Exercise 4

Module 1 - Introduction to Cryptography and Data Security

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

May 30, 2017

Contents

1 Encryption with different modes of operation

a) ECB

b) CBC und IV = 11001

c) CFB und IV = 11001

d) CTR und IV = 11001

e) OFB und IV = 11001

2 Fault propagation

a) Assume that an error occurred in the cipher block y_i while the transmission. Which plain text blocks are affected on Bobs side when we are using the ECB mode?

b) Again there is a mistake in block y_i while transmission this time we are using the CBC mode which plain text blocks are affected now?

c) Assume not that in the plaintext block x_i on side on Alice happened. Which blocks are affected by this error if we use CBC mode?

d) What happens if we loose one block while transmitting the data? Consider the cases that it was noticed that one block is missing and that is was not. Which blocks are affected if we use CBC mode?

3 Euclidean algorithm : calculation of the gcd

a) a = 12903; b = 11594

b) a = 525252; b = 691041

c) n = 2689, m = 4001

4 Euclidean algorithm : multiplicative inverse

a) Calculate the inverse elements in Zm for the following a modulo m:

a).1 a = 1215, m = 3094

a).2 x = 1005; m = 364

a).3 a = 154; m = 543

a).4 x = 2951; m = 4854

b) Which condition must be fulfilled so that an inverse a^{-1} exists?

5 Square and multiply

a) x = 3, e = 45, m = 107

b) x = 5, e = 68, m = 107

c) x = 8; e = 55; m = 191

d) x = 7; e = 102; m = 191