Exploration of Cryptography

Whitfield Diffie

Distinguished Visiting Professor

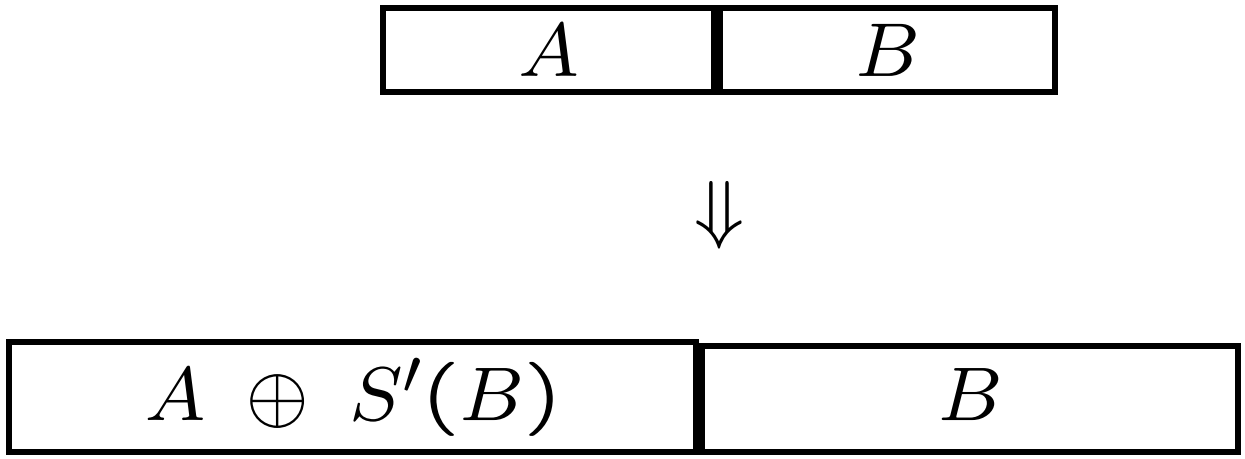
Zhejiang University

Homework II

Problem 1

Feistel type systems: DES, Magma are only superficially different from straight through systems like AES.

"Feistelized" S-box



Homework Problem 1 (Cont'd)

Write Magma as a straight-through system using Feistelized S-boxes

Homework Problem 1 (Cont'd)
Just Something to Think About

What are the problems with writing DES as a straight-through system using Feistelized S-boxes?

Homework Problem 2

Cellular Automata in SM4

Two cellular automata are used in SM4, one

$$L(B) = B \oplus B \lll 2 \oplus B \lll 10 \oplus B \lll 18 \oplus B \lll 24$$

in the encryption process and one

$$L'(K) = K \oplus K \lll 13 \oplus K \lll 23$$

in the key schedule.

Determine whether L' is invertible.

Homework Problem 3
Balance

A sequence of bits is balanced if it has the same number of 0s and 1s. A function is called balanced if the sequence of its outputs over all inputs is balanced.

Homework Problem 3 (Cont'd)

Demonstrate that every column in the table of an invertible n-bit to n-bit function must be balanced.

Homework Problem 4
Balance (Cont'd)

Show that the linear functions (other than 0) are balanced.

Homework Problem 5
R S A

Suppose that the RSA modulus is $126,619$ and the encrypting exponent is 33. What is the decrypting exponent?