and hence, non-zero output difference)

\[
p = \prod_{i}^{n} p_i = \prod_{i}^{m} \hat{p}_i
\]
**n-round Differential Characteristic**

A set of input and output differences that approximates $n$ rounds of a cipher

- $\text{Prob}(\Delta I_1 \xrightarrow{F} \Delta O_1) = p_1$
- $\text{Prob}(\Delta I_2 \xrightarrow{F} \Delta O_2) = p_2$
- ...
- $\text{Prob}(\Delta I_n \xrightarrow{F} \Delta O_n) = p_n$

**Active S-box**

S-box involved in characteristic which has non-zero input difference (and hence, non-zero output difference)

**$m$ Active S-boxes**

Involves $m$ active S-boxes

- $\text{Prob}(\Delta_\alpha \xrightarrow{s_i^r} \Delta_\beta) = \hat{p}_1$
- $\text{Prob}(\Delta_\alpha \xrightarrow{s_i^r} \Delta_\beta) = \hat{p}_2$
- ...
- $\text{Prob}(\Delta_\alpha \xrightarrow{s_i^r} \Delta_\beta) = \hat{p}_m$

Total probability

$p = \prod^n_i p_i = \prod^m_i \hat{p}_i$
What is Cryptanalysis?

Example: Differential Cryptanalysis

**n-round Differential Characteristic**

A set of input and output differences that approximates \( n \) rounds of a cipher

- \( \text{Prob}(\Delta l_1 \xrightarrow{F} \Delta o_1) = p_1 \),
- \( \text{Prob}(\Delta l_2 \xrightarrow{F} \Delta o_2) = p_2 \),
- \( \ldots \)
- \( \text{Prob}(\Delta l_n \xrightarrow{F} \Delta o_n) = p_n \)

**Total probability**

\[ p = \prod_{i}^{n} p_i = \prod_{i}^{m} \hat{p}_i \]

**m Active S-boxes**

Involves \( m \) active S-boxes

- \( \text{Prob}(\Delta_{\alpha_1} \xrightarrow{s_{i_r}} \Delta_{\beta_1}) = \hat{p}_1 \),
- \( \text{Prob}(\Delta_{\alpha_2} \xrightarrow{s_{i_r}} \Delta_{\beta_2}) = \hat{p}_2 \),
- \( \ldots \)
- \( \text{Prob}(\Delta_{\alpha_m} \xrightarrow{s_{i_r}} \Delta_{\beta_m}) = \hat{p}_m \)

**Active S-box**

S-box involved in characteristic which has non-zero input difference (and hence, non-zero output difference)
What is Cryptanalysis?
Example: Differential Cryptanalysis

Forming a $n$-round Differential Characteristic
Concatenating $n$ 1-round differential characteristics

Round 1

Remarks

- $\text{Prob}(1 \xrightarrow{S_4^1} 2) = \hat{p}_1 = \frac{16}{16} = 1$
- $\text{Prob}(0001 \xrightarrow{F} 0010) = p_1 = \frac{16}{16} = 1$
What is Cryptanalysis?
Example: Differential Cryptanalysis

Forming a *n*-round Differential Characteristic

Concatenating *n* 1-round differential characteristics

Round 1

Remarks

- \( \text{Prob}(1 \xrightarrow{S_4} 2) = \hat{p}_1 = \frac{16}{16} = 1 \)
- \( \text{Prob}(0001 \xrightarrow{F} 0010) = \rho_1 = \frac{16}{16} = 1 \)
What is Cryptanalysis?
Example: Differential Cryptanalysis

Round 2

Remarks
- \( \text{Prob}(1 \xrightarrow{S_3^2} 2) = \hat{p}_2 = 16/16 = 1 \)
- \( \text{Prob}(0010 \xrightarrow{F} 0020) = p_2 = 16/16 = 1 \)

Round 3

Remarks
- \( \text{Prob}(2 \xrightarrow{S_3^3} 6) = \hat{p}_3 = 4/16 = 0.25 \)
- \( \text{Prob}(0020 \xrightarrow{F} 0220) = p_3 = 4/16 = 0.25 \)
What is Cryptanalysis?
Example: Differential Cryptanalysis

Round 2

Remarks

\[
\text{Prob}(1 \xrightarrow{S_3^2} 2) = \hat{p}_2 = \frac{16}{16} = 1
\]

\[
\text{Prob}(0010 \xrightarrow{F} 0020) = p_2 = \frac{16}{16} = 1
\]

Round 3

Remarks

\[
\text{Prob}(2 \xrightarrow{S_3^3} 6) = \hat{p}_3 = \frac{4}{16} = 0.25
\]

\[
\text{Prob}(0020 \xrightarrow{F} 0220) = p_3 = \frac{4}{16} = 0.25
\]
What is Cryptanalysis?
Example: Differential Cryptanalysis

Round 2

\[ \begin{array}{c}
S^2_1 & S^2_2 & S^2_3 & S^2_4 \\
\end{array} \]

Remarks
- \( \text{Prob}(1 \xrightarrow{S^2_3} 2) = \hat{p}_2 = 16/16 = 1 \)
- \( \text{Prob}(0010 \xrightarrow{F} 0020) = \rho_2 = 16/16 = 1 \)

Round 3

\[ \begin{array}{c}
S^3_1 & S^3_2 & S^3_3 & S^3_4 \\
\end{array} \]

Remarks
- \( \text{Prob}(2 \xrightarrow{S^3_3} 6) = \hat{p}_3 = 4/16 = 0.25 \)
- \( \text{Prob}(0020 \xrightarrow{F} 0220) = \rho_3 = 4/16 = 0.25 \)
What is Cryptanalysis?
Example: Differential Cryptanalysis

3-round Diff Characteristic

Analysis
- Active S-boxes = 3
- Characteristics:
  - Prob(0001 \xrightarrow{F} 0010) = p_1 = 1
  - Prob(0010 \xrightarrow{F} 0020) = p_2 = 1
  - Prob(0020 \xrightarrow{F} 0220) = p_3 = 0.25
- Total probability, $p = 1 \times 1 \times 0.25 = 0.25$
What is Cryptanalysis?
Example: Differential Cryptanalysis

- Total probability, $p = 0.25 > 1/2^{16} = 2^{-16}$
- Therefore, the above 3-round differential characteristic is a distinguisher
What is Cryptanalysis?
Example: Differential Cryptanalysis

- Total probability, $p = 0.25 > 1/2^{16} = 2^{-16}$
- Therefore, the above 3-round differential characteristic is a distinguisher
What is Cryptanalysis?

Example: Differential Cryptanalysis

- Total probability, $p = 0.25 > 1/2^{16} = 2^{-16}$
- Therefore, the above 3-round differential characteristic is a distinguisher
Key Recovery Attack

Remarks

- Initialize $2^{4+4} = 256$ counters
- For every ciphertext pair
  - Guess 8 bits of round subkey in the last round
  - If difference of decrypted nibbles matches predicted difference, increment counter
- The round subkey with the highest count is the correct subkey
What is Cryptanalysis?
Example: Differential Cryptanalysis

Attack Complexities
- 4-round key recovery attack
  - First 3 rounds – distinguisher
  - Additional 1 round – key recovery
- Data complexity, $N = c/p$ chosen plaintexts, $c=$small constant
- Time complexity, $N \times 2^8$ partial decryptions
- Memory complexity - store counters
What is Cryptanalysis?
Example: Differential Cryptanalysis

Other attacks based on differential cryptanalysis:
- Integral
- Truncated Differential
- Impossible Differential
- Boomerang
- Rectangle
- Related-key Differential
- Slide
Outline

1. Introduction
   - Objectives of this Presentation

2. Overview of Block Ciphers
   - Basic Components of Block Ciphers
   - Evaluating a Cipher

3. What is Cryptanalysis?
   - The Basics of Cryptanalysis
   - Example: Differential Cryptanalysis
   - Other Cryptanalysis Techniques
   - Breaking a Cipher
   - Why Cryptanalysis is Important?

4. Resources
In general, there exists attacks based on:

- **differential** cryptanalysis
- **linear** cryptanalysis
- **algebraic** cryptanalysis
- a combination of the above
- **implementation** aspects (e.g. side-channel, timing)
What is Cryptanalysis?

Breaking a Cipher

Outline

1. Introduction
   - Objectives of this Presentation

2. Overview of Block Ciphers
   - Basic Components of Block Ciphers
   - Evaluating a Cipher

3. What is Cryptanalysis?
   - The Basics of Cryptanalysis
   - Example: Differential Cryptanalysis
   - Other Cryptanalysis Techniques
   - Breaking a Cipher
   - Why Cryptanalysis is Important?

4. Resources
What is meant by 'a cipher is broken'?

- The cipher can be cryptanalyzed/attacked with complexity less than exhaustive key search.
- Attack is considered *theoretical* if amount of data, time and/or memory is *unfeasible* to obtain/run using currently available technology.
- Attack is considered *practical* if amount of data, time and/or memory is *feasible* to obtain/run using currently available technology.

**Example**

- Block cipher key size = 128 bits
- Time complexity of attack = $2^{110}$
- If processor capable of performing $10^{12}$ (one trillion) calculations per second, then cryptanalysis will complete after $4.1163 \times 10^{13}$ years!
What is meant by ’a cipher is broken’?

- The cipher can be cryptanalyzed/attacked with **complexity** less than exhaustive key search
- Attack is considered **theoretical** if amount of data, time and/or memory is **unfeasible** to obtain/run using currently available technology
- Attack is considered **practical** if amount of data, time and/or memory is **feasible** to obtain/run using currently available technology

**Example**

- Block cipher key size = 128 bits
- Time complexity of attack = $2^{110}$
- If processor capable of performing $10^{12}$ (one trillion) calculations per second, then cryptanalysis will complete after $4.1163 \times 10^{13}$ years!
What is meant by 'a cipher is broken’? 

- The cipher can be cryptanalyzed/attacked with complexity less than exhaustive key search.
- Attack is considered *theoretical* if amount of data, time and/or memory is *unfeasible* to obtain/run using currently available technology.
- Attack is considered *practical* if amount of data, time and/or memory is *feasible* to obtain/run using currently available technology.

**Example**

- Block cipher key size = 128 bits
- Time complexity of attack = $2^{110}$
- If processor capable of performing $10^{12}$ (one trillion) calculations per second, then cryptanalysis will complete after $4.1163 \times 10^{13}$ years!
What is meant by ’a cipher is broken’?

- The cipher can be cryptanalyzed/attacked with **complexity** less than exhaustive key search
- Attack is considered **theoretical** if amount of data, time and/or memory is **unfeasible** to obtain/run using currently available technology
- Attack is considered **practical** if amount of data, time and/or memory is **feasible** to obtain/run using currently available technology

**Example**

- Block cipher key size = 128 bits
- Time complexity of attack = $2^{110}$
- If processor capable of performing $10^{12}$ (one trillion) calculations per second, then cryptanalysis will complete after $4.1163 \times 10^{13}$ years!
What is Cryptanalysis?

Breaking a Cipher
What is Cryptanalysis?
Breaking a Cipher

Other meanings of 'break'
Cryptanalysis on reduced-round versions of a cipher (often publishable result). Example: Cryptanalysis on 8 out of 10 full rounds of the Advanced Encryption Standard (AES)

Note
There exist attacks on full round version of block ciphers
What is Cryptanalysis?
Breaking a Cipher

Other meanings of 'break'

Cryptanalysis on reduced-round versions of a cipher (often publishable result). Example: Cryptanalysis on 8 out of 10 full rounds of the Advanced Encryption Standard (AES)

Note
There exist attacks on full round version of block ciphers
What is Cryptanalysis?
Breaking a Cipher

Other meanings of 'break'
Cryptanalysis on reduced-round versions of a cipher (often publishable result). Example: Cryptanalysis on 8 out of 10 full rounds of the Advanced Encryption Standard (AES)

Note
There exist attacks on full round version of block ciphers
Outline

1. Introduction
   - Objectives of this Presentation

2. Overview of Block Ciphers
   - Basic Components of Block Ciphers
   - Evaluating a Cipher

3. What is Cryptanalysis?
   - The Basics of Cryptanalysis
   - Example: Differential Cryptanalysis
   - Other Cryptanalysis Techniques
   - Breaking a Cipher
   - Why Cryptanalysis is Important?

4. Resources
What is Cryptanalysis?

Why Cryptanalysis is Important?

Why? Cryptanalysis results represent the security analysis of the cipher. The absence of such results in a cipher proposal will cast some doubts on the security of the cipher.
What is Cryptanalysis?

Why Cryptanalysis is Important?

Why?

Cryptanalysis results represent the security analysis of the cipher

The absence of such results in a cipher proposal will cast some doubts on the security of the cipher.
Why? Cryptanalysis results represent the security analysis of the cipher.
The absence of such results in a cipher proposal will cast some doubts on the security of the cipher.
[Schneier, 2000]

- Designing a cryptographic algorithm is easy but analysis is hard
- Extensive analyses of an algorithm – simplified variants, reduced-round versions and alternate implementations – show the designer knew what he was doing when he created the algorithm
- The Twofish [Schneier et al., 1999] designers spent 1000 man-hours on cryptanalysis and wrote a book consisting primarily on cryptanalysis
- Third-party cryptanalysis should start after this level of analysis
What is Cryptanalysis?
Why Cryptanalysis is Important?

[Schneier, 2000]
- Designing a cryptographic algorithm is easy but analysis is hard
- Extensive analyses of an algorithm – simplified variants, reduced-round versions and alternate implementations – show the designer knew what he was doing when he created the algorithm
- The Twofish [Schneier et al., 1999] designers spent 1000 man-hours on cryptanalysis and wrote a book consisting primarily on cryptanalysis
- Third-party cryptanalysis should start after this level of analysis
What is Cryptanalysis?

Why Cryptanalysis is Important?

[Schneier, 2000]

- Designing a cryptographic algorithm is easy but analysis is hard
- Extensive analyses of an algorithm – simplified variants, reduced-round versions and alternate implementations – show the designer knew what he was doing when he created the algorithm
- The Twofish [Schneier et al., 1999] designers spent 1000 man-hours on cryptanalysis and wrote a book consisting primarily on cryptanalysis
- Third-party cryptanalysis should start after this level of analysis
What is Cryptanalysis?
Why Cryptanalysis is Important?

[Schneier, 2000]

- Designing a cryptographic algorithm is easy but analysis is hard.
- Extensive analyses of an algorithm – simplified variants, reduced-round versions and alternate implementations – show the designer knew what he was doing when he created the algorithm.
- The Twofish [Schneier et al., 1999] designers spent 1000 man-hours on cryptanalysis and wrote a book consisting primarily on cryptanalysis.
- Third-party cryptanalysis should start after this level of analysis.
**What is Cryptanalysis?**

**Why Cryptanalysis is Important?**

---

Cryptanalysis is one of the core technical disciplines necessary for the National Security Agency (NSA) to accomplish its mission and provide critical intelligence to the nation’s leaders, and the need for Cryptanalysts will remain constant in our ever-changing global environment.

Source: National Security Agency

Job Description of Cryptanalyst (Job ID 11428)

[National Security Agency, 2010]
What is Cryptanalysis?

Why Cryptanalysis is Important?

Ensuring the security remains current

- In Eurocrypt 2008 KeeLoq – 528-round block cipher used in car keys – broken in less than a day [Indesteege et al., 2008]
- Related-Key attacks on the full AES-192 and AES-256 [Biryukov and Khovratovich, 2009, Biryukov et al., 2009]
- Related-Key attacks of practical complexity on reduced-round AES-256 [Biryukov et al., 2010]
Summary

1. Basic components of a block cipher (linear, nonlinear components)
2. Basics of cryptanalysis (Kerckhoffs’, threat model, attack complexities, phases of an attack)
3. Definitions of ‘break’
4. Importance of cryptanalysis
What is Cryptanalysis?

Why Cryptanalysis is Important?

Summary

1. Basic components of a block cipher (linear, nonlinear components)
2. Basics of cryptanalysis (Kerckhoffs’, threat model, attack complexities, phases of an attack)
3. Definitions of ‘break’
4. Importance of cryptanalysis
Summary

1. Basic components of a block cipher (linear, nonlinear components)
2. Basics of cryptanalysis (Kerckhoffs’, threat model, attack complexities, phases of an attack)
3. Definitions of ‘break’
4. Importance of cryptanalysis
What is Cryptanalysis?

Why Cryptanalysis is Important?

Summary

1. Basic components of a block cipher (linear, nonlinear components)
2. Basics of cryptanalysis (Kerckhoffs’, threat model, attack complexities, phases of an attack)
3. Definitions of ‘break’
4. Importance of cryptanalysis
Associations

International Association for Cryptologic Research (IACR)

- [http://www.iacr.org](http://www.iacr.org)
- IACR-sponsored conferences
- Calendar of events in cryptology
- Open positions in cryptology
Associations

Malaysian Society for Cryptology Research (MSCR)

- http://www.mscr.org.my
- Activities
- International Journal of Cryptology Research
Major Conferences and Journals

Top Crypto Conferences

- CRYPTO
- EUROCRYPT
- ASIACRYPT
- Fast Software Encryption (FSE)
- Workshop on Cryptographic Hardware and Embedded Systems (CHES)
- Cryptographers’ Track at RSA Conference (CT-RSA)

All published by Springer-Verlag
Let’s publish in these conferences :) !
Major Conferences and Journals

Top Crypto Conferences

- CRYPTO
- EUROCRYPT
- ASIACRYPT
- Fast Software Encryption (FSE)
- Workshop on Cryptographic Hardware and Embedded Systems (CHES)
- Cryptographers’ Track at RSA Conference (CT-RSA)

All published by Springer-Verlag
Let’s publish in these conferences :)!
Resources

Major Conferences and Journals

Other Regular Conferences

- Public Key Cryptography (PKC)
- Theory of Cryptography Conference (TCC)
- Selected Areas in Cryptography (SAC)
- Australasian Conference on Information Security and Privacy (ACISP)
- International Conference on Cryptology in India (Indocrypt)
- International Conference on Information Security and Cryptology (ICISC)
- International Conference on Applied Cryptography and Network Security (ACNS)
- China International Conference on Information Security and Cryptology (Inscrypt)
- Africacrypt
Major Journals

- Journal of Cryptology (Springer)
- Cryptologia (Taylor & Francis)
- Journal of Mathematical Cryptology (De Gruyter)
- IEEE Transactions on Information Theory (IEEE)
- International Journal of Information Security (Springer)
- Information Processing Letters (Elsevier)
- SIAM Journal on Computing (SIAM)
Recommended Reading for Beginners

Differential and Linear Cryptanalysis


Integral Cryptanalysis

THANK YOU
v7.0.0. Available at http://www.3gpp.org/.

Key Recovery Attacks of Practical Complexity on AES-256 Variants with up to 10 Rounds.

Related-key Cryptanalysis of the Full AES-192 and AES-256.

Distinguisher and Related-Key Attack on the Full AES-256.

CNSS Policy No. 15, Fact Sheet No. 1 National Policy on the use of the Advanced Encryption Standard (AES) to Protect National Security Systems and National Security Information.
Committee on National Security Systems.
Available at http://www.cnss.gov/policies.html.

Algebraic and Slide Attacks on KeeLoq.
Springer-Verlag.

SMS4 Encryption Algorithm for Wireless Networks.

RSA Code-Breaking Contest Again Won by Distributed.Net and Electronic Frontier Foundation (EFF): DES Challenge III Broken in Record 22 Hours.
Press Release.
Available at [http://www.eff.org/Privacy/Crypto/Crypto_misc/DESCracker/HTML/19990119_deschallenge3.html](http://www.eff.org/Privacy/Crypto/Crypto_misc/DESCracker/HTML/19990119_deschallenge3.html).

A Practical Attack on KeeLoq.
Springer-Verlag.

RSA's DES Challenge III is solved in record time.

Markov Ciphers and Differential Cryptanalysis.
Springer-Verlag.
National Security Agency (2010).
Careers in Cryptanalysis and Signal Analysis at National Security Agency (NSA).

Available at http://nsri.etri.re.kr/.

Office of State Commercial Cryptography Administration, P.R. China (2006).
The SMS4 Block Cipher (in Chinese).

A Self-Study Course in Block Cipher Cryptanalysis.
Cryptologia, 24(1):18–33.

The Twofish Encryption Algorithm.
John Wiley & Sons.

The 128-bit Blockcipher CLEFIA.