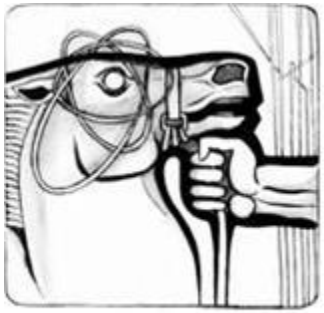
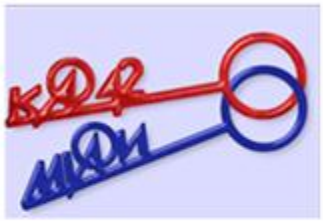
One Little Cipher Story



MEPhI



Department of Cryptology

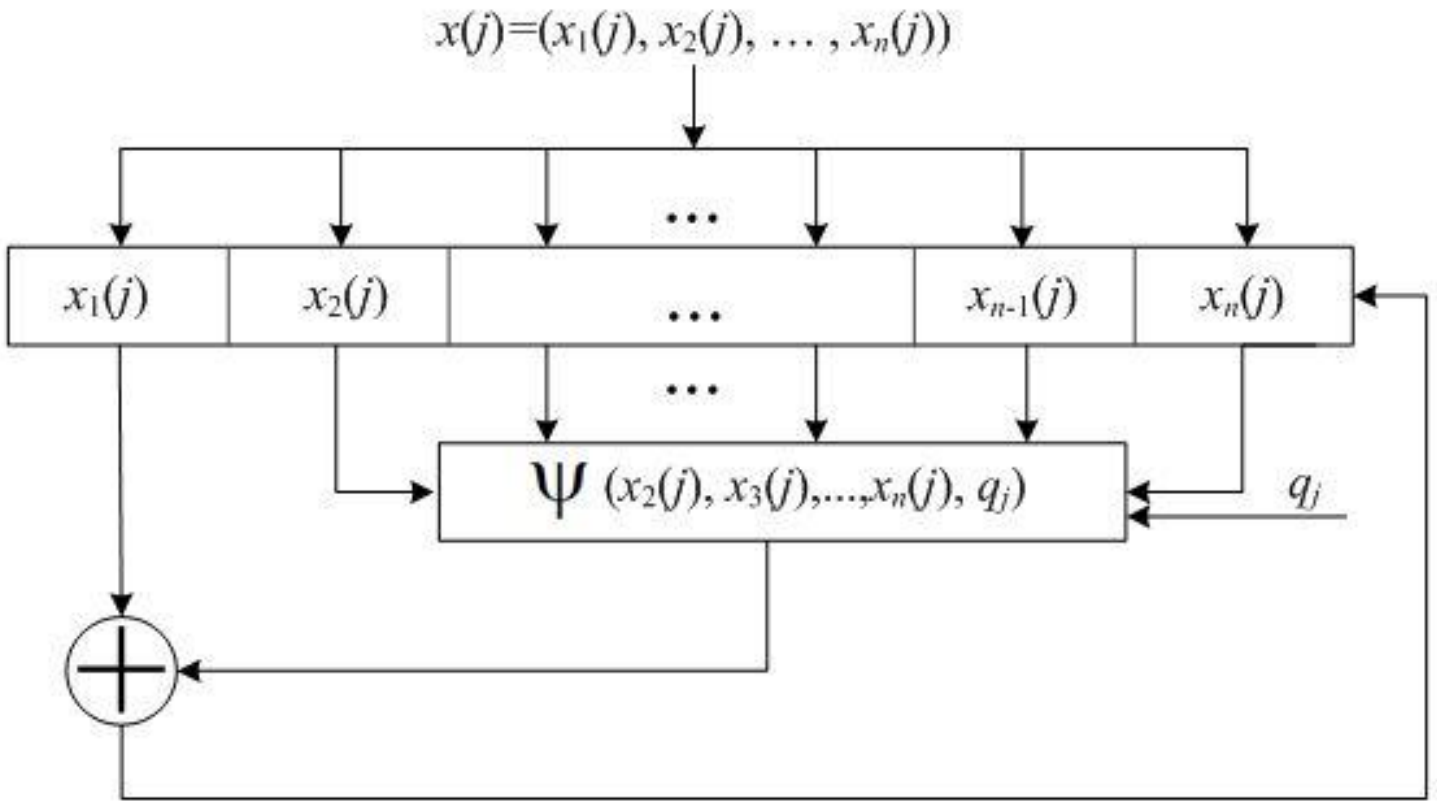
Alisa Koreneva, Vladimir Fomichev

RUMP Session, EUROCRYPT 2012

Subject of the Research

- **Generalized Feistel Networks**

Cipher under Research



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

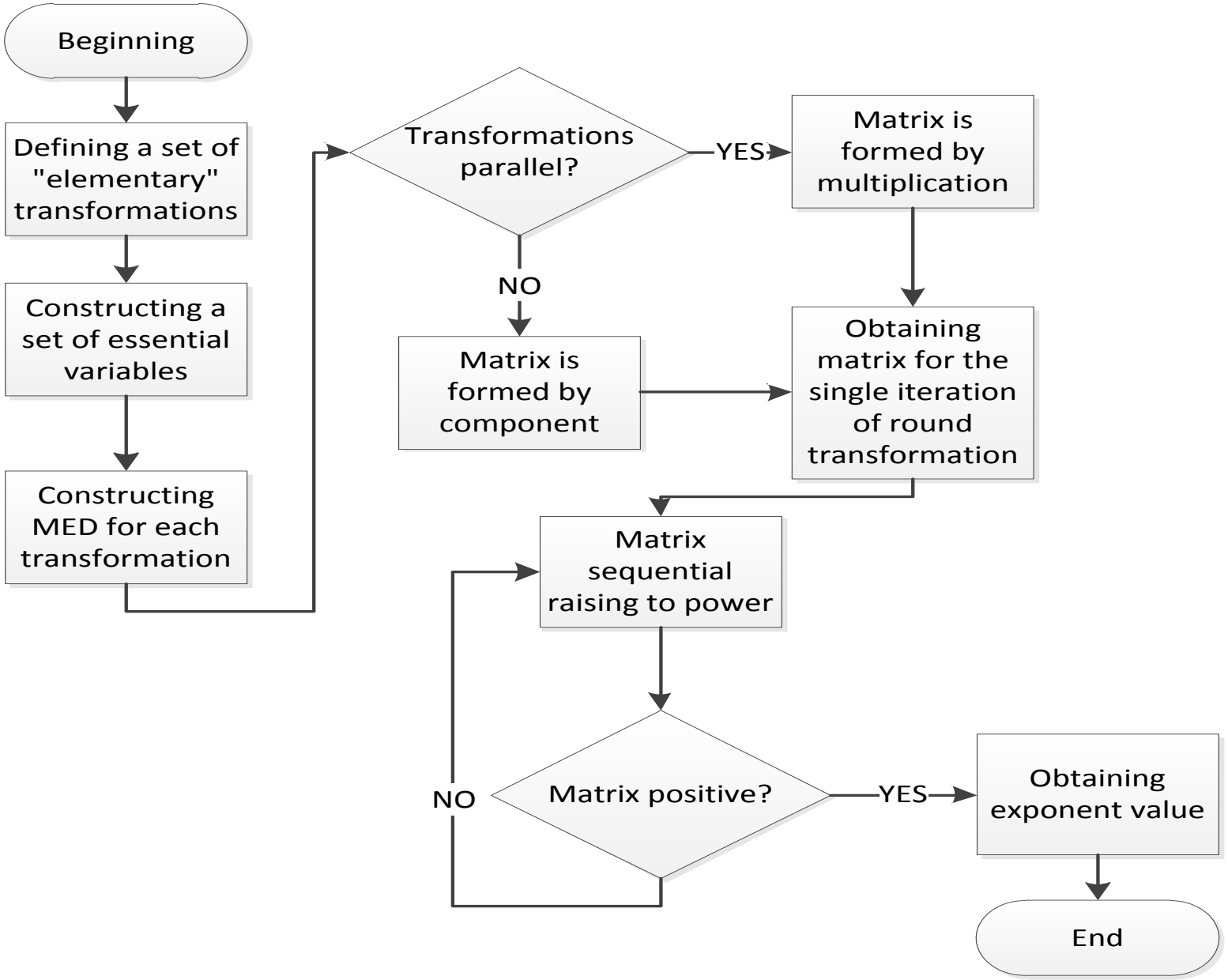
Cipher's Involution

Definition: The Feistel function $\psi(y_2,\ldots,y_n,k)$ is an invariant under involution τ_{n-1}, if $\boldsymbol{\psi(y_2,\ldots,y_n,k)=\psi(y_n,\ldots,y_2,k)}$.

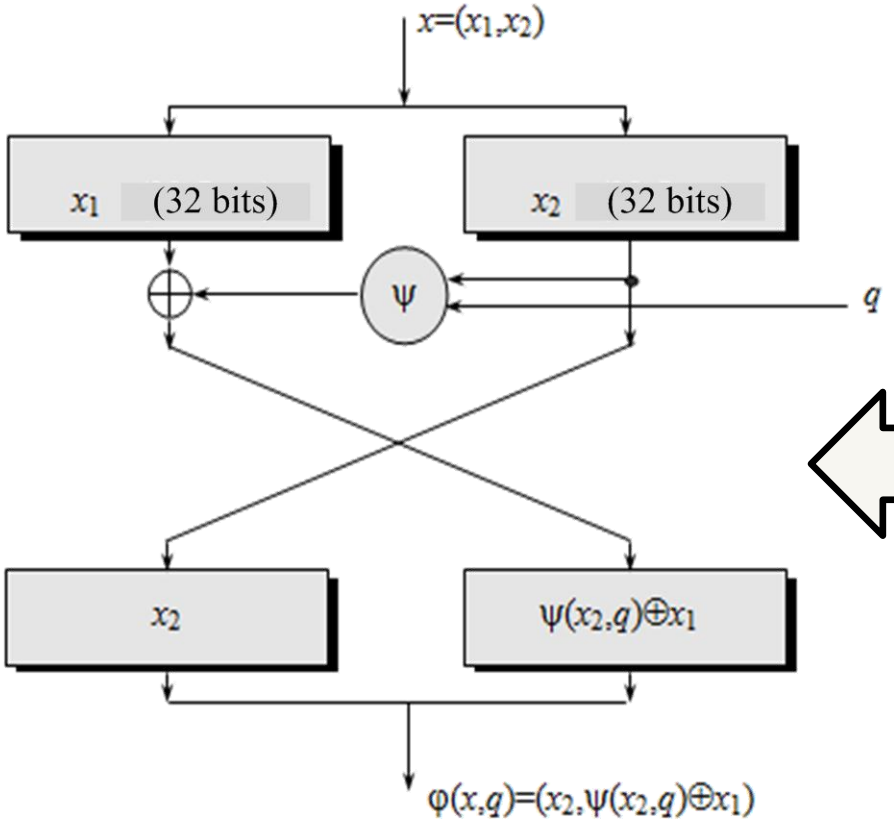
The Criterion:

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

Minimal number of rounds



Results for DES algorithm



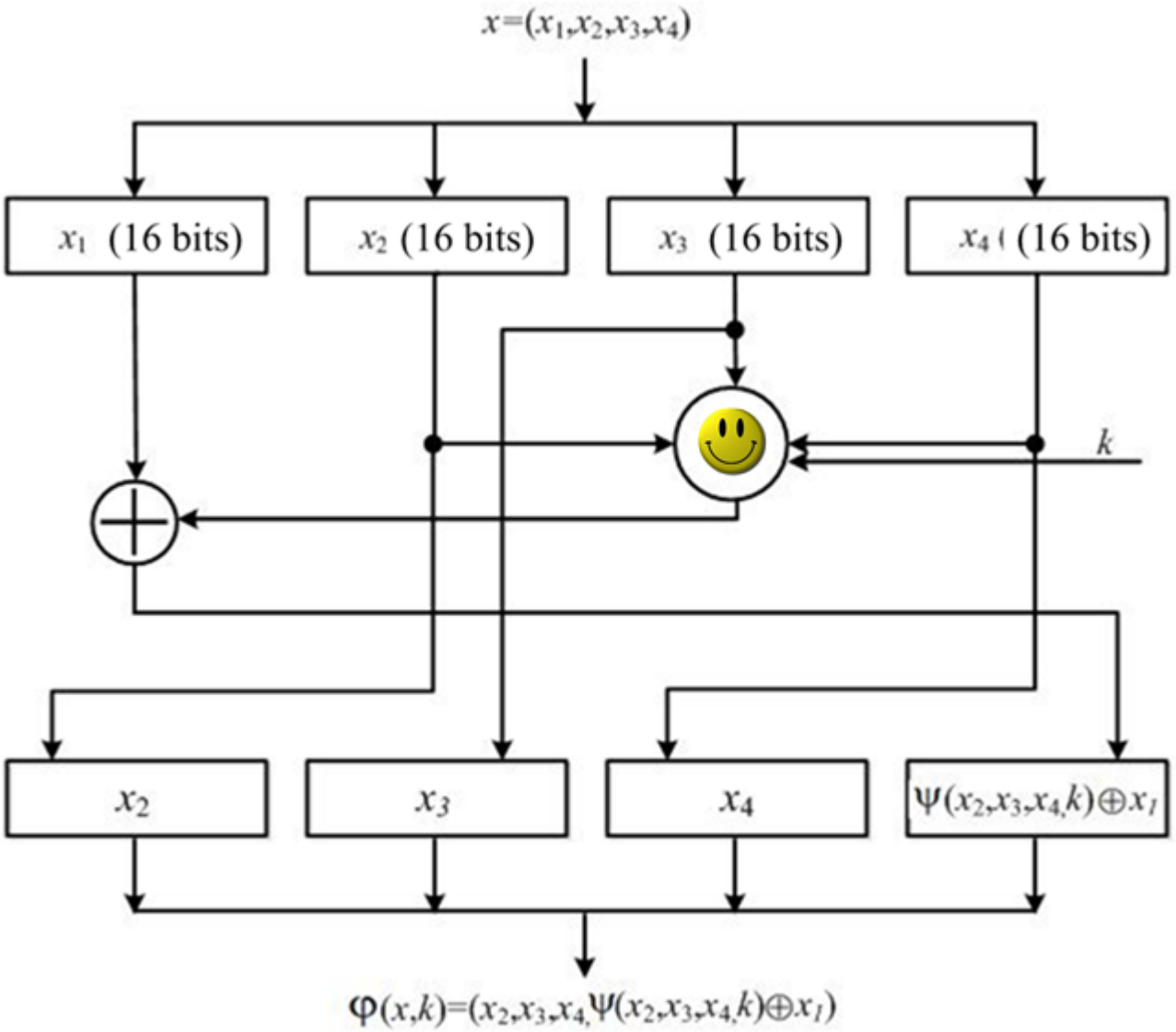
	1 … 32	33 … 64
1 … 32	0	1
33 … 64	1	Ψ

***MED – Matrix of Essential Dependence (64X64 for DES)**

The exponent value for DES MED = 5

Symbol 0: Zero matrix (32x32)
Symbol 1: Unity matrix (32x32)
Symbol Ψ: MED for the round function Ψ (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