جامعة المنوفية
كلية الهندسة الإلكترونية بمنوف
زمن الإمتحان: ثلاث ساعات

مادة مقرر: نظم تأمين المعلومات
إمتحان الفصل الدراسى الثانى
الفرقة الثالثة - اتصالات

(١٣)

Q1.

A) Explain a stream cipher and its applications?

B) How many keys are required for two people to communicate via a cipher?

C) Which parameters and design choices determine the actual algorithm of a Feistel cipher?

D) Briefly describe SubBytes?

Q2.

A) Explain with a given example the Vernam cipher?

B) What are the techniques of steganography?

C) Compare between Cipher Modes in Fig. 1 and Fig. 2? What are names, operation, advantages and applications?

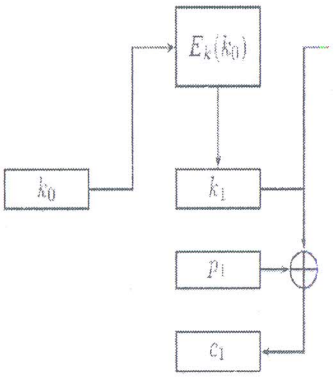

Fig. 1

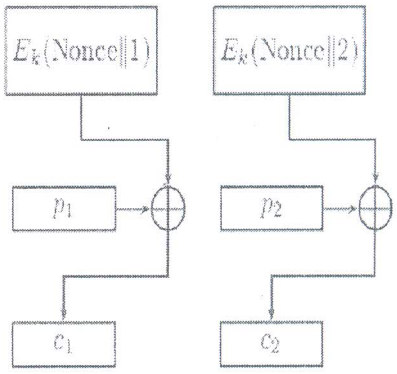

Fig. 2

D) Using digital signature standard (DSS) with $p = 1031$, $q = 105$ and $h = 16$. The user private key $x = 50$ and random integer $k = 13$. The message hash value is $H(M) = 100$. Find a digital signature (r, s) and how to verify it.

Note: $g = h^{(p-1)/q} \bmod p$, $y = g^x \bmod p$, $r = (g^k \bmod p) \bmod q$, $u_1 = [s^{-1}H(M)] \bmod q$

$s = [k^{-1}(H(M) + xr)] \bmod q$, $u_2 = [s^{-1}r] \bmod q$, $v = [(g^{u_1}y^{u_2}) \bmod p] \bmod q$

تابع صفحة رقم (2)

Q3.

A) What are applications and benefits of IPsec?

B) What are cryptographic algorithms for IEEE 802.11i?

C) The ECC Diffie-Hellman cryptosystem parameters are $E_{11}(1,4)$ and $G = (2,3)$. B's secret key is $n_B = 2$. Chooses the random value $k = 1$.

i) Find B's public key P_B.

ii) A wishes to encrypt the message $P_m = (8,5)$ and determine the ciphertext C_m.

Note: $x_R = (\lambda^2 - x_p - x_Q) \bmod p$, $y_R = (\lambda(x_p - x_R) - y_p) \bmod p$, $P_B = n_B \times G$, $C_m = \{kG, P_m + kP_B\}$

$$\lambda = \begin{cases} \left(\frac{y_Q - y_p}{x_Q - x_p}\right) \bmod p & \text{if } P \neq Q \\ \left(\frac{3x_p^2 + a}{2y_p}\right) \bmod p & \text{if } P = Q \end{cases}$$

Q4.

A) Compare between temporal key integrity protocol and counter mode-CBC MAC protocol?

B) What are IEEE 802.11i phases of operation?

C) Encrypt message the "Reading is useful" using Rivest-Shamir-Adleman (RSA) algorithm with two prime numbers $p = 5$, $q = 11$ and $d = 3$?

D) Explain the case of Fig.