
# Cryptography and Architectures for Computer Security

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

**Prof. G. Pelosi**

**September 13th, 2018 – Exam Session**

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

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

**Time: 2h:30'. 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.**

**Question1 [3 pts]**
Consider the TLS protocol answer the following questions:

**(a)** Can an *active* attacker break the confidentiality property of a TLS connection if the ciphersuites accepted by both the client and the server include insecure choices? How?

**(b)** Consider the TLS ciphersuites `TLS_DHE_ECDSA_WITH_AES_256_SHA256`, using an ECDSA keypair relying on the P-521 curve and `TLS_DHE_ECDSA_WITH_AES_192_SHA384` using an ECDSA keypair relying on the P-384 curve. Which one provides the most homogeneous security margin across all the primitives?

**Question 2 [5 pts]**
Consider a password hashing scheme composed as follows: given a 7 printable ASCII (also known as 7-bit ASCII) character password and a single byte salt, the concatenation of the password and the salt is hashed 1024 times with SHA-2-512. The result is stored, together with the salt, as the password hash.

**(a)** Considering a CPU able to compute $2^{23}$ SHA-2-512 hashes per second, and the availability of 128GiB of RAM, compute the chain length of a rainbow table aimed at breaking the aforementioned password hashing scheme minimizing the computation time for a worst case lookup. Calculate the time required to compute the rainbow table, not taking into account the memory access time. Do not take into account the space required for the index or other data structure required to access the table in $O(1)$.

**(b)** Patch the password hashing scheme adding enough salt so that the aforementioned attack requires at least $2^{128}$ SHA-2-512 computations.

**(c)** Is it possible to find whether a user's password is "password" followed by his date of birth when employing your patched scheme?

**Question 3 [3 pts]**
Describe the design principles of a stream cipher, mentioning its most common structures.

**Question 4 [5 pts]**
Consider the finite field $\mathbb{F}_{2^4}$.

**(a)** Compute the number of irreducible and primitive polynomials that can be employed to represent the elements of the field.

**(b)** Exhibit the value of all primitive polynomials, justifying your answer.

**Question 5 [5 pts]**

**(a)** Consider an instance of the Diffie-Hellmann protocol over the multiplicative group $G = (\mathbb{F}^*_{11^2}, \cdot)$. Considering the primitive polynomial $f(x) = x^2 + 1 \in \mathbb{F}_{11}[x]$, the elements of the field are represented as first degree polynomials of the form $\theta_1\alpha+\theta_0$ with $\theta_0, \theta_1 \in \mathbb{F}_{11}$, and $\alpha \in \mathbb{F}_{11^2} \backslash \mathbb{F}_{11}$ such that $\alpha^2 \equiv -1$.

State if the following discrete logarithms exists and, in the positive case, compute their values.

$$x_1 = \log^{\mathtt{D}}_{\alpha}(-1),\ x_2 = \log^{\mathtt{D}}_{1/\alpha}(-1)$$

**(b)** Many implementations of the Diffie-Hellman protocol assume to work in a subgroup $G$ of the multiplicative group $(\mathbb{Z}_p, \cdot)$; in order to simply the implementation is it a good idea to employ a subgroup of the $(\mathbb{Z}_p, +)$, with the same prime $p$?. How is security affected?

**Question 6 [14 pts]**

**(a)** Apply the Pollard's $\rho$ method to factorize the RSA modulus $n = p \cdot q = 551_{\text{dec}}$.
Assume $f(x) = x^2 + 1 \bmod n$ as the "random-walking" function. Show every step of the computation. (As a backup alternative, apply a "trivial division" strategy).

**(b)** Describe the Pollard's $P - 1$ factoring algorithms, pointing out its computational complexity.

**(c)** Given the values $e_1 = 9$, $e_2 = 11$ state which of them is an admissible public exponent, motivating your answer. Show the value of the corresponding RSA public and private keys $k_{\text{pub}}$=$(e, n)$, $k_{\text{priv}}$=$(p, q, \varphi(n), d)$.

**(d)** Sign the message $m$=$256_{\mathtt{dec}} \in \mathbb{Z}_n$ (without employing any padding scheme) through applying the CRT. Describe each step of the procedure.

**(e)** Consider a schoolbook RSA cryptosystem employing the Montgomery multiplication as building block. Write down the pseudo code of both the encryption and the CRT-based decryption transformations, pointing out their asymptotic computational complexities.

**(f)** Consider the modulus $N = 29_{\text{dec}}$ and the value $A = 6_{\text{dec}}$. Assuming a binary encoding of the operands and the smallest possible value for the Montgomery radix $R$

- compute the value $\widetilde{A}$ that is the result of mapping $A$ into the Montgomery domain;
- apply the Montgomery multiplication algorithm to compute $\widetilde{A}^2$.

Show every step of the computations.