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 SHA-256$^{300}(p_1||\text{salt})$ (i.e., compute SHA-256(...SHA-256(SHA-256$(p_1||\text{salt})$)...), applying 300 times the SHA-256$(\cdot)$ function) and 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 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 SHA-256$^{300}(p)$ and store the hash.

Solution:
The second password scheme is definitely stronger than the first one as an attacker only needs to perform a bruteforce attack over a password space of $(2^7)^7 = 2^{49}$ possible passwords, while the second requires a minimum exhaustive search over a keyspace of $(2^7)^9 = 2^{63}$ to effectively crack the scheme. The third password scheme is as strong as the second, as far as the effort required to bruteforce a single password goes, but is not employing a salt to prevent TMTO-based attacks such as Rainbow tables. As the required bruteforce efforts (2^{63} operations) is within the possibility of large organizations, the use of the salt is required for the password scheme not to be breached.

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.

Solution:
see lectures ...

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

(a) Verify that $f(x) = x^6 + x^5 + x^4 + x + 1 \in \mathbb{F}_2[x]$ is a primitive polynomial.

(b) 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 $\gamma = \alpha^{-127} \in \mathbb{F}_{2^6}$.

(c) 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.
$x \equiv \log_{\alpha^{21}}^{\mathtt{D}}(\alpha^9) \bmod |\alpha^{21}|$, $y \equiv \log_{\alpha^9}^{\mathtt{D}}(1) \bmod |\alpha^9|$, $z \equiv \log_{\alpha^9}^{\mathtt{D}}(\alpha^{-9}) \bmod |\alpha^9|$.

(d) Describe what are the known algorithms to solve a discrete logarithm, specifying their computational complexity.

Solution:

(a) $n = |\mathbb{F}_{2^6}^*| = 63 = 3^2 \cdot 7$. Proper divisors of n: 3, 7, 9, 21. if $\alpha \in \mathbb{F}_{2^6} \setminus \mathbb{F}_2$ is a root of $f(x)$ (i.e., $\alpha^6 = \alpha^5 + \alpha^4 + \alpha + 1$) and this polynomial is primitive, then:

$\alpha^3 \not\equiv 1$ (True);

$\alpha^7 \equiv (\alpha^5 + \alpha^4 + \alpha + 1) + \alpha^5 + \alpha^2 + \alpha \equiv \alpha^4 + \alpha^2 + 1 \not\equiv 1$ (True);

$\alpha^9 \equiv (\alpha^4 + \alpha^2 + 1) \cdot \alpha^2 \equiv \alpha^5 + \alpha^4 + \alpha + 1 + \alpha^4 + \alpha^2 \equiv \alpha^5 + \alpha^2 + \alpha + 1 \not\equiv 1$ (True);

$\alpha^{21} \equiv (\alpha^9)^2 \cdot \alpha^3 \equiv \alpha^{13} + \alpha^7 + \alpha^5 + \alpha^3 \equiv \alpha \cdot (\alpha^6)^2 + \alpha^4 + \alpha^2 + 1 + \alpha^5 + \alpha^3 \equiv$
$\alpha \cdot (\alpha^{10} + \alpha^8 + \alpha^2 + 1) + \alpha^4 + \alpha^2 + 1 + \alpha^5 + \alpha^3 \equiv \alpha \cdot (\alpha^5 + \alpha^4 + \alpha + 1 + \alpha^3 + \alpha^2 + \alpha + \alpha^5 + \alpha^3 +$
$\alpha + \alpha^2 + 1) + \alpha^4 + \alpha^2 + 1 + \alpha^5 + \alpha^3 \equiv (\alpha^5 + \alpha^2) + \alpha^4 + \alpha^2 + 1 + \alpha^5 + \alpha^3 \equiv \alpha^4 + \alpha^3 + 1 \not\equiv 1$
(True);

$\alpha^{63} \equiv (\alpha^4 + \alpha^3 + 1) \cdot (\alpha^4 + \alpha^3 + 1)^2 \equiv (\alpha^4 + \alpha^3 + 1) \cdot (\alpha^5 + \alpha^3 + \alpha + \alpha^5 + \alpha^4 + \alpha + 1 + 1) \equiv$
$(\alpha^4 + \alpha^3 + 1) \cdot (\alpha^4 + \alpha^3) \equiv \alpha^5 + \alpha^3 + \alpha + \alpha^5 + \alpha^4 + \alpha + 1 + \alpha^4 + \alpha^3 \equiv 1$ (True).

(b) $\beta = \alpha^{15}$, ord(α)= $n = 63$.
ord(β)= $\frac{n}{\gcd(n,15)} = \frac{63}{3} = 21$.

$\gamma \equiv \alpha^{-127} \equiv \alpha^{-1} \equiv \alpha^{63-1} \alpha^{62} \alpha^{(111110)_{\text{bin}}} \equiv$
$\equiv (((((\alpha)^2 \cdot \alpha)^2 \cdot \alpha)^2 \cdot \alpha)^2 \cdot \alpha)^2 \equiv$
$\equiv ((\alpha^5 + \alpha^4 + \alpha + 1) \cdot \alpha)^2 \cdot \alpha)^2 \cdot \alpha)^2 \equiv$
$\equiv (((\alpha^4 + \alpha^2 + 1)^2 \cdot \alpha)^2 \cdot \alpha)^2 \equiv$
$\equiv ((1 + \alpha^2)^2 \cdot \alpha)^2 \equiv$
$\equiv (\alpha + \alpha^5)^2 \equiv \alpha^5 + \alpha^4 + \alpha^3 + 1$. Verification: $\gamma \cdot \alpha \bmod f(x) = 1$.

(c) $x \equiv \log_{\alpha^{21}}^{\mathtt{D}}(\alpha^9) \bmod |\alpha^{21}|$ this log does not exist as α^{21} has order 3, this means that the subgroup generated by α^{21} is $A = \{1, \alpha^{21}, \alpha^{-21} \equiv \alpha^{42}\}$ and $42 \bmod 63 \not\equiv 9$, this means that $\alpha^9 \notin A$.

$y \equiv \log^{\mathtt{D}}_{\alpha^9}(1) \bmod |\alpha^9|$, this logarithm exists as the multiplicative group generated by α^9 contains the neutral element 1, and the exponent of the log radix to get 1 is $y = 0$.

$z \equiv \log^{\mathtt{D}}_{\alpha^9}(\alpha^{-9}) \bmod |\alpha^9|$, this logarithm exists as the finite multiplicative group generated by α^9 contains the inverse α^{-9} for the definition of group, and the exponent of the log radix to get it is $z = -1 \bmod 7 = 6$, as $|\alpha^9| = ord(\alpha^9) = 7$.

(d) see lectures ...

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 $k_{\mathtt{pub}}$=$\langle n, A, [k_{\mathtt{priv}}]A\rangle$, where n is the prime factor of m and A=$(3, 4)$. Obviously, Bob keeps secret its private-key $k_{\mathtt{priv}}$=3∈$\mathbb{Z}_n$.

The other communicating party, say Alice, wishes to send the binary message, $\mathtt{msg}$=$(101)_{\mathtt{bin}}$, 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.

Solution:

(a)

	0	1	2	3	4	5	6
x^3+3	3	4	4	2	4	2	2
y^2	0	1	4	2	2	4	1

$G = \{\, \mathcal{O}\ (1,2)\ (1,5)\ (2,2)\ (2,5)\ (3,3)\ (3,4)\ (4,2)\ (4,5)\ (5,3)\ (5,4)\ (6,3)\ (6,4)\,\}$
$m = |G| = 13$.
Num. of primitive elements: $\varphi(m) = 12$.

(b) $A = (3, 4)$, $m = 13 = (1101)_{\mathtt{bin}}$, $B = [13]A = [2]([2]([2]A + A)) + A$.

$\lambda_{[2]A} = \frac{3x_A^2+0}{2y_A} = \frac{3\cdot 9+0}{2\cdot 4} \equiv_7 6$
$x_{[2]A} = \lambda^2_{[2]A} - 2x_A \equiv_7 36 - 6 \equiv_7 2$.
$y_{[2]A} = -y_A + \lambda_{[2]A} \cdot (x_A - x_{[2]A}) \equiv_7 -4 + 6 \cdot (3 - 2) \equiv_7 2 \Rightarrow [2]A = (2, 2)$.

$\lambda_{[3]A} = \frac{y_{[2]A}-y_A}{x_{[2]A}-x_A} = \frac{2-4}{2-3} \equiv_7 2$.
$x_{[3]A} = \lambda^2_{[3]A} - x_A - x_{[2]A} \equiv_7 4 - 3 - 2 \equiv_7 6$.

$y_{[3]A} = -y_{[2]A} + \lambda_{[3]A} \cdot (x_{[2]A} - x_{[3]A}) \equiv_7 -2 + 2 \cdot (2-6) \equiv_7 4 \Rightarrow [3]A = (6,4).$

$\lambda_{[6]A} = \frac{3x_{[3]A}^2+0}{2y_{[3]A}} = \frac{3\cdot 36+0}{2\cdot 4} \equiv_7 -2^{-1} \equiv_7 3$
$x_{[6]A} = \lambda_{[6]A}^2 - 2x_{[3]A} \equiv_7 9 - 12 \equiv_7 4.$
$y_{[6]A} = -y_{[3]A} + \lambda_{[6]A} \cdot (x_{[3]A} - x_{[6]A}) \equiv_7 -4 + 3 \cdot (6-4) \equiv_7 2 \Rightarrow [6]A = (4,2).$

$\lambda_{[12]A} = \frac{3x_{[6]A}^2+0}{2y_{[6]A}} = \frac{3\cdot 16+0}{2\cdot 2} \equiv_7 5$
$x_{[12]A} = \lambda_{[12]A}^2 - 2x_{[6]A} \equiv_7 25 - 8 \equiv_7 3.$
$y_{[12]A} = -y_{[6]A} + \lambda_{[12]A} \cdot (x_{[6]A} - x_{[12]A}) \equiv_7 -2 + 5 \cdot (4-3) \equiv_7 3 \Rightarrow [12]A = (3,3).$

$\lambda_{[13]A} = \frac{y_{[12]A}-y_A}{x_{[12]A}-x_A} = \frac{3-4}{3-3} \equiv_7 \infty \Rightarrow [13]A = \mathcal{O}.$

(c) $[r]A = [4](3,4) = [2]([2](3,4))$

$\lambda_{[4]A} = \frac{3x_{[2]A}^2+0}{2y_{[2]A}} = \frac{3\cdot 4+0}{2\cdot 2} \equiv_7 3$
$x_{[4]A} = \lambda_{[4]A}^2 - 2x_{[2]A} \equiv_7 9 - 4 \equiv_7 5.$
$y_{[4]A} = -y_{[2]A} + \lambda_{[4]A} \cdot (x_{[2]A} - x_{[4]A}) \equiv_7 -2 + 3 \cdot (2-5) \equiv_7 3 \Rightarrow [4]A = (5,3).$

$[k_{\texttt{priv}}]A = [3](3,4) = (6,4)$ see point **(b)**

$$\begin{cases} \gamma = [r]A = [4](3,4) = (5,3) \\ \delta = m \texttt{ bitwiseXOR } \texttt{xCoord}([r]k_{\texttt{priv}}) = (101)_{\texttt{bin}} \oplus (110)_{\texttt{bin}} = (011)_{\texttt{bin}} \end{cases}$$

(d) see lectures ...

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: $\texttt{00}, \texttt{e1}, \texttt{e4}, \texttt{25}, \texttt{o6}$, and $\texttt{e9}$, 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 $e{=}5_{\texttt{dec}}$ be the public exponent of a RSA public-key $k_{pub}{=}\langle e, n\rangle$. Knowing the factorization of the modulus n, compute the value of the corresponding RSA private-key $k_{priv}{=}(p, q, \varphi(n), d)$. Show every step of the computation.

(d) Decrypt the message $c{=}550_{\texttt{dec}}{\in}\mathbb{Z}_n$ (provided without any padding scheme) through applying the CRT. Describe each step of the procedure.

(e) Assume to work into the Montgomery domain: $(\widetilde{\mathbb{Z}}_p, +, \times),\ p = 19$

- 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.

Solution:

(a), (b)
$x = \lceil \sqrt{n} \rceil = 24$. $n - x^2 = 25 = y^2$ is a perfect square.
This means the factors are: $x - y = 19$, $x + y = 29$.
Therefore for RSA: $p = 19$, $q = 29$.
see lectures ...

(c) see lectures ...
$\varphi(n) = 504 = 2^4 \cdot 3 \cdot 7$,
$d \equiv \varphi(n) e^{\varphi(\varphi(n))-1} \equiv_{504} 5^{95} \equiv_{504} \ldots \equiv_{504} 101$.

(d) see lectures ...
$\texttt{RSADecrypt\_CRT}(550_{\texttt{dec}}) = \ldots \equiv_{551} -1 \equiv_{551} 550$.

(e) see lectures ...
$N = 19$, $R = 2^5 = 32$,
$R' = R^{-1} \bmod N = 32^{-1} \bmod 19 = \ldots = 3$,
$N' = N^{-1} \bmod R = 19^{-1} \bmod 32 = \ldots = 27$
see lectures ...
$C = \cdots = (00100)_{\texttt{bin}} = 4_{\texttt{dec}}$