Liljana Babinkostova

Department of Mathematics, Boise State University

Spring 2012
A cryptosystem is an ordered 4-tuple \((\mathcal{M}, \mathcal{C}, \mathcal{K}, T)\) where \(\mathcal{M}\), \(\mathcal{C}\), and \(\mathcal{K}\) are called the message space, the ciphertext space, and the key space and where \(T : \mathcal{M} \times \mathcal{K} \rightarrow \mathcal{C}\) is a transformation such that for each \(k \in \mathcal{K}\), the mapping \(T_k : \mathcal{M} \rightarrow \mathcal{C}\) is invertible.
A cryptosystem is an ordered 4-tuple \((M, C, K, T)\) where \(M\), \(C\), and \(K\) are called the message space, the ciphertext space, and the key space and where \(T : M \times K \rightarrow C\) is a transformation such that for each \(k \in K\), the mapping \(T_k : M \rightarrow C\) is invertible.

**Definition**
Let \((G, \oplus)\) be a finite group. For a function \(f : G^t \rightarrow G^t\) the function \(\sigma_f : G^{2t} \rightarrow G^{2t}\) defined by \(\sigma_f(x, y) = (x \oplus f(y), y)\) is called a *Feistel round function*. 
A cryptosystem is an ordered 4-tuple \((\mathcal{M}, \mathcal{C}, \mathcal{K}, T)\) where \(\mathcal{M}\), \(\mathcal{C}\), and \(\mathcal{K}\) are called the message space, the ciphertext space, and the key space and where \(T : \mathcal{M} \times \mathcal{K} \rightarrow \mathcal{C}\) is a transformation such that for each \(k \in \mathcal{K}\), the mapping \(T_k : \mathcal{M} \rightarrow \mathcal{C}\) is invertible.

**Definition**

Let \((G, \oplus)\) be a finite group. For a function \(f : G^t \rightarrow G^t\) the function \(\sigma_f : G^{2^t} \rightarrow G^{2^t}\) defined by \(\sigma_f(x, y) = (x \oplus f(y), y)\) is called a *Feistel round function*.
The n-round DES encryption algorithm can be described as a product of permutations: 

\[ T_k = P^{-1} \circ \Theta \circ (\Theta \circ \sigma_{k_n}) \circ \cdots \circ (\Theta \circ \sigma_{k_1}) \circ P \]

where \( k \) is the cipher key, \( P \) is the initial (fixed) permutation, and \( k_1, k_2, \cdots, k_n \) are round subkeys derived from the cipher key \( k \).

For all \( 1 \leq i \leq n \), the \( i \)th round consists of the permutation \( \Theta \circ \sigma_{k_i} \) where \( \sigma_{k_i} : M \rightarrow M \) is the Feistel round function and \( \Theta : M \rightarrow M \) is the "swap function" defined for \( x, y \in G \) as \( \Theta(x, y) = (y, x) \).
The \( n \)-round DES encryption algorithm can be described as a product of permutations

\[
T_k = P^{-1} \circ \Theta \circ (\Theta \circ \sigma_{k_n}) \circ \cdots \circ (\Theta \circ \sigma_{k_1}) \circ P
\]

where \( k \) is the cipher key, \( P \) is the initial (fixed) permutation, and \( k_1, k_2, \cdots, k_n \) are round subkeys derived from the cipher key \( k \).
The n-round DES encryption algorithm can be described as a product of permutations

\[ T_k = P^{-1} \circ \Theta \circ (\Theta \circ \sigma_{k_n}) \circ \cdots \circ (\Theta \circ \sigma_{k_1}) \circ P \]

where \( k \) is the cipher key, \( P \) is the initial (fixed) permutation, and \( k_1, k_2, \cdots, k_n \) are round subkeys derived from the cipher key \( k \).

For all \( 1 \leq i \leq n \), the \( i \)th round consists of the permutation \( \Theta \circ \sigma_{k_i} \) where \( \sigma_{k_i} : M \rightarrow M \) is the Feistel round function and \( \Theta : M \rightarrow M \) is the “swap function defined for \( x, y \in G^t \) as

\[ \Theta(x, y) = (y, x). \]
Fundamental Theorem of Finite Abelian Groups

**Theorem**

*Every finite Abelian group is a direct product of cyclic groups of prime-power order.*
Theorem
Every finite Abelian group is a direct product of cyclic groups of prime-power order.

Every cyclic group of order $n$ is isomorphic to $\mathbb{Z}_n$. 
Theorem
Every finite Abelian group is a direct product of cyclic groups of prime-power order.

Every cyclic group of order \( n \) is isomorphic to \( \mathbb{Z}_n \).

Corollary
Every finite Abelian group is isomorphic to a group of the form

\[ \mathbb{Z}_{p_1^{n_1}} \times \mathbb{Z}_{p_2^{n_2}} \times \cdots \times \mathbb{Z}_{p_k^{n_k}} \]

where \( p_i, 1 \leq i \leq k \) are primes.
For the past 25 years Elliptic Curves are widely used in Public-Key Cryptography. They offer increased speed, less memory and smaller key sizes.

An elliptic curve $E$ over a field $K$ is the set of points $E(K) := \{\infty\} \cup \{(x, y) \in K \times K | y^2 = x^3 + Ax + B\}$ where $A, B \in K$ and $4A^3 + 27B^2 \neq 0$. 

[Weierstrass equation of Elliptic Curves:]

The case of Elliptic Curves in Cryptography
The case of Elliptic Curves in Cryptography

For the past 25 years Elliptic Curves are widely used in Public-Key Cryptography. They offer increased speed, less memory and smaller key sizes.

Weierstrass equation of Elliptic Curves:
An elliptic curve $E$ over a field $K$ is the set of points

$$E(K) := \{ \infty \} \cup \{ (x, y) \in K \times K | y^2 = x^3 + Ax + B \}$$

where $A, B \in K$ and $4A^3 + 27B^2 \neq 0$. 
Let $E$ be an elliptic curve defined by $y^2 = x^3 + Ax + B$. Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be points on $E$ with $P_1, P_2 \neq \infty$. Define $P_1 + P_2 = P_3 = (x_3, y_3)$ as follows:
Let $E$ be an elliptic curve defined by $y^2 = x^3 + Ax + B$. Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be points on $E$ with $P_1, P_2 \neq \infty$. Define $P_1 + P_2 = P_3 = (x_3, y_3)$ as follows:

1. If $x_1 \neq x_2$, then

   $$x_3 = m^2 - x_1 - x_2, \quad y_3 = m(x_1 - x_3) - y_1,$$

   where $m = \frac{y_2 - y_1}{x_2 - x_1}$.
Let $E$ be an elliptic curve defined by $y^2 = x^3 + Ax + B$. Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be points on $E$ with $P_1, P_2 \neq \infty$. Define $P_1 + P_2 = P_3 = (x_3, y_3)$ as follows:

1. If $x_1 \neq x_2$, then

   $$x_3 = m^2 - x_1 - x_2, \quad y_3 = m(x_1 - x_3) - y_1,$$

   where $m = \frac{y_2 - y_1}{x_2 - x_1}$.

2. If $x_1 = x_2$ and $y_1 \neq y_2$, then $P_1 + P_2 = \infty$. 

Liljana Babinkostova

MATH 509 n-round DES over finite groups
The Group Law in Elliptic Curves

Let \( E \) be an elliptic curve defined by \( y^2 = x^3 + Ax + B \). Let \( P_1 = (x_1, y_1) \) and \( P_2 = (x_2, y_2) \) be points on \( E \) with \( P_1, P_2 \neq \infty \). Define \( P_1 + P_2 = P_3 = (x_3, y_3) \) as follows:

1. If \( x_1 \neq x_2 \), then
   \[
   x_3 = m^2 - x_1 - x_2, \quad y_3 = m(x_1 - x_3) - y_1,
   \]
   where \( m = \frac{y_2 - y_1}{x_2 - x_1} \).

2. If \( x_1 = x_2 \) and \( y_1 \neq y_2 \), then \( P_1 + P_2 = \infty \).

3. If \( P_1 = P_2 \) and \( y_1 \neq 0 \), then
   \[
   x_3 = m^2 - 2x_1, \quad y_3 = m(x_1 - x_3) - y_1,
   \]
   where \( m = \frac{3x_1^2 + A}{2y_1} \).
Let $E$ be an elliptic curve defined by $y^2 = x^3 + Ax + B$. Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be points on $E$ with $P_1, P_2 \neq \infty$. Define $P_1 + P_2 = P_3 = (x_3, y_3)$ as follows:

1. If $x_1 \neq x_2$, then
   
   $$x_3 = m^2 - x_1 - x_2, \quad y_3 = m(x_1 - x_3) - y_1,$$
   
   where $m = \frac{y_2 - y_1}{x_2 - x_1}$.

2. If $x_1 = x_2$ and $y_1 \neq y_2$, then $P_1 + P_2 = \infty$.

3. If $P_1 = P_2$ and $y_1 \neq 0$, then
   
   $$x_3 = m^2 - 2x_1, \quad y_3 = m(x_1 - x_3) - y_1,$$
   
   where $m = \frac{3x_1^2 + A}{2y_1}$.

4. If $P_1 = P_2$ and $y_1 = 0$, then $P_1 + P_2 = \infty$. 

Liljana Babinkostova

MATH 509 n-round DES over finite groups
Theorem

Let $E$ be an elliptic curve over the finite field $\mathbb{F}_p$. Then

$$E(\mathbb{F}_p) \cong \mathbb{Z}_n \text{ or } E(\mathbb{F}_p) \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$$

for some integer $n \geq 1$, or for some integers $n_1, n_2 \geq 1$ with $n_1 | n_2$. 
Simplified DES based on \((\mathbb{Z}_3, \oplus \text{mod } 3)\)

**E-DES** defines a cryptosystem with \(\mathcal{M} = \mathcal{C} = \{0, 1, 2\}^{18}\) and \(\mathcal{K} = \{0, 1, 2\}^{20}\). The encryption algorithm \(T_k\) can be expressed as

\[
T_k = P^{-1} \circ \sigma_{k_2} \circ \Theta \circ \sigma_{k_1} \circ P
\]

where \(k_1\) is derived from the cipher key \(k\) using the compression permutation

\[
S_1 = (16 \ 17 \ 12 \ 15 \ 20 \ 10 \ 11 \ 3 \ 7 \ 19 \ 13 \ 9 \ 8 \ 1 \ 18)
\]

and \(k_2\) using the compression permutation

\[
S_2 = (6 \ 7 \ 2 \ 20 \ 4 \ 3 \ 9 \ 8 \ 18 \ 10 \ 15 \ 14 \ 11 \ 12 \ 5)
\]
Simplified DES based on \((\mathbb{Z}_3, \oplus \mod 3)\)

**Initial Permutation:**

\[ P = (6 \ 3 \ 16 \ 11 \ 7 \ 17 \ 14 \ 8 \ 5 \ 15 \ 1 \ 2 \ 4 \ 18 \ 13 \ 9 \ 10 \ 12) \]

**Expansion Permutation:**

\[ E = (9 \ 1 \ 2 \ 3 \ 4 \ 5 \ 6 \ 3 \ 4 \ 5 \ 6 \ 7 \ 8 \ 9 \ 1) \]
Simplified DES based on \((\mathbb{Z}_3, \oplus \text{mod } 3)\)

### S-box 3

| 4 | 5 | 13 | 23 | 10 | 14 | 8 | 25 | 6 | 12 | 17 | 16 | 26 | 3 | 20 | 19 | 22 | 15 | 0 | 24 | 9 | 18 | 7 | 1 | 21 | 11 | 2 |
|---|---|----|----|----|----|---|----|---|----|----|----|----|---|----|----|----|----|---|----|---|----|----|---|----|----|---|----|
| 6 | 7 | 15 | 25 | 12 | 16 | 10 | 0 | 8 | 14 | 19 | 18 | 1 | 5 | 22 | 21 | 24 | 17 | 2 | 26 | 11 | 20 | 9 | 3 | 23 | 13 | 4 |
| 7 | 8 | 16 | 26 | 13 | 17 | 11 | 1 | 9 | 15 | 20 | 19 | 2 | 6 | 23 | 22 | 25 | 18 | 3 | 0 | 12 | 21 | 10 | 4 | 24 | 14 | 5 |
| 8 | 9 | 17 | 0 | 14 | 18 | 12 | 2 | 10 | 16 | 21 | 20 | 3 | 7 | 24 | 23 | 26 | 19 | 4 | 1 | 13 | 22 | 11 | 5 | 25 | 15 | 6 |
| 13 | 14 | 22 | 5 | 19 | 23 | 17 | 7 | 15 | 21 | 26 | 25 | 8 | 12 | 2 | 1 | 4 | 24 | 9 | 6 | 18 | 0 | 16 | 10 | 3 | 20 | 11 |
| 12 | 13 | 21 | 4 | 18 | 22 | 16 | 6 | 14 | 20 | 25 | 24 | 7 | 11 | 1 | 0 | 3 | 23 | 8 | 5 | 17 | 26 | 15 | 9 | 2 | 19 | 10 |
| 19 | 20 | 1 | 11 | 25 | 2 | 23 | 13 | 21 | 0 | 5 | 4 | 14 | 18 | 10 | 7 | 10 | 3 | 15 | 12 | 24 | 6 | 22 | 16 | 9 | 26 | 17 |
| 0 | 1 | 9 | 19 | 6 | 10 | 4 | 21 | 2 | 8 | 13 | 12 | 22 | 26 | 16 | 15 | 18 | 11 | 23 | 20 | 5 | 14 | 3 | 24 | 17 | 7 | 25 |
| 20 | 21 | 2 | 12 | 26 | 3 | 24 | 14 | 22 | 1 | 6 | 5 | 15 | 19 | 9 | 8 | 11 | 4 | 16 | 13 | 25 | 7 | 23 | 17 | 10 | 0 | 18 |

Example

Assume that the S-box input to the S-box 3 is 22010. The first and the last nits combine to form 20, which corresponds to row 5 of the S-box. The middle 3 nits combine to form 201, which correspond to the column 18. The entry under row 5, column 18 is 24. The output will be 24 $\oplus 3 \equiv 220$. 

Liljana Babinkostova

MATH 509 n-round DES over finite groups
Simplified DES based on \((\mathbb{Z}_3, \oplus_{\text{mod} 3})\)

**S-box 3**

| 4 | 5 | 13 | 23 | 10 | 14 | 8 | 25 | 6 | 12 | 17 | 16 | 26 | 3 | 20 | 19 | 22 | 15 | 0 | 24 | 9 | 18 | 7 | 1 | 21 | 11 | 2 |
|---|---|----|----|----|----|---|----|---|----|----|----|----|---|----|----|----|----|---|----|----|----|---|----|----|----|
| 6 | 7 | 15 | 25 | 12 | 16 | 10 | 0 | 8 | 14 | 19 | 18 | 1 | 5 | 22 | 21 | 24 | 17 | 2 | 26 | 11 | 20 | 9 | 3 | 23 | 13 | 4 |
| 7 | 8 | 16 | 26 | 13 | 17 | 11 | 1 | 9 | 15 | 20 | 19 | 2 | 6 | 23 | 22 | 25 | 18 | 3 | 0 | 12 | 21 | 10 | 4 | 24 | 14 | 5 |
| 8 | 9 | 17 | 0 | 14 | 18 | 12 | 2 | 10 | 16 | 21 | 20 | 3 | 7 | 24 | 23 | 26 | 19 | 4 | 1 | 13 | 22 | 11 | 5 | 25 | 15 | 6 |
| 13 | 14 | 22 | 5 | 19 | 23 | 17 | 7 | 15 | 21 | 26 | 25 | 8 | 12 | 2 | 1 | 4 | 24 | 9 | 6 | 18 | 0 | 16 | 10 | 3 | 20 | 11 |
| 12 | 13 | 21 | 4 | 18 | 22 | 16 | 6 | 14 | 20 | 25 | 24 | 7 | 11 | 1 | 0 | 3 | 23 | 8 | 5 | 17 | 26 | 15 | 9 | 2 | 19 | 10 |
| 19 | 20 | 1 | 11 | 25 | 2 | 23 | 13 | 21 | 0 | 5 | 4 | 14 | 18 | 10 | 7 | 10 | 3 | 15 | 12 | 24 | 6 | 22 | 16 | 9 | 26 | 17 |
| 0 | 1 | 9 | 19 | 6 | 10 | 4 | 21 | 2 | 8 | 13 | 12 | 22 | 26 | 16 | 15 | 18 | 11 | 23 | 20 | 5 | 14 | 3 | 24 | 17 | 7 | 25 |
| 20 | 21 | 2 | 12 | 26 | 3 | 24 | 14 | 22 | 1 | 6 | 5 | 15 | 19 | 9 | 8 | 11 | 4 | 16 | 13 | 25 | 7 | 23 | 17 | 10 | 0 | 18 |

**Example**

Assume that the S-box input to the S-box 3 is 22010.
Simplified DES based on \((\mathbb{Z}_3, \oplus \mod 3)\)

**S-box 3**

<table>
<thead>
<tr>
<th>4</th>
<th>5</th>
<th>13</th>
<th>23</th>
<th>10</th>
<th>14</th>
<th>8</th>
<th>25</th>
<th>6</th>
<th>12</th>
<th>17</th>
<th>16</th>
<th>26</th>
<th>3</th>
<th>20</th>
<th>19</th>
<th>22</th>
<th>15</th>
<th>0</th>
<th>24</th>
<th>9</th>
<th>18</th>
<th>7</th>
<th>1</th>
<th>21</th>
<th>11</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>7</td>
<td>15</td>
<td>25</td>
<td>12</td>
<td>16</td>
<td>10</td>
<td>0</td>
<td>8</td>
<td>14</td>
<td>19</td>
<td>18</td>
<td>1</td>
<td>5</td>
<td>22</td>
<td>21</td>
<td>24</td>
<td>17</td>
<td>2</td>
<td>26</td>
<td>11</td>
<td>20</td>
<td>9</td>
<td>3</td>
<td>23</td>
<td>13</td>
<td>4</td>
</tr>
<tr>
<td>7</td>
<td>8</td>
<td>16</td>
<td>26</td>
<td>13</td>
<td>17</td>
<td>11</td>
<td>1</td>
<td>9</td>
<td>15</td>
<td>20</td>
<td>19</td>
<td>2</td>
<td>6</td>
<td>23</td>
<td>22</td>
<td>25</td>
<td>18</td>
<td>3</td>
<td>0</td>
<td>12</td>
<td>21</td>
<td>10</td>
<td>4</td>
<td>24</td>
<td>14</td>
<td>5</td>
</tr>
<tr>
<td>8</td>
<td>9</td>
<td>17</td>
<td>0</td>
<td>14</td>
<td>18</td>
<td>12</td>
<td>2</td>
<td>10</td>
<td>16</td>
<td>21</td>
<td>20</td>
<td>3</td>
<td>7</td>
<td>24</td>
<td>23</td>
<td>26</td>
<td>19</td>
<td>4</td>
<td>1</td>
<td>13</td>
<td>22</td>
<td>11</td>
<td>5</td>
<td>25</td>
<td>15</td>
<td>6</td>
</tr>
<tr>
<td>13</td>
<td>14</td>
<td>22</td>
<td>5</td>
<td>19</td>
<td>23</td>
<td>17</td>
<td>7</td>
<td>15</td>
<td>21</td>
<td>26</td>
<td>25</td>
<td>8</td>
<td>12</td>
<td>2</td>
<td>1</td>
<td>4</td>
<td>24</td>
<td>9</td>
<td>6</td>
<td>18</td>
<td>0</td>
<td>16</td>
<td>10</td>
<td>3</td>
<td>20</td>
<td>11</td>
</tr>
<tr>
<td>12</td>
<td>13</td>
<td>21</td>
<td>4</td>
<td>18</td>
<td>22</td>
<td>16</td>
<td>6</td>
<td>14</td>
<td>20</td>
<td>25</td>
<td>24</td>
<td>7</td>
<td>11</td>
<td>1</td>
<td>0</td>
<td>3</td>
<td>23</td>
<td>8</td>
<td>5</td>
<td>17</td>
<td>26</td>
<td>15</td>
<td>9</td>
<td>2</td>
<td>19</td>
<td>10</td>
</tr>
<tr>
<td>19</td>
<td>20</td>
<td>1</td>
<td>11</td>
<td>25</td>
<td>2</td>
<td>23</td>
<td>13</td>
<td>21</td>
<td>0</td>
<td>5</td>
<td>4</td>
<td>14</td>
<td>18</td>
<td>10</td>
<td>7</td>
<td>10</td>
<td>3</td>
<td>15</td>
<td>12</td>
<td>24</td>
<td>6</td>
<td>22</td>
<td>16</td>
<td>9</td>
<td>26</td>
<td>17</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>9</td>
<td>19</td>
<td>6</td>
<td>10</td>
<td>4</td>
<td>21</td>
<td>2</td>
<td>8</td>
<td>13</td>
<td>12</td>
<td>22</td>
<td>26</td>
<td>16</td>
<td>15</td>
<td>18</td>
<td>11</td>
<td>23</td>
<td>20</td>
<td>5</td>
<td>14</td>
<td>3</td>
<td>24</td>
<td>17</td>
<td>7</td>
<td>25</td>
</tr>
<tr>
<td>20</td>
<td>21</td>
<td>2</td>
<td>12</td>
<td>26</td>
<td>3</td>
<td>24</td>
<td>14</td>
<td>22</td>
<td>1</td>
<td>6</td>
<td>5</td>
<td>15</td>
<td>19</td>
<td>9</td>
<td>8</td>
<td>11</td>
<td>4</td>
<td>16</td>
<td>13</td>
<td>25</td>
<td>7</td>
<td>23</td>
<td>17</td>
<td>10</td>
<td>0</td>
<td>18</td>
</tr>
</tbody>
</table>

**Example**

Assume that the S-box input to the S-box 3 is 22010. The first and the last nits combine to form 20, which corresponds to row 5 of the S-box.
Simplified DES based on \((\mathbb{Z}_3, \oplus \mod 3)\)

S-box 3

| 4 | 5 | 13 | 23 | 10 | 14 | 8 | 25 | 6 | 12 | 17 | 16 | 26 | 3 | 20 | 19 | 22 | 15 | 0 | 24 | 9 | 18 | 7 | 1 | 21 | 11 | 2 |
|---|---|----|----|----|----|---|----|---|----|----|----|----|---|----|----|----|----|---|----|----|----|---|----|----|---|---|---|---|
| 6 | 7 | 15 | 25 | 12 | 16 | 10 | 0 | 8 | 14 | 19 | 18 | 1 | 5 | 22 | 21 | 24 | 17 | 2 | 26 | 11 | 20 | 9 | 3 | 23 | 13 | 4 |
| 7 | 8 | 16 | 26 | 13 | 17 | 11 | 1 | 9 | 15 | 20 | 19 | 2 | 6 | 23 | 22 | 25 | 18 | 3 | 0 | 12 | 21 | 10 | 4 | 24 | 14 | 5 |
| 8 | 9 | 17 | 0 | 14 | 18 | 12 | 2 | 10 | 16 | 21 | 20 | 3 | 7 | 24 | 23 | 26 | 19 | 4 | 1 | 13 | 22 | 11 | 5 | 25 | 15 | 6 |
| 13 | 14 | 22 | 5 | 19 | 23 | 17 | 7 | 15 | 21 | 26 | 25 | 8 | 12 | 2 | 1 | 4 | 24 | 9 | 6 | 18 | 0 | 16 | 10 | 3 | 20 | 11 |
| 12 | 13 | 21 | 4 | 18 | 22 | 16 | 6 | 14 | 20 | 25 | 24 | 7 | 11 | 1 | 0 | 3 | 23 | 8 | 5 | 17 | 26 | 15 | 9 | 2 | 19 | 10 |
| 19 | 20 | 1 | 11 | 25 | 2 | 23 | 13 | 21 | 0 | 5 | 4 | 14 | 18 | 10 | 7 | 10 | 3 | 15 | 12 | 24 | 6 | 22 | 16 | 9 | 26 | 17 |
| 0 | 1 | 9 | 19 | 6 | 10 | 4 | 21 | 2 | 8 | 13 | 12 | 22 | 26 | 16 | 15 | 18 | 11 | 23 | 20 | 5 | 14 | 3 | 24 | 17 | 7 | 25 |

Example

Assume that the S-box input to the S-box 3 is 22010. The first and the last nits combine to form 20, which corresponds to row 5 of the S-box. The middle 3 nits combine to form 201, which correspond to the column 18. The entry under row 5, column 18 is 24.
Simplified DES based on \((\mathbb{Z}_3, \oplus \mod 3)\)

**S-box 3**

| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 |
|---|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|---|
| 4 | 5 | 13 | 23 | 10 | 14 | 8 | 25 | 6 | 12 | 17 | 16 | 26 | 3 | 20 | 19 | 22 | 15 | 0 | 24 | 9 | 18 | 7 | 1 | 21 | 11 | 2 |
| 6 | 7 | 15 | 25 | 12 | 16 | 10 | 0 | 8 | 14 | 19 | 18 | 1 | 5 | 22 | 21 | 24 | 17 | 2 | 26 | 11 | 20 | 9 | 3 | 23 | 13 | 4 |
| 7 | 8 | 16 | 26 | 13 | 17 | 11 | 1 | 9 | 15 | 20 | 19 | 2 | 6 | 23 | 22 | 25 | 18 | 3 | 0 | 12 | 21 | 10 | 4 | 24 | 14 | 5 |
| 8 | 9 | 17 | 0 | 14 | 18 | 12 | 2 | 10 | 16 | 21 | 20 | 3 | 7 | 24 | 23 | 26 | 19 | 4 | 1 | 13 | 22 | 11 | 5 | 25 | 15 | 6 |
| 13 | 14 | 22 | 5 | 19 | 23 | 17 | 7 | 15 | 21 | 26 | 25 | 8 | 12 | 2 | 1 | 4 | 24 | 9 | 6 | 18 | 0 | 16 | 10 | 3 | 20 | 11 |
| 12 | 13 | 21 | 4 | 18 | 22 | 16 | 6 | 14 | 20 | 25 | 24 | 7 | 11 | 1 | 0 | 3 | 23 | 8 | 5 | 17 | 26 | 15 | 9 | 2 | 19 | 10 |
| 19 | 20 | 1 | 11 | 25 | 2 | 23 | 13 | 21 | 0 | 5 | 4 | 14 | 18 | 10 | 7 | 10 | 3 | 15 | 12 | 24 | 6 | 22 | 16 | 9 | 26 | 17 |
| 0 | 1 | 9 | 19 | 6 | 10 | 4 | 21 | 2 | 8 | 13 | 12 | 22 | 26 | 16 | 15 | 18 | 11 | 23 | 20 | 5 | 14 | 3 | 24 | 17 | 7 | 25 |
| 20 | 21 | 2 | 12 | 26 | 3 | 24 | 14 | 22 | 1 | 6 | 5 | 15 | 19 | 9 | 8 | 11 | 4 | 16 | 13 | 25 | 7 | 23 | 17 | 10 | 0 | 18 |

**Example**

Assume that the S-box input to the S-box 3 is 22010. The first and the last nits combine to form 20, which corresponds to row 5 of the S-box. The middle 3 nits combine to form 201, which correspond to the column 18. The entry under row 5, column 18 is 24. The output will be \(24_3 = 220\).
Let $T_{\Pi} = \{ T_k : k \in K \}$ be the set of all encryption transformations for the cryptosystem $\Pi = (M, C, K, T)$.

Let $T_k^{-1}$ denote the inverse of $T_k$. In a cryptosystem where $M = C$, the mapping $T_k$ is a permutation.

Let $\langle T_{\Pi} \rangle$ denotes the subgroup of $S_M$ that is generated by the set $T_{\Pi}$.

Definition A cryptosystem $\Pi$ is called closed if its set of encryption transformations $T_{\Pi}$ is closed under functional composition i.e. for every $k_1, k_2 \in K$ there is $k_3 \in K$ such that $T_{k_1} \circ T_{k_2} = T_{k_3}$.

Question 1: Is n-round DES over any finite group $G$ closed?
Let $T_\Pi = \{ T_k : k \in \mathcal{K} \}$ be the set of all encryption transformations for the cryptosystem $\Pi = (\mathcal{M}, \mathcal{C}, \mathcal{K}, T)$. Let $T_k^{-1}$ denote the inverse of $T_k$. In a cryptosystem where $\mathcal{M} = \mathcal{C}$ the mapping $T_k$ is a permutation.
Algebraic properties of DES

Let $\mathcal{I}_\Pi = \{ T_k : k \in \mathcal{K} \}$ be the set of all encryption transformations for the cryptosystem $\Pi = (\mathcal{M}, \mathcal{C}, \mathcal{K}, T)$. Let $T_k^{-1}$ denote the inverse of $T_k$. In a cryptosystem where $\mathcal{M} = \mathcal{C}$ the mapping $T_k$ is a permutation. Let $\langle \mathcal{I}_\Pi \rangle$ denotes the subgroup of $S_{\mathcal{M}}$ that is generated by the set $\mathcal{I}_\Pi$.

**Definition**

A cryptosystem $\Pi$ is called **closed** if its set of encryption transformations $\mathcal{I}_\Pi$ is closed under functional composition i.e for every $k_1, k_2 \in \mathcal{K}$ there is $k_3 \in \mathcal{K}$ such that $T_{k_1} \circ T_{k_2} = T_{k_3}$.
Let $\mathcal{T}_\Pi = \{ T_k : k \in \mathcal{K} \}$ be the set of all encryption transformations for the cryptosystem $\Pi = (\mathcal{M}, \mathcal{C}, \mathcal{K}, T)$. Let $T_k^{-1}$ denote the inverse of $T_k$. In a cryptosystem where $\mathcal{M} = \mathcal{C}$ the mapping $T_k$ is a permutation. Let $\langle \mathcal{T}_\Pi \rangle$ denotes the subgroup of $S_{\mathcal{M}}$ that is generated by the set $\mathcal{T}_\Pi$.

**Definition**

A cryptosystem $\Pi$ is called *closed* if its set of encryption transformations $\mathcal{T}_\Pi$ is closed under functional composition i.e for every $k_1, k_2 \in \mathcal{K}$ there is $k_3 \in \mathcal{K}$ such that $T_{k_1} \circ T_{k_2} = T_{k_3}$.

**Question 1:** Is $n$-round DES over any finite group $G$ closed?
Definition
A cryptosystem is pure if and only if for every three keys $k_1, k_2$, and $k_3$ there exists a key $k_4$ such that $T_{k_1} \circ T_{k_2}^{-1} \circ T_{k_3} = T_{k_4}$.

Question 2: Is $n$-round DES over any finite group $G$ pure?

Definition
A cryptosystem $\Pi$ is faithful if different keys represent different permutations (if $k$ and $\ell$ are distinct elements of $K$, then $T_k \neq T_\ell$ are distinct elements of $T_\Pi$).

Question 3: Is $n$-round DES over any finite group $G$ faithful? How many distinct transformations are represented by the DES keys?
Questions about the algebraic properties of DES

Definition
A cryptosystem is pure if and only if for every three keys $k_1, k_2$, and $k_3$ there exists a key $k_4$ such that $T_{k_1} \circ T_{k_2}^{-1} \circ T_{k_3} = T_{k_4}$.

Question 2: Is n-round DES over any finite group $G$ pure?
Questions about the algebraic properties of DES

Definition
A cryptosystem is *pure* if and only if for every three keys $k_1, k_2$, and $k_3$ there exists a key $k_4$ such that $T_{k_1} \circ T_{k_2}^{-1} \circ T_{k_3} = T_{k_4}$.

Question 2: Is n-round DES over any finite group $G$ pure?

Definition
A cryptosystem $\Pi$ is *faithful* if different keys represent different permutations (if $k$ and $\ell$ are distinct elements of $K$, then $T_k \neq T_{\ell}$ are distinct elements of $T_\Pi$).
Questions about the algebraic properties of DES

Definition
A cryptosystem is *pure* if and only if for every three keys $k_1, k_2,$ and $k_3$ there exists a key $k_4$ such that $T_{k_1} \circ T_{k_2}^{-1} \circ T_{k_3} = T_{k_4}.$

**Question 2:** Is n-round DES over any finite group $G$ pure?

Definition
A cryptosystem $\Pi$ is *faithful* if different keys represent different permutations (if $k$ and $\ell$ are distinct elements of $K$, then $T_k \neq T_\ell$ are distinct elements of $T_\Pi$).

**Question 3:** Is n-round DES over any finite group $G$ faithful? How many distinct transformations are represented by the DES keys?
Questions about the algebraic properties of DES

Question 4: Is the identity $I \in T^{\text{DES}}$?

Question 5: What is the group generated by one-round DES over any finite group?

Question 6: For how many keys $k_1, k_2, k_3 \in K$ is true that $T^{k_3} = T^{k_1} \circ T^{k_2}$?

Question 7: Is $n$-round DES over any finite group homogeneous?
Questions about the algebraic properties of DES

Question 4: Is the identity $I \in \mathcal{T}_{DES}$?
Questions about the algebraic properties of DES

Question 4: Is the identity $I \in T_{DES}$?

Question 5: What is the group generated by one-round DES over any finite group?
Questions about the algebraic properties of DES

Question 4: Is the identity $I \in T_{DES}$?

Question 5: What is the group generated by one-round DES over any finite group?

Question 6: For how many keys $k_1, k_2, k_3 \in K$ is true that $T_{k_3} = T_{k_1} \circ T_{k_2}$?
Questions about the algebraic properties of DES

Question 4: Is the identity \( I \in \mathcal{T}_{DES} \)?

Question 5: What is the group generated by one-round DES over any finite group?

Question 6: For how many keys \( k_1, k_2, k_3 \in \mathcal{K} \) is true that \( T_{k_3} = T_{k_1} \circ T_{k_2} \)?

Question 7: Is n-round DES over any finite group homogeneous?