Cryptography and Architectures for Computer Security

Exam Code: 095947 (old 090959), A.Y. 2014–2015, Semester: 2

Prof. G. Pelosi

September 30th, 2015 – Exam Session

Name: ..... Surname: .....

Student ID: ..... Signature: .....

Time: 2h:30'. Use of textbooks, notes, phones or Internet connected devices is not allowed. Prior to turn in your paper, write your name on any additional sheet and sign it.

Question 1 [4 pts]
Consider the four basic modes of operations of block ciphers (ECB, CBC, OFB, CFB). For all four modes of operation analyze the effect on the decryption of remaining blocks if, for the sequence of ciphertext blocks $c_1, c_2 \ldots, c_n$, one ciphertext block c_j $(0 \leq j < n)$ is erroneous.
Specify which plaintext blocks $x_j x_{j+1}, \ldots$ are computed correctly.

Question 2 [2 pts]
One of the recommendations for a proper use of "One-time pad" (to ensure perfect secrecy) is to never reuse the same key for encryption of two different messages. The simplest way to implement it is to generate a random key sequence of the same length as message and to encrypt using, $C_i = M_i + K_i \bmod 26$ where K_i are random key symbols and $\mathcal{M} = \mathcal{K} = \mathcal{C} = \mathbb{Z}_{26}$.
Explain how the knowledge of two different ciphertext sequences $C_1 C_2 \ldots$ and $C'_1 C'_2 \ldots$ obtained by applying the same secret key, can compromise the security of the system.

Question 3 [4 pts]
Digital signature, developed using public key cryptography, is a means for communication counterparts in cyberspace to authenticate themselves to each other. Briefly describe the trust model adopted in an X.509 standard Public Key Infrastructure (PKI) and the trust model underlying the use of the Pretty Good Privacy (PGP) system.

Question 4 [6 pts]

(a) Consider the finite field $\mathbb{F}_{5^2}$

(a.1) Write the number of irreducible and primitive polynomials.

(a.2) Check if $f_1(x) = x^2 - 3x + 2 \in \mathbb{F}_5[x]$ and $f_2(x) = x^2 + 3x + 3 \in \mathbb{F}_5[x]$ are primitive polynomials. Show all the roots of the primitive polynomials.

(b) Consider the cyclic group $(\mathbb{Z}_{25}^*, \cdot)$

(b.1) Show the order of the group and the number of generators.

(b.2) Exhibit the order and the value of at least one generator for each subgroup.

(c) What are the public parameters of a Diffie-Hellmann key agreement scheme and how should they be generated in case a generic finite field $\mathbb{F}_{p^k}$ arithmetics is employed?

Question 5 [6 pts]

The so called S-box (Substitution box) is widely used cryptographic primitive in symmetric-key cryptosystems.

(a) In AES (Advanced Encryption Standard) the 16 S-boxes in each round are identical. All these S-boxes implement the inverse function in the Galois Field $\mathbb{F}_{2^8}$. Such a function can also be seen as a mapping $S : \{0,1\}^8 \mapsto \{0,1\}^8$ such that 8 input bits are mapped to 8 output bits:

$$S : x \in \mathbb{F}_{2^8} \mapsto x^{-1} \in \mathbb{F}_{2^8}$$

What is the total number of possible mappings one can specify for function S?
What is the total number of possible bijective mappings one can specify for function S?

(b) Construct the Galois field of 16 elements $\mathbb{F}_{2^4}$, using a primitive polynomial $f(x) = x^4 + x + 1 \in \mathbb{F}_2[x]$. Compute the powers x^i, $0 \leq i \leq 14$ and represent these powers (multiplicative group) as either polynomials of the form $a_0 + a_1 x + a_2 x^2 + a_3 x^3$ or tuples (a_0, a_1, a_2, a_3).

(c) Assume we want to implement an S-box using the Galois $\mathbb{F}_{2^4}$.

If we would like that our S-box is bijective (like the one employed in the AES cipher) is it a good choice to use one of the functions

$$S_1 : x \in \mathbb{F}_{2^4} \mapsto x^3 \in \mathbb{F}_{2^4}$$

$$S_2 : x \in \mathbb{F}_{2^4} \mapsto x^4 \in \mathbb{F}_{2^4}$$

Motivate your answer.

(d) Is the S-box S_2 a good choice for preventing linear and/or differential cryptanalyses? Motivate your answer.

Question 6 [12 pts]

(a) Describe the Fermat primality test and the Miller-Rabin primality test.

(b) Apply the Pollard's ρ method[1] to factor the RSA public modulus $n = p \cdot q = 527$

(c) A Local Area Network uses a public key infrastructure based on a school-book RSA implementation (without OAEP), with known public modulus $n = 527$. User A and B have public exponents $e_A = 11$ and $e_B = 7$, respectively.

(c.1) Calculate the private exponents of A and B.

(c.2) User C encrypts a message M for both A and B. Assume that an observer sees the ciphertexts $C_A = 13$ and $C_B = 28$ and does not know the secret keys.
Can the observer derive the plaintext message?
Motivate your answer and show every step of the computation.

(d) Explain why the OAEP padding scheme is employed in RSA implementations

(e) Assume to use the Montgomery arithmetics for a software implementation of an RSA cryptosystem. Show the pseudo-code of the encryption and decryption (with CRT) primitives, defining all the appropriate sub-routines.

What are theoretical speedups of these implementations with respect to the school-book implementations of the encryption and decryption functions?

.

[1] as a back-up strategy you can apply a trivial division method