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

Thursday, February 19, 2015

1. The field $\mathbb{F}_{2^5}$ can be constructed as $\mathbb{F}_2[x]/\langle x^5 + x^2 + 1\rangle$, where addition and multiplication is computed modulo the polynomial $x^5 + x^2 + 1$.
   (a) (2 pts) Compute $(x^4 + x^2) \cdot (x^3 + x + 1)$ in this field.
   (b) (4 pts) Use the Extended Euclidean Algorithm to compute the multiplicative inverse of $x^4 + x^3 + 1$ in this field.

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

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

   Given a 4-bit key K and a 4-bit plaintext x an encryption function e_K is defined as follows

$$e_K(x) = S(S(x \oplus K) \oplus K).$$

   An adversary sees a plaintext $x = 0110$ and the corresponding ciphertext $e_K(0110) = 0100$. Find the secret key K. Is the solution K unique?

3. Consider the following Boolean function of three binary variables a, b, c

$$f(a, b, c) = ab + bc + ac,$$

   where '+' is the addition modulo 2 and $ab = 1$ if and only if $a = b = 1$.
   (a) (2 pts) Show that the probability that $f(a, b, c) = 0$ is equal to $1/2$, that is, the function $f(a, b, c)$ take value 0 and 1 equally many times as the input (a, b, c) takes all possible values.
   (b) (2 pts) Show that the probability that $f(a, b, c) = a$ is equal to $3/4$.
   (c) (2 pts) Assume that such a function has been used in a stream cipher construction to combine three secret sequences and that the set of possible first input sequences is known to the attacker. The attacker observes the output sequence. Explain how the attacker can use the property (b) to find the correct first input sequence.

4. (6 pts) Consider a hash function h which uses AES encryption operation E_K with 128-bit key K as a compression function to compute the chaining value H_i as follows:

$$\begin{aligned} H_0 &= IV \\ H_i &= E_{M_i}(H_{i-1}), \text{ for } i = 1, 2, ..., \ell, \end{aligned}$$

   where IV is a fixed known 128-bit initial value, and the message M is presented as a sequence of ℓ blocks M_i of 128 bits each. As usual, we set $h(M) = H_\ell$. Given a hash value H show that it takes roughly about 2^{64} steps of computation and about the same amount of memory to find a message of two blocks $M = M_1||M_2$ such that $h(M) = H$. Hint: Use meet-in-the-middle technique. Is h a good hash function?

5. Consider the RSA cryptosystem with modulus $n = 101 \cdot 131 = 13231$.
   (a) (2 pts) A random number generator produces two random numbers: 1323 and 4563. Show that 4563 is not a suitable value for the public encryption exponent e. Explain.
   (b) (2 pts) Compute the private decryption exponent d using $e = 1323$.
   (c) (2 pts) Decrypt the ciphertext $c = 202$ using the Chinese Remainder Theorem and the knowledge of the prime factors of the modulus.

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