Module:	Level:	Exam:
Computer Security	2^{nd} Year Master (Artificial Vision)	Regular Final Session
Unauthorized documents	Duration: 1 hour 30	Scientific calculator allowed

Sunday, January 14, 2024

Answer clearly and concisely

Exercise 1 : 07 pts (Operation modes and Padding)

A plaintext M is divided into six blocks, $m_1, m_2, \ldots m_6$, encrypted with a symmetric cryptosystem, producing the encrypted blocks $c_1, c_2, \ldots c_6$. During transmission, errors affected some blocks.

1) What is the decryption result of each block c_i in each of the following scenarios ?
   (a) ECB "Electronic Code Book" operation mode and c_1 and c_4 are erroneous.
   (b) CBC "Cipher Block Chaining" operation mode and IV, c_2, and c_4 are erroneous.
   (c) CBC "Cipher Block Chaining" operation mode and only c_3 is erroneous.
   (d) CTR "Counter" operation mode and IV, c_2, and c_4 are erroneous.

   We use a symmetric cryptosystem with a block size of 64 bits to encrypt a plaintext M'.
2) What is the number of encrypted blocks and the ciphertext size in each of the following scenarios?
   (a) M' of 72 bits with PKCS#5 padding.
   (b) M' of 128 bits with PKCS#7 padding.
   (c) M' of 80 bits with ANSI X.9.23 padding.

Exercise 2 : 07 pts (RSA Cryptosystem)

Ali uses an RSA system with $p = 29$ and $q = 41$.

1) Calculate the values of the RSA modulus N and $\varphi(n)$, the Euler's totient.
2) What is the smallest usable value of the encryption exponent e such that $e \leq 10$? Justify your answer.
3) What are Ali's public and private keys in this case ?
4) Omar wants to send securely the plaintext $m = 32$ to Ali. What is the corresponding cryptogram c ?
5) What plaintext m corresponds to the cryptogram $c = 32$ sent by Omar to Ali ?
6) Show that, knowing the value of the RSA modulus N $(N = pq)$ and the associated Euler's totient $\varphi(N)$, we can determine the values of p and q.
7) Using the method proposed in the previous question, determine the values of p and q if the RSA modulus $N = 899$ and the associated Euler's totient $\varphi(N) = 840$.

Note: $\forall m \in \mathbb{Z}_n - \{0\}, m^{281} \equiv m \mod n$.

Exercise 3 : 06 pts (Data Ecryption Standard (DES))

Consider the DES (Data Encryption Standard) cryptosystem.
Recall that its round function is $f(R_{i-1}, K_i) = P(S(E(R_{i-1}) \oplus K_i))$.

1) The right half block received by a round is $R_{i-1} = (1B8FA541)_{16}$ and $K_i = (F358F3134A15)_{16}$. Give the binary results of its expansion and after mixing it with the subkey.
2) The input data of the S-Boxes is $(7C24ACC3E017)_{16}$. Give the output binary values of S_3, S_6 and S_7.

Model Answer + Grading Rubric

Answer of exercise 1

1) The decryption result of each block c_i in each of the given scenarios are summarized in the following table:

		m_1	m_2	m_3	m_4	m_5	m_6
01,00 pts	(a)	erroneous	correct	correct	erroneous	correct	correct
01,00 pts	(b)	erroneous	erroneous	erroneous	erroneous	erroneous	correct
01,00 pts	(c)	correct	correct	erroneous	erroneous	correct	correct
01,00 pts	(d)	erroneous	erroneous	erroneous	erroneous	erroneous	erroneous

2) The number of encrypted blocks and the ciphertext size in each of the given scenarios are summarized in the following table:

		Number of encrypted blocks	Ciphertext size
01,00 pts	M' of 72 bits with PKCS#5 padding	2	128 bits
01,00 pts	M' of 128 bits with PKCS#7 padding	3	192 bits
01,00 pts	M' of 80 bits with ANSI X.9.23 padding	2	128 bits

Answer of exercise 2

1) The RSA module $\boxed{n = p \times q = 29 \times 41 = 1189}$. 00,50 pts
   The Euler's totient is $\boxed{\varphi(n) = (p-1)(q-1) = 28 \times 40 = 2^2 \times 7 \times 2^3 \times 5 = 1220}$. 00,50 pts

2) The smalled usable value of the encryption exponent e such that $e \leq 10$, is $\boxed{e = 3}$ because $PGCD(3, 1220) = 1$ and: 01,00 pts
   - $\forall i \in \{2, 4, 6, 8, 10\} : \; PGCD(i, 1220) \neq 1$.
   - $PGCD(5, 1220) = 1$ but $5 > 3$.
   - $PGCD(7, 1220) = 1$ but $7 > 3$.
   - $PGCD(9, 1220) = 1$ but $9 > 3$

3) Ali's public key is $\boxed{(n, e) = (1189, 3)}$. 00,50 pts
   The decryption exponent d must satisfy $e \times d \equiv 1 \mod \varphi(n)$ and using the extended Euclidean algorithm , we obtain:
   $1120 \times (1) + 3 \times (-373) = 1$. The decryption exponent is: $d = -373 \mod 1120 = 747 \mod 1120$.

i	r_i	q_i	α_i	β_i
1	1120	–	1	0
2	3	373	0	1
3	1	3	1	-373
4	0	–	–	–

   Ali's private key is $\boxed{(n, d) = (1189, 747)}$. 00,50 pts

4) The cryptogram c corresponding to the plaintext $m = 20$:
   $m = 32$ et $c = m^e \mod n = 32^3 \mod 1189 = 2^{5^3} \mod 1189 = 2^{15} \mod 1189 = 2 \times 2^2 \times 2^4 \times 2^8 \mod 1189 = 2 \times 4 \times 16 \times 256 \mod 1189$. Hence, $\boxed{c = 665}$. 01,00 pts

5) The plaintext m corresponding to the cryptogram $c = 32$:
$m = c^d \mod n = 32^{747} \mod 1189 = 32^{281} \times 32^{281} \times 32^{185} \mod 1189 = 32^{187} \mod 1189 = 2^{935} \mod 1189 = 2^{281} \times 2^{281} \times 2^{281} \times 2^{92} \mod 1189 = 2^{95} \mod 1189 = 2^{15} \times 2^{15} \times 2^{15} \times 2^{15} \times 2^{15} \times 2^{15} \times 2^{5} \mod 1189 = 665^6 \times 32 \mod 1189 = 122 \times 32 \mod 1189$. Ainsi $\boxed{m = 337}$. **01,00 pts**

6) We know that: $n = pq$, so $q = \frac{n}{p}$.
We know also that: $\varphi(n) = (p-1)(q-1) = pq - p - q + 1 = n - p - q + 1 = n - p - \frac{n}{p} + 1$
It follows that: $p\varphi(n) = np - p^2 - n + p \implies \boxed{p^2 - p(n - \varphi(n) + 1) + n = 0}$
This is a quadratic equation in p , with: $a = 1,\ b = -(n - \varphi(n) + 1)$ and $c = n$.
It can be readily solved using the well-known quadratic formula:
$$\boxed{(p,q) = \frac{-b \pm \sqrt{|b|^2 - 4ac}}{2a} = \frac{(n+1-\varphi(n)) \pm \sqrt{[n-\varphi(n)+1]^2 - 4n}}{2}}.$$ **01,00 pts**

7) We have $n = 899$ and $\varphi(n) = 840$:
$(p,q) = \frac{(n+1-\varphi(n)) \pm \sqrt{[n-\varphi(n)+1]^2 - 4n}}{2} = \frac{(899-840+1) \pm \sqrt{[899-840+1]^2 - 4\times 899}}{2} = \frac{60 \pm \sqrt{60^2 - 4\times 899}}{2} = \frac{60 \pm 2}{2}$
Hence, $\boxed{p = 29 \text{ and } q = 31}$. (or $p = 31$ and $q = 29$)
01,00 pts

Answer of exercise 3

1) We have: $R_{i-1} = (1B8FA541)_{16} = (00011011100011111010010101000001)_2$
and $K_i = (F358F3134A15)_{16} = (111100110101100011110011000100110100101000010101)_2$:
After expansion:
$\boxed{E(R_{i-1}) = (1000\ 1111\ 0111\ 1100\ 0101\ 1111\ 1101\ 0000\ 1010\ 1010\ 0000\ 0010)_2}$ **01,50 pts**
After mixing with the subkey:
$\boxed{E(R_{i-1}) \oplus K_i = (0111\ 1100\ 0010\ 0100\ 1010\ 1100\ 1100\ 0011\ 1110\ 0000\ 0001\ 0111)_2}$ **01,50 pts**

2) The input data of the S-Boxes is $(7C24ACC3E017)_{16}$:
$(7C24ACC3E017)_{16} = (\boxed{011111}\,000010\,\boxed{010010}\,101100\,\boxed{110000}\,111110\,\boxed{000000}\,010111)_2$
The output of S_3 is: $S_3(010010) = S_3(0,9) = 13 = \boxed{(1101)_2}$ **01,00 pts**
The output of S_6 is: $S_6(111110) = S_6(2,15) = 6 = \boxed{(0110)_2}$ **01,00 pts**
The output of S_7 is: $S_7(000000) = S_7(0,0) = 4 = \boxed{(0100)_2}$ **01,00 pts**