Block ciphers

Attacks and Security

Differential cryptanalysis

• Differential cryptanalysis is a general cryptanalytic technique proposed by Eli Biham and Adi Shamir in the late 80’s.
  – Applicable primarily to block ciphers, but also to stream ciphers and cryptographic hash functions.
  – Success in attacking DES-like ciphers. However, differential cryptanalysis known by the intelligence community and one of the secret design goals for DES. No practical attacks against DES result from this technique.

Definition

• Generally a chosen-plaintext attack. Start with two plaintexts whose difference is a chosen binary string. Goal is to find difference patterns that result in predictable differences at the ciphertext level.

\[
\begin{array}{cccccccccccc}
P_1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\
\Delta & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
\end{array}
\]
Differentials on DES

- DES is a Feistel network
  - Differentials propagate predictably through permutations and XOR operations
- Looking within the F() function
  - Expansion permutation (differentials traceable)
  - XOR with key (differentials propagate)
  - S-Boxes are applied AFTER key XOR

S-DES

- S-DES (simplified DES) will be used for an example of differential cryptanalysis.
- Important step is to examine how differentials propagate through S-Boxes

The S-Box is read as follows. Let \( (I_0, I_1, I_2, I_3) \) be a 4-bit input to \( S_0 \). Index the table at \( (m, n) \), where \( m = (I_0, I_3) \) and \( n = (I_1, I_2) \); write the value in binary as 2-bit output.
Example

- Consider differential $\Delta = 0111$

| P1 (m,n) | P2 (m,n) | Q1 | Q2 | $\Delta$
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>0000</td>
<td>01</td>
<td>0111</td>
<td>1.3</td>
<td>20</td>
</tr>
<tr>
<td>0001</td>
<td>11</td>
<td>0110</td>
<td>0.3</td>
<td>10</td>
</tr>
<tr>
<td>0010</td>
<td>00</td>
<td>0101</td>
<td>1.2</td>
<td>01</td>
</tr>
<tr>
<td>0011</td>
<td>10</td>
<td>0100</td>
<td>0.2</td>
<td>11</td>
</tr>
<tr>
<td>0100</td>
<td>20</td>
<td>1111</td>
<td>3.3</td>
<td>10</td>
</tr>
<tr>
<td>0101</td>
<td>31</td>
<td>1110</td>
<td>2.3</td>
<td>11</td>
</tr>
<tr>
<td>0110</td>
<td>21</td>
<td>1101</td>
<td>3.2</td>
<td>11</td>
</tr>
<tr>
<td>0111</td>
<td>31</td>
<td>1100</td>
<td>2.2</td>
<td>01</td>
</tr>
</tbody>
</table>

Table shows outputs of $S_0$ when the inputs differ by 0111.
- The statistical distribution of output differentials is unbalanced. $5/8$ of differentials equal 01. The differential 11 does not occur.