Cryptography and Security of Digital Devices

Exam Code: 095947 (old 090959), A.Y. 2019–2020, Semester: 2

Prof. G. Pelosi

February 18th, 2020 – Exam Session

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

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

Time: 2h:15'. Use of textbooks, notes, internet connected laptops (or any other devices) and of software tools is not allowed. Pencil writing is allowed.
Write your name on any additional sheet and sign it.

Question 1 [2 pts]

An X.509 certificate for `foo.com` includes the 256 bit RSA public key for the aforementioned common name, and its MD5 hash signed with 512 bit RSA by Faust Certification Authority inc. Alice's browser contains a valid, trusted root CA certificate for Faust CA inc.

(a) Highlight which are Alice's concerns (all of them) toward the security of a possible TLS communication with foo.com, instantiated with the aforementioned X.509 certificate.

Question 2 [6 pts]

Rosen Association inc. mandates the use of encrypted disk volumes for its own employees enforcing the following:

- All the disks have two partitions, one containing the OS binaries (with a non-integrity checking filesystem), while the other hosts the employee data. The OS partition is to be encrypted with AES-256-CBC with a randomized IV when the partition is created, while the user data partition (i.e., the employee partition) should employ AES-256-CTR, using the string "NEXUS6-ROSENInc." as IV.
- All the employee partitions are set up by the system administrator which, during formatting, takes care to fill the space within the encrypted volume with zeroes, so to fill the effective physical diskspace with random data.
- The employees are enforced to pick their disk encryption passwords as 16 character random strings containing decimal digits. The password is hashed through SHA-2-256 to fill in the AES-256 key.

(a) Discuss the choices of Rosen inc. concerning the choice of the encryption algorithm for the OS partition, highlighting issues and proposing a way to fix them.

(b) Discuss the choice of the encryption algorithm for the employee partition, and the decision of the system adminstrator to wipe the internal space of the disk volume.

(c) Discuss the password policy chosen by Rosen, providing a quantitative estimate for the attacker effort to be spent to completely break the whole system, in the most efficient way possible

Question 3 [2 pts]

A company is employing keyed RIPEMD-64 hashes (64-bit digest) as an integrity checking mechanism for files on a disk. The security officer is currently concerned with the security margin against intentional replacement of files with garbage data and suggests to change the keyed hashing mechanism to SHA-2-256. The commercial department points out that employing SHA-2-256 would increment the amount of required disk space and, to reduce the migration costs, proposes to employ SHA-2-256 to hash the file contents, and store only the first quarter of the digest for integrity checking.

(a) Is the security officer concern well justified? Provide a quantitative motivation to it.

(b) Is it possible to adopt the commercial department solution? Justify quantitatively the answer.

Question 4 [4 pts]
Consider the finite field $\mathbb{F}_{2^6}$.

(a) Show the number of irreducible polynomials that can be used to represent the field elements.

(b) Show the number of primitive polynomials that can be used to represent the field elements.

(c) Verify that $f(x)$=$x^6 + x + 1$ is a primitive polynomial.

Question 5 [6 pts]
Consider the following relation: $11 \equiv 2^x \bmod 13$.

(a) Compute the discrete logarithm $x \equiv_{\varphi(13)} \log_2^{\mathrm{D}} 11$ applying the Pohlig-Hellman method.

(b) Show the computational complexity of the Pohlig-Hellman algorithm. When is it appropriate to use this method?

Question 6 [12 pts]

(a) Consider the RSA modulus $n = p \cdot q = 713 = 23 \cdot 31$

- Apply the Miller-Rabin primality test to the factor p employing as bases $a = 3$, $b = 7$.
- Given the public exponent e=$7 \in \mathbb{Z}^*_{\varphi(n)}$, show the value of the RSA private key, k_{priv}=$(p, q, \varphi(n), d)$ and specify every step of the computation.
- Apply a Right-to-Left Square & Multiply strategy to compute the ciphertext $c_1 = m^{13} \bmod n$, with $m = 101 \bmod n$ employing a radix-2 encoding of the exponent, and apply a Left-to-Right Square & Multiply strategy to re-compute the same value employing a radix-4 encoding of the exponent.

(b) Assume to work into the Montgomery domain: $(\widetilde{\mathbb{Z}}_p, +, \times),\ p = 23$

- Show the working principle of the Montgomery Multiplication and the smallest admissible value for the Montgomery Radix: R

- Exhibit the values R', p' that satisfy the relation: $\gcd(R,p){=}R\,R'{-}p\,p'{=}1$, justifying the procedure
- Compute the Montgomery multiplication $\widetilde{C} = \text{MonPro}(\widetilde{A},\widetilde{B}) = \widetilde{A} \times \widetilde{B} \times R^{-1} \bmod p$, where $\widetilde{A} = 16_{\text{dec}}$ and $\widetilde{B} = 11_{\text{dec}}$, assuming a binary encoding of the operands.