CS-E4320 Cryptography and Data Security (5 cr)

EXAM
Wednesday, December 13, 2017

This is a 30 point exam.

1. (3 pts) Answer the following questions:
   (a) (1 pt) Describe the One Time Pad (OTP) algorithm. What are the limitations of this cipher? Give one alternative cipher?
   (b) (1 pt) Given a hash function with tags of length b bits. What is collision attack? What is the generic complexity of this attack?
   (c) (1 pt) Describe the three Generals problem in the context of secret sharing.
2. (3 pts) Given a 4-stage LFSR with connection polynomial $c(x) = 1 + c_1x + c_2x^2 + c_3x^3 + c_4x^4$, $c_i \in \{0, 1\}$.
   (a) (2 pts) Given the sequence `01100100` generated by this LFSR, what is the value of the coefficients c_i?
   (b) (1 pt) Draw the corresponding LFSR.
3. (6 pts) We consider blocks of 128 bits and a hash function H which tags messages M of n blocks ($M = M_1||M_2 \cdots ||M_n$) as $H(M) = AES_0(M_1) \oplus AES_0(M_2) \oplus \cdots \oplus AES_0(M_n)$, where AES_0 denotes the AES block cipher encryption function with the key 0.
   (a) (3 pts) Can we generate a preimage for messages $M = M_1$ of one block? Explain your solution.
   (b) (3 pts) Given a message $M = M_1||M_2$ and its hash value $h = H(M)$, how many messages $M' = M_1'||M_2'$ of length two blocks have the same hash value?
4. (3 pts) Solve the equation $7x = 1 \pmod{131}$.
5. (3 pts) Use the CRT to solve the following system:
$$\begin{cases} x = 15 \mod 31 \\ x = 8 \mod 37. \end{cases}$$
6. (3 pts) We consider the Diffie-Hellman key exchange protocol over $\mathbb{F}_{2^5} = \mathbb{F}_2[x]/ < x^5+x^2+1 >$. The primitive element chosen in the scheme is $\alpha = x^2$. The private keys are $a = 3$ and $b = 12$. What is the session key k_{AB}?
7. (9 pts) We consider the RSA public key cipher. The public key of Bob_1 is $(e_1 = 5, N = 221)$. The public key of Bob_2 is $(e_2 = 13, N = 221)$. Alice want to send the message m to both Bob_1 and Bob_2. We denote the corresponding ciphertexts c_1 and c_2.
   (a) (2 pts) Use the Extended Euclidian algorithm to find u and v such that $5 \cdot u + 13 \cdot v = 1$.
   (b) (2 pts) Given $c_2 = 214$, compute $c_2^2 \bmod 221$.
   (c) (2 pts) Given $c_1 = 41$, check that $m = c_2^2 \cdot c_1^{-5}$. (HINT: $c_1^{-5} = 167$)
   (d) (3 pts) Explain why Eve is able to recover the message m without knowing the private exponents d_1 and d_2.

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