



Cryptography and Architectures for Computer Security

Exam Code: 095947 (old 090959), A.Y. 2017–2018, Semester: 2

Prof. G. Pelosi

January 24th, 2019 – Exam Session

Name: Surname:

Student ID: Signature:

Time: 2h, 30min. Use of textbooks, notes, or Internet connected devices (including smartphones) is not allowed. The usage of simple calculators is allowed. Prior to turn in your paper, write your name on any additional sheet and sign it.

Question 1 [3 pts]

Consider the Vigenere cipher over the lowercase English alphabet, where the key has length 6. For which of the following message spaces will this scheme be perfectly secret? (Check all that apply.)

- (i) The set of all 7-character strings of lowercase English letters.
- (ii) The set of all strings of lowercase English letters containing at most 6 characters.
- (iii) The set of all 6-character strings of lowercase English letters.
- (iv) The set of all 5-character strings of lowercase English letters.

Question 2 [3 pts]

Describe the Web-of-Trust (WoT) concept used in PGP, GnuPG, and other OpenPGP-compatible systems to establish the authenticity of the binding between a public key and its owner. Describe the centralized trust model of a public key infrastructure (PKI), pointing out advantages and disadvantages with respect to WoT.

Question 3 [3 pts]

Consider the following three basic modes of operations of block ciphers: ECB, CBC, and CTR. For each modes of operation analyze the effect on the decryption of remaining blocks if, for the sequence of ciphertext blocks c_1, c_2, \dots, c_n , one ciphertext block c_j ($0 \leq j < n$) is erroneous. Specify which plaintext blocks x_j, x_{j+1}, \dots are computed correctly.

Question 4 [5 pts]

- (a) Consider the cyclic group $(\mathbb{Z}_{64}^*, \cdot)$. Compute the cardinality of the group, the number of its generators and show the order of the element $3 \in \mathbb{Z}_{64}^*$.
- (b) Consider the finite field \mathbb{F}_{2^6} . Find the number of irreducible and primitive polynomials. Determine if $f(x) = x^6 + x + 1 \in \mathbb{F}_2[x]$ is a primitive polynomial and show all its roots.

Question 5 [6 pts]

Consider the group of points over the elliptic curve $\mathbb{E}(\mathbb{F}_{13}) : y^2 = x^3 + 2x$, with order $n = |\mathbb{E}(\mathbb{F}_{13})| = 12$.

- (a) Verify the “non-singularity” of the curve and compute the number of generators of the group.
- (b) Verify that $P = (2, 5)$ is a generator, then compute the coordinates of $Q = -P$ and show its order.
- (c) Discuss the parameter settings and the mathematical security of an elliptic curve cryptosystem employing a group with a composite order.

Question 6 [14 pts]

Consider an RSA cryptosystem

- (a) Apply the Pollard’s rho factorization method to the RSA modulus $n = p \cdot q = 551$ showing each step of the computation.
- (b) Describe the Miller-Rabin primality test and apply it to the factor p employing as bases $a = 3, b = 7$.
- (c) Given the modulus factorization found as answer to (a), and the secret exponent $d=19$,
 - compute the encryption exponent e ;
 - decrypt the message $c=300_{\text{decimal}} \in \mathbb{Z}_n$ (provided without any padding scheme) through applying the CRT. Describe each step of the procedure
- (d) Assume to work into the Montgomery domain: $(\mathbb{Z}_p, +, \times), p = 13$.
Compute the Montgomery multiplication $C=A \times B \bmod p$, where $A=6_{\text{decimal}}$ and $B=3_{\text{decimal}}$ are values in the Montgomery domain. Assume a binary encoding of the operands.
- (e) Show the computational complexity of performing a RSA encryption applying the Montgomery strategy to execute the modular multiplications.
Show the said computational complexity when the Montgomery strategy is applied to operands encoded in Radix-4.