Module:	**Level:**	**Exam:**
Computer Security	2nd 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, $m_1, m_2, \dots m_6$, encrypted with a symmetric cryptosystem, producing the encrypted blocks $c_1, c_2, \dots c_6$. 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.