Prof. Dr. Rudolf Mathar, Dr. Arash Behboodi, Jose Leon

Exercise 6

Friday, June 3, 2016

Problem 1. (*AES encryption errors*) A sequence of message blocks is encrypted with AES in the modes ECB, CBC, OFB, CFB, and CTR. The ciphertext is sent from Alice to Bob over a channel with random transmission errors.

a) Bob wants to decrypt the ciphertext. Assume that exactly one bit in one block of the ciphertext changes during transmission. How many bits are wrongly decrypted in the worst case?

b) What happens, if one bit of the ciphertext is lost or an additional bit is inserted?

Problem 2. (*AES mix columns*) The step `MixColumns` of the AES scheme is given by $\boldsymbol{r} = \boldsymbol{T}\boldsymbol{c}$ with input $\boldsymbol{c} = (c_0, c_1, c_2, c_3)' \in \mathbb{F}_{2^8}^4$, output $\boldsymbol{r} = (r_0, r_1, r_2, r_3)' \in \mathbb{F}_{2^8}^4$, and the circulant matrix

$$\boldsymbol{T} = \begin{pmatrix} x & (x+1) & 1 & 1 \\ 1 & x & (x+1) & 1 \\ 1 & 1 & x & (x+1) \\ (x+1) & 1 & 1 & x \end{pmatrix} \in \mathbb{F}_{2^8}^{4\times 4},$$

for the polynomial field $\mathbb{F}_{2^8} = \mathbb{F}_2[X]/(x^8 + x^4 + x^3 + x + 1)\mathbb{F}_2[X]$.

Show $(c_3u^3 + c_2u^2 + c_1u + c_0)((x+1)u^3 + u^2 + u + x) \mod (u^4 + 1) = r_3u^3 + r_2u^2 + r_1u + r_0$.

Problem 3. (*AES round key*) Consider the following AES-128 key given in hexadecimal notation:

$$K = 2D\ 61\ 72\ 69\ 65\ 00\ 76\ 61\ 6E\ 00\ 43\ 6C\ 65\ 65\ 66\ 66$$

a) What is the round key K_0?

b) What are the first 4 bytes of round key K_1?

Problem 4. (*Triple DES*) Suppose Triple DES is performed by choosing two keys K_1, K_2 and computing $E_{K_1}(E_{K_2}(E_{K_2}(m)))$. Note that the order of the keys has been modified from the usual two-key version of Triple DES.

Show how to obtain the correct two separate keys K_1 and K_2 with a chosen-plaintext attack and brute-force attack.