Exercise 2

Module 1 - Introduction to Cryptography and Data Security

Knut Lucas Andersen
Master Applied Information Security
isits AG International School of IT Security

May 7, 2017

Contents

1 DES-history

a) What was/is the name of the authority that called out for the development of DES?

b) In which year DES was standardised?

c) Which authority also was said to have influenced the standardisation of DES?

d) Which company did submit the cipher?

e) Which kind of structure is used in Lucifer?

f) Which key length was supported by Lucifer, originally?

2 Basics of block ciphers

a) what meaning does the (balanced) feistel-network have for the processing of data?

b) Point out the characteristics of a feistel-structure related to the encryption and decryption.

c) Claude Shannon says there are two types of primitive Operations so build up strong encryption algorithms. Name and describe these two in a few sentences.

3 Avalanche effect in DES

a) Which S-boxes are influenced by this bit in the first round. Also calculate the input bits of all S-boxes.

b) Calculate the bit string at the end of the first round. (L1 und R1)

c) Calculate the output bits for the case that all input bits are zeros! (x25=0). How many bits did change in L1 and R1 compared to exercise b)?

4 Non-linearity of S-boxes

a) x1 = 000001, x2 = 100000

b) x1 = 001100, x2 = 111001

c) x1 = 010011, x2 = 011110

5 Brute-Force Attacke auf den DES

a) How many chips of this kind do we have to run parallel so we can calculate the DES-Key in a single day?

b) How much would these chips cost if one chip costs 10 Euro and we calculate 100% overhead for running the chips parallel, the power supply and anything else?

c) Why is this design of such a key searching machine only the upper limit of security?

6 DES bit complement