T-79.4502 Cryptography and Data Security (5 cr)
T-110.5210 Cryptosystems (5 cr)

Students of the course T-110.5210 Cryptosystems (4 cr): Give answers to at most four (4) problems. Please, mark clearly that your exam is for 4 credits only!

EXAM
Wednesday, December 17, 2014

1. (6 pts) In the round key expansion procedure, AES uses 8-bit constants C_i, $i = 1, 2, 3, ..., 30$ that can be computed as

$$C_i = 2^{i-1} \quad = x^{i-1}$$

in polynomial arithmetic modulo $m(x) = x^8 + x^4 + x^3 + x + 1$, that is, in Galois field $GF(2^8)$ with polynomial $m(x)$. Compute C_{10}, C_{11} and C_{20}.

2. (6 pts) Let us consider a 4-bit S-box S defined as follows:

x	$S(x)$
0 = 0000_2	a = 1010_2
1 = 0001_2	6 = 0110_2
2 = 0010_2	9 = 1001_2
3 = 0011_2	0 = 0000_2
4 = 0100_2	c = 1100_2
5 = 0101_2	b = 1011_2
6 = 0110_2	7 = 0111_2
7 = 0111_2	d = 1101_2
8 = 1000_2	f = 1111_2
9 = 1001_2	1 = 0001_2
a = 1010_2	3 = 0011_2
b✓ = 1011_2	e = 1110_2
c✓ = 1100_2	5✓ = 0101_2
d = 1101_2	2 = 0010_2
e = 1110_2	8 = 1000_2
f = 1111_2	4 = 0100_2

Given two 4-bit keys K_1 and K_2 and a 4-bit plaintext x we define an encryption function e_{K_1,K_2} such that

$$e_{K_1,K_2}(x) = S(S(x \oplus K_1) \oplus K_2).$$

An adversary sees two plaintexts $x = 0$ and $x = 1$ and the corresponding ciphertexts

$$e_{K_1,K_2}(0) = \mathtt{e} \text{ and } e_{K_1,K_2}(1) = 5.$$

Find secret keys K_1 and K_2 using the Meet-in-the-Middle method and the look-up table of S. Is the solution K_1 and K_2 unique?

3. (a) (3 pts) Describe the operation of the Counter (CTR) mode of a block cipher.

   (b) (3 pts) Block cipher in CTR mode can be regarded as a key stream generator to be used as a stream cipher. Once initialized, how many steps does it take this keystream generator to be back in its initial state? What is the length of the period in bits of the key stream sequence of such a stream cipher?

4. Consider the RSA cryptosystem with modulus $n = 31 \cdot 43 = 1333$.

   (a) (3 pts) Compute the private decryption exponent d using public encryption exponent $e = 257$.

   (b) (3 pts) Encrypt the plaintext $m = 32$.

5. Alice and Bob are using the Diffie-Hellman key exchange method in the multiplicative group $\mathbb{F}_{17}^*$ with a generator element $g = 3$. Unfortunately their communication channel is not properly authenticated and Mallory interferes in their communication and performs a Man-in-the-Middle attack. Mallory uses the same $x = 4$ as his private exponent to compute his public keys he sends to Alice and Bob.

   (a) (3 pts) This choice of Mallory restricts the possible Diffie-Hellman session keys that can result from Alice's and Bob's computation. Which are the possible values?

   (b) (3 pts) Alice sends her public key $A = 10$ and Bob sends his public key $B = 11$. Compute the Diffie-Hellman session keys of Alice and Bob. Explain what happens when Alice sends messages to Bob encrypted using her session key?

Exam Calculator Policy. It is allowed to use a function calculator, however no programmable calculator.