Cryptography and Architectures for Computer Security

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

Prof. G. Pelosi

July 24th, 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 [4 pts]

(a) 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.

- 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.

(b) A company is employing 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 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.

- Is the security officer concern well justified? Provide a quantitative motivation to it.
- Is it possible to adopt the commercial department solution? Justify quantitatively the answer.

Question 2 [6 pts]

Consider the sequence $\{w_i\}_{i\geq 0} = \{s_i \oplus t_i\}_{i\geq 0}$, where: $\{s_i\}_{i\geq 0}$ is generated by the LFSR with characteristic[1] polynomial $1 + x + x^2$, and
$\{t_i\}_{i\geq 0}$ is generated by the LFSR with characteristic polynomial $1 + x + x^3$.

(a) What are the periods of $\{s_i\}_{i\geq 0}$ and $\{t_i\}_{i\geq 0}$?

(b) Draw the structure of the keystream generator corresponding to $\{w_i\}_{i\geq 0}$

(c) What are the possible periods of the sequence $\{w_i\}_{i\geq 0}$ and why?

[1] the *characteristic polynomial* $G(x)$ of an LFSR with length L is related to the *Connection polynomial*, $C(x)$, through the following relations: $G(x) = x^L C(x^{-1})$ and $C(x) = x^L G(x^{-1})$.

Question 3 [8 pts]
Consider the finite field $\mathbb{F}_{2^6}$.

(a) Establish if $f(x) = x^6 + x^2 + 1 \in \mathbb{F}_2[x]$, $g(x) = x^6 + x^3 + 1 \in \mathbb{F}_2[x]$ are irreducible and/or primitive polynomials.

(b) Let $\beta{=}\alpha{+}1$ be a generator of $\mathbb{F}^*_{2^6}$, where $\mathbb{F}_{2^6}{\cong}\mathbb{F}_2[x]/(g(x)){\cong}\mathbb{F}_2(\alpha)$, with $\alpha{\in}\{\mathbb{F}_{2^6}\backslash\mathbb{F}_2\}$ and $g(\alpha) = 0$. Show the generators of each subgroup of $(\mathbb{F}^*_{2^6}, \cdot)$.

(c) Compute the following discrete logarithm:
$m \equiv \log^{\mathtt{D}}_{\alpha+1}(\alpha^5 + \alpha^2) \bmod |\alpha + 1|$, applying the BSGS method.

Question 4 [6 pts]
Explain briefly why elliptic curve based cryptosystems usually provide shorter keys with respect to RSA or discrete log systems employing a modular integer arithmetic.
Consider the elliptic curve $y^2 = x^3 + 6x + 3$ over $\mathbb{Z}_{11}$

(a) How many points lie on it ?

(b) What is the sum of the points (4, 5) and (5, 9)?

Question 5 [6 pts]
(a) Apply the Pollard's ρ method to factorize the RSA modulus $n = p \cdot q = 713$.
Assume $f(x) = x^2 + 1 \bmod n$ as "random-walking" function.
Show every step of the computation.
(As a backup alternative, apply a "trivial division" strategy).

(b) Choose an admissible public exponent e between the values $e = 11_{\mathtt{dec}}$ and $e = 13_{\mathtt{dec}}$ and compute the value of the corresponding RSA private key $k_{priv} = (p, q, \varphi(n), d)$. Show every step of the computation.

(c) Sign the message $m{=}100_{\mathtt{dec}} \in \mathbb{Z}_n$ (without employing any padding scheme) through applying the CRT. Describe each step of the procedure.

Question 6 [6 pts]
Consider a school-book implementation of the RSA encryption function with $k_{\mathtt{pub}}{=}\langle 3, n\rangle$, $n{=}3{\times}17$; employing the Montgomery arithmetics primitive $\mathtt{MMul}_n(\cdot, \cdot)$.

(a) Write the pseudo-code of an encryption primitive (employing the $\mathtt{MMul}_n(\cdot, \cdot)$) taking as input the public key and a plaintext message in the integer domain.

(b) Show the value $\widetilde{m}$ of $m{=}42 \in \mathbb{Z}_n$ in the Montgomery domain, assuming the smallest value of the Montgomery radix, and show the computation of $\widetilde{m^2} = \mathtt{MMul}_n(\widetilde{m}, \widetilde{m})$ assuming a binary encoding of $\widetilde{m}$.

(c) Show the value of $\widetilde{c}{=}\mathtt{MMul}_n(\widetilde{m^2}, \widetilde{m})$ and the corresponding value of the ciphertext c in the integer domain.