One Little Cipher Story

MEPhI

Department of Cryptology

Alisa Koreneva, Vladimir Fomichev
RUMP Session, EUROCRYPT 2012
Subject of the Research

- Generalized Feistel Networks
Cipher under Research

\[ x(j) = (x_1(j), x_2(j), \ldots, x_n(j)) \]

- \( j \) – number of round
- \( q_j \) – round key
- \( x(j) = (x_1(j), \ldots, x_n(j)) \) – blocks of text
- \( \Psi(x_2, \ldots, x_n, q_j) \), – round function
**Definition:** The Feistel function $\psi(y_2,\ldots,y_n,k)$ is an invariant under involution $\tau_{n-1}$, if $\psi(y_2,\ldots,y_n,k) = \psi(y_n,\ldots,y_2,k)$.

**The Criterion:**

The $h$-round generalized Feistel cipher with function $\psi(y_2,\ldots,y_n,k)$ is an involution $\iff \psi(y_2,\ldots,y_n,k)$ is an invariant under involution $\tau_{n-1}$. 
Beginning

Defining a set of "elementary" transformations

Constructing a set of essential variables

Constructing MED for each transformation

Transformations parallel?

YES

Matrix is formed by multiplication

NO

Matrix is formed by component

Obtaining matrix for the single iteration of round transformation

Matrix sequential raising to power

Matrix positive?

NO

End

YES

Obtaining exponent value
Results for DES algorithm

*MED – Matrix of Essential Dependence (64x64 for DES)
The exponent value for DES MED = 5

<table>
<thead>
<tr>
<th>1</th>
<th>...</th>
<th>32</th>
<th>33</th>
<th>...</th>
<th>64</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>32</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>33</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>64</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Symbol 0: Zero matrix (32x32)
Symbol 1: Unity matrix (32x32)
Symbol $\Psi$: MED for the round function $\Psi$ (32x32)
One Little Cipher

- The round function (full description is given in my research work)
Thank you! 

Thank you for your attention!

e-mail: alisa.koreneva@gmail.com