Cryptography and Architectures for Computer Security

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

Prof. G. Pelosi

January 24th, 2019 – Exam Session

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

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

Time: 2h, 30min. 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]
Consider the Vigenere cipher over the lowercase English alphabet, where the key has length 6. For which of the following message spaces will this scheme be perfectly secret? (Check all that apply.)

(i) The set of all 7-character strings of lowercase English letters.

(ii) The set of all strings of lowercase English letters containing at most 6 characters.

(iii) The set of all 6-character strings of lowercase English letters.

(iv) The set of all 5-character strings of lowercase English letters.

Solution:
Perfect secrecy means that there is no recoverable information about plaintexts looking at the ciphertexts. Thus, in a ciphertext-only scenario, options (iii) and (iv) do not leak any information to the cryptoanalyst (e.g., the length of the plaintext) if the portion of the key (with each digit uniformly and randomly chosen) employed in the encryption transformation has a fixed length and such length is the same of any plaintext message.

Question 2 [3 pts]
Describe the Web-of-Trust (WoT) concept used in PGP, GnuPG, and other OpenPGP-compatible systems to establish the authenticity of the binding between a public key and its owner. Describe the centralized trust model of a public key infrastructure (PKI), pointing out advantages and disadvantages with respect to WoT.

Solution:
see lectures...

Question 3 [3 pts]
Consider the following three basic modes of operations of block ciphers: ECB, CBC, and CTR. For each modes of operation analyze the effect on the decryption of remaining blocks if, for the sequence of ciphertext blocks $c_1, c_2 \ldots, c_n$, one ciphertext block c_j $(0 \leq j < n)$ is erroneous. Specify which plaintext blocks x_j, $x_{j+1}, \ldots$ are computed correctly.

Solution:
see lectures...

Question 4 [5 pts]

(a) Consider the cyclic group $(\mathbb{Z}_{64}^*, \cdot)$. Compute the cardinality of the group, the number of its generators and show the order of the element $3 \in \mathbb{Z}_{64}^*$.

(b) Consider the finite field $\mathbb{F}_{2^6}$. Find the number of irreducible and primitive polynomials. Determine if $f(x) = x^6 + x + 1 \in \mathbb{F}_2[x]$ is a primitive polynomial and show all its roots.

Solution:

(a) $n = |\mathbb{Z}_{64}^*| = \varphi(64) = 32$
$num.of generators = \varphi(32) = 16$
proper divisors of 32 are 2,4,8,16, thus $3^4 \equiv_{64} 17$, $3^{16} \equiv_{64} (3^4)^4 \equiv_{64} 17^4 \equiv_{64} = 1$
$\Rightarrow ord_{64}(3) = 16$.

(b) $N_6(2) = ...2^6 = \sum_{d|6} (N_d(2) \cdot d) \Rightarrow N_6(2) = \frac{64-2\cdot1-1\cdot2-2\cdot3}{6} = 9$.
$M_6(2) = \frac{\varphi(63)}{6} = \frac{36}{6} = 6$.
$f(x) = x^6 + x + 1$ is primitive iif $f(\alpha) = 0, \alpha \in \mathbb{F}_{2^6} \backslash \mathbb{F}_2$ and $\alpha^7 \neq 1$, $\alpha^9 \neq 1$, $\alpha^{21} \neq 1$, $\alpha^{63} = 1$.... $f(x)$ is primitive!
The six roots of $f(x)$ are conjugate with α, that is: α^{2^j}, $j = 0, 1, 2, 3, 4, 5$. ...

Question 5 [6 pts]

Consider the group of points over the elliptic curve $\mathbb{E}(\mathbb{F}_{13}) : y^2 = x^3 + 2x$,
with order $n = |\mathbb{E}(\mathbb{F}_{13})| = 12$.

(a) Verify the "non-singularity" of the curve and compute the number of generators of the group.

(b) Verify that $\mathrm{P} = (2, 5)$ is a generator, then compute the coordinates of $\mathrm{Q} = -\mathrm{P}$ and show its order.

(c) Discuss the parameter settings and the mathematical security of an elliptic curve cryptosystem employing a group with a composite order.

Solution:

(a) $\Delta = 4(2^3) + 27(0) \equiv_{13} 8 \neq 0 \Rightarrow \mathbb{E}(\mathbb{F}_{13})$ is non-singular.
Number of generators $= \varphi(n) = \varphi(12) = 4$

(b) As $n = 12 = 2^2 \cdot 3$, $\mathrm{P} = (2, 5)$ is a generator if and only if $[2]\mathrm{P} \neq \mathcal{O}$, $[4]\mathrm{P} \neq \mathcal{O}$, $[3]\mathrm{P} \neq \mathcal{O}$, $[6]\mathrm{P} \neq \mathcal{O}$
Consider the computation of $[2]\mathrm{P} = [2](2, 5)$:
$\lambda \equiv_{13} \frac{3(2^2)+2}{10} \equiv_{13} 10^{-1} \equiv_{13} 10^{11} \equiv_{13} 4$.

$$\begin{cases} x_{[2]\mathrm{P}} \equiv_{13} 4^2 - 2(2) \equiv_{13} 12 \\ y_{[2]\mathrm{P}} \equiv_{13} -5 + 4(2 - 12) \equiv_{13} 7 \end{cases}$$

Consider the computation of $[2]\mathrm{P} = [2]([2](2,5)) = [2](12,7)$:
$\lambda \equiv_{13} \frac{3(-1)^2+2}{14} \equiv_{13} 3(7^{-1}) \equiv_{13} 3 \cdot 2 \equiv_{13} 6$.

$$\begin{cases} x_{[4]\mathrm{P}} \equiv_{13} 6^2 - 2(12) \equiv_{13} 12 \\ y_{[4]\mathrm{P}} \equiv_{13} -7 + 6(12-12) \equiv_{13} 6 \end{cases}$$

Consider the computation of $[3]\mathrm{P} = [2](2,5) + (2,5) = (12,7) + (2,5) = [3](2,5)$:
$\lambda \equiv_{13} \frac{7-5}{12-2} \equiv_{13} 5^{-1}) \equiv_{13} 5^{11} \equiv_{13} 8$.

$$\begin{cases} x_{[3]\mathrm{P}} \equiv_{13} 8^2 - 12 - 2 \equiv_{13} 11 \\ y_{[3]\mathrm{P}} \equiv_{13} -7 + 8(12-11) \equiv_{13} 1 \end{cases}$$

Consider the computation of $[6]\mathrm{P} = [2]([3](2,5)) = [2](11,1)$:
$\lambda \equiv_{13} \frac{3(11)^2+2}{2} \equiv_{13} 7$.

$$\begin{cases} x_{[6]\mathrm{P}} \equiv_{13} 7^2 - 2(11) \equiv_{13} 1 \\ y_{[6]\mathrm{P}} \equiv_{13} -1 + 7(11-1) \equiv_{13} 4 \end{cases}$$

$\mathrm{P} = (2,5)$ is a generator.
Consider $\mathrm{Q} = -\mathrm{P} = (2,-5) = (2,8)$ and say m the order of Q, thus $[m]\mathrm{Q} = \mathcal{O}$.
Note that $[m]\mathrm{Q} = \mathcal{O} \Leftrightarrow [m]([-1]\mathrm{P}) = \mathcal{O} \Leftrightarrow [m]\mathrm{P} = \mathcal{O}$, therefore m = $ord(\mathcal{P}) = n = 12$.

(c) see lectures...

Question 6 [14 pts]
Consider an RSA cryptosystem

(a) Apply the Pollard's rho factorization method to the RSA modulus $n = p \cdot q = 551$ showing each step of the computation.

(b) Describe the Miller-Rabin primality test and apply it to the factor p employing as bases a = 3, b = 7.

(c) Given the modulus factorization found as answer to (a), and the secret exponent d=19,

- compute the encryption exponent e;
- decrypt the message c=$300_{\text{decimal}} \in \mathbb{Z}_n$ (provided without any padding scheme) through applying the CRT. Describe each step of the procedure

(d) Assume to work into the Montgomery domain: $(\mathbb{Z}_p, +, \times)$, $p = 13$.
Compute the Montgomery multiplication C=$A \times B$ mod p, where A=6_{decimal} and B=3_{decimal} are values in the Montgomery domain. Assume a binary encoding of the operands.

(e) Show the computational complexity of performing a RSA encryption applying the Montgomery strategy to execute the modular multiplications.
Show the said computational complexity when the Montgomery strategy is applied to operands encoded in Radix-4.

Solution:

(a) ... $p = 19$, $q = 29$.

(b) see lectures ...

(c) $\varphi(n)$=504, $\varphi(\varphi(n))$=144,
$e \equiv_{\varphi(n)} d^{-1} \equiv_{\varphi(n)} d^{\varphi(\varphi(n))-1} \equiv_{\varphi(n)} 19^{143} \equiv_{504} 451$.
$m = \mathtt{Dec}_{k_{priv}}(c) = c^d \bmod n \Leftrightarrow$
$\text{CRT} : \begin{cases} m_p \equiv_p 15^1 \\ m_q \equiv_{29} 10^3 \equiv_{14} \end{cases}$ $m \equiv_{551} 15 \times 29 \times 2 + 14 \times 19 \times 26 \equiv_{551} 870 + 6916 \equiv_{551}$
$7786 \equiv_{551} 72$.

$m = \mathtt{Dec}_{k_{priv}}(300) = 300^{451} \bmod 551 \Leftrightarrow$
$\text{CRT} : \begin{cases} m_p \equiv_{19} c^{d \bmod \varphi(p)} \\ m_q \equiv_q c^{d \bmod \varphi(q)} \end{cases}$ $m \equiv_n m_p \times q \times (q^{-1} \bmod p) + m_q \times p \times (p^{-1} \bmod q)$

(d) see lectures ... $C \equiv_{13} 6$

(e) see lectures ...