



# Cryptography and Architectures for Computer Security

Exam Code: 095947 (old 090959), A.Y. 2018–2019, Semester: 2

Prof. G. Pelosi

September 6th, 2019

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

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

**Time: 2h, 15min. 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]

You are in charge to decide which of the two following password storage schemes should be used for storing login passwords on a computing platform.

- Accept a password  $p$  with a maximum length of 14, 7-bit ASCII, characters, split it into two halves  $p_1, p_2$ , compute  $\text{SHA-256}^{300}(p_1||\text{salt})$  (i.e., compute  $\text{SHA-256}(\dots\text{SHA-256}(\text{SHA-256}(p_1||\text{salt}))\dots)$ , applying 300 times the  $\text{SHA-256}(\cdot)$  function) and  $\text{SHA-256}^{300}(p_2||\text{salt})$  with a 20 bytes salt and store the two hashes (together with the salts).
- Accept a password  $p$  with a minimum length of 9, 7-bit ASCII, characters and a maximum of 14, compute  $\text{SHA-256}^{300}(p||\text{salt})$  with a 8 bytes salt and store the hash (together with the salt).
- Accept a password  $p$  with a minimum length of 9, 7-bit ASCII, characters and a maximum of 14, compute  $\text{SHA-256}^{300}(p)$  and store the hash.

### Question 2 [3 pts]

Describe the available options to authenticate a user employing the `ssh` protocol and specify proper cipher suites and key-length choices.

### Question 3 [8 pts]

Consider the finite field  $\mathbb{F}_{2^6}$ .

- Verify that  $f(x) = x^6 + x^5 + x^4 + x + 1 \in \mathbb{F}_2[x]$  is a primitive polynomial.
- Let  $\alpha \in \mathbb{F}_{2^6}^* \setminus \mathbb{F}_2$  be a root of  $f(x)$ .  
What is the order of  $\beta = \alpha^{15}$ ? Compute  $\gamma = \alpha^{-127} \in \mathbb{F}_{2^6}$ .
- Assuming  $\mathbb{F}_{2^6} \cong \mathbb{F}_2[x]/(f(x))$ , state which one(s) among the following discrete logs exist, justifying your answer both in the positive and in the negative case.  
 $x \equiv \log_{\alpha^{21}}(\alpha^9) \pmod{|\alpha^{21}|}$ ,  $y \equiv \log_{\alpha^9}(1) \pmod{|\alpha^9|}$ ,  $z \equiv \log_{\alpha^9}(\alpha^{-9}) \pmod{|\alpha^9|}$ .
- Describe what are the known algorithms to solve a discrete logarithm, specifying their computational complexity.

**Question 4 [8 pts]**

Consider an Elliptic Curve (EC) defined by the following equation:

$$\mathbb{E}(\mathbb{F}_7) : y^2 = x^3 + 3$$

- (a) Show the coordinates of all points on  $\mathbb{E}(\mathbb{F}_7)$ , the order of the group,  $m=|\mathbb{E}(\mathbb{F}_7)|$ , and point out the number of primitive elements.
- (b) In order to verify the following equality:  $[m]A=\mathcal{O}$ ; compute the scalar multiplication  $[m]A$ , with  $A=(3,4)$ , through applying a *double-and-add* strategy.

One of the end-points of a communication, say Bob, publishes the equation of the curve  $\mathbb{E}(\mathbb{F}_7)$  and its own EC-ElGamal public-key  $k_{\text{pub}}=\langle n, A, [k_{\text{priv}}]A \rangle$ , where  $n$  is the prime factor of  $m$  and  $A=(3,4)$ . Obviously, Bob keeps secret its private-key  $k_{\text{priv}}=3\in\mathbb{Z}_n$ .

The other communicating party, say Alice, wishes to send the binary message,  $\text{msg}=(101)_{\text{bin}}$ , to Bob and chooses a nonce  $r=4$ .

- (c) Show the ciphertext value,  $\langle \gamma, \delta \rangle$ , transmitted by Alice; and show how Bob get the plaintext.
- (d) Explain why elliptic curve based cryptosystems exhibit public key sizes smaller than both RSA public keys and ElGamal-based public keys when the security guarantees of the mentioned systems in terms of mathematical strength are the same.

**Question 5 [12 pts]**

- (a) Apply the Fermat's factorization method to the RSA modulus  $n = p \cdot q = 551$  showing each step of the computation (As a backup strategy apply a trivial division strategy).

(Hint) The last two decimal digits of a perfect square can be found among the following values: 00, e1, e4, 25, o6, and e9, where 'e' stands for an even decimal digit and 'o' for an odd decimal digit.

- (b) Describe the Miller-Rabin primality test, and show its application to the greatest factor of  $n$ , with base  $a = 3$ .
- (c) Let  $e=5_{\text{dec}}$  be the public exponent of a RSA public-key  $k_{\text{pub}}=\langle e, n \rangle$ . Knowing the factorization of the modulus  $n$ , compute the value of the corresponding RSA private-key  $k_{\text{priv}}=\langle p, q, \varphi(n), d \rangle$ . Show every step of the computation.
- (d) Decrypt the message  $c=550_{\text{dec}}\in\mathbb{Z}_n$  (provided without any padding scheme) through applying the CRT. Describe each step of the procedure.
- (e) Assume to work into the Montgomery domain:  $(\tilde{\mathbb{Z}}_p, +, \times)$ ,  $p = 19$
- Compute the Montgomery multiplication  $C=A\times B \bmod p$ , where  $A=13_{\text{dec}}$  and  $B=4_{\text{dec}}$  are values in the Montgomery domain. Assume a binary encoding of the operands.
  - Explain the reasons to employ a Montgomery-based arithmetic for the efficient implementation of RSA or discrete log.-based cryptosystems.