Cryptography and Architectures for Computer Security

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

Prof. G. Pelosi

July 17th, 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.

Question 1 [4 pts]
Consider the case of a per-file data-at-rest encryption, where a single block cipher key is employed for every file.

(a) From a performance standpoint, which mode of operation would you choose between CBC and CTR for encrypting/decrypting each file in the mentioned scenario?

(b) From a security standpoint, which mode of operation would you choose between CBC and CTR? (Hint: Distinguish the case where the `IV`s of two files are different from the one where they match...)

Question 2 [4 pts]
Consider the following two password hashing schemes:

1. Accept a seven lowercase alphabetic character password. Draw a random salt s, 32b in length, compute $h = \text{SHA-2-256}(s||\texttt{password}||s)$. Store $h||s$.
2. Accept seven lowercase alphabetic strings drawn at random from an English dictionary with 65536 terms. Compute $h = \text{SHA-2-256}(s_1||s_2||s_3||s_4||s_5||s_6||s_7)$ and store h

Argue which one of the two password schemes can be fruitfully attacked with a time to memory tradeoff such as a rainbow table. For the said scheme, compute the chain length of a rainbow table, assuming to have 16 GiB of available storage, and employing a storage strategy which has no overhead save for storing the table data (i.e., omit any storage requirement for the indexing). Considering the time to compute SHA-2-256 to be 100μs, and the time to perform a table lookup to be 1μs, compute the worst case password finding time.

Question 3 [3 pts]
Considering the Tor transport anonymity protocol:

1. What is the working principle providing transport anonimity in the Tor relay network?
2. When is a malicious relay able to selectively drop the relay cells belonging to the circuit of a specific client connected to the Tor network?

Question 4 [10 pts]

(a) Consider an instance of the Diffie-Hellmann protocol with public parameters described as follows: $G \subseteq (\mathbb{Z}_{7^3}^*, \cdot)$, $G = \langle g \rangle$. Compute the cardinality of the group, the number of its generators and the number of subgroups.

(b) Consider an instance of the Diffie-Hellmann protocol with public parameters described as follows: $G \subseteq (\mathbb{F}_{7^3}^*, \cdot)$, $G = \langle g \rangle$. Compute the cardinality of the group, the number of its generators and the number of subgroups.
Find the number of irreducible and primitive polynomials that can be employed to represent the field elements.
Determine if $f(x) = x^3 - x - 1 \in \mathbb{F}_7[x]$ is reducible or not.

(c) Keeping into account the Pohlig-Hellman attack, which cyclic group between $(\mathbb{Z}_{7^3}^*, \cdot)$ and $(\mathbb{F}_{7^3}^*, \cdot)$ is preferable?

Question 5 [14 pts]

(a) Apply the Pollard's ρ method to factorize the RSA modulus $n = p \cdot q = 851_{\text{dec}}$.
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 $e_1 = 3 \cdot 5$, $e_2 = 5^2$ state which of them is an admissible public exponent, motivating your answer. Show the value of the corresponding RSA public and private keys k_{pub}=(e, n), k_{priv}=$(p, q, \varphi(n), d)$.

(d) Sign the message m=$111_{\texttt{dec}} \in \mathbb{Z}_n$ (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 $N = 23_{\text{dec}}$ and the value $A = 17_{\text{dec}}$. 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.