7PM CLASS TEST

Question 1 (1.0 mark)

The greatest common divisor of two numbers n_1 and n_2 is $gcd(n_1, n_2) = a(n_1) + b(n_2)$. If $n_1 = 335$ and $n_2 = 2398$, what are the values of a and b?

A. $a = 43,\ b = -6$
B. $a = -6,\ b = 43$
C. $a = -158,\ b = 1131$
D. $a = 1131,\ b = -158$
E. None of the above

Answer: D $-\ a = 1131, b = -158$

Explanation:

n1	n2	r	q	a1	b1	a2	b2
2398	335	53	7	1	0	0	1
335	53	17	6	0	1	1	-7
53	17	2	3	1	-7	-6	43
17	2	1	8	-6	43	19	-136
2	1	0	2	19	-136	-158	1131

$$\gcd(335,2398) = (1131)(335) + (-158)(2398) = 1$$

Question 2 (1.0 mark)

You and Alice has agreed to experiment the Diffie-Hellman key exchange protocol. Both of you agreed on the value of generator $g = 7$ and a prime $p = 23$. Alice has computed her public key, $Pub_A = 16$, and sent it to you. You chose 9 as your private key, $Pri_y = 9$, and computed your public key, $Pub_y = 15$. What is the common key?

A. 15
B. 16
C. 8
D. 9
E. 12

Answer: Option C (8).

Explanation:

$$K = (Pub_A)^{Pri_y}\ mod\ p$$

$$K = (16)^9\ mod\ 23 = 8$$

Question 3 (1.0 mark)

Encryption of large blocks using TEA (or any fixed size block cipher), as you have done for one of the tasks in your assignment, can be achieved through the means of modes. We consider an Cipher Feedback Mode (CFB mode) operation for a block cipher which implements the decryption as $P_i = C_i \oplus S_s[E(K, C_{i-1})]$ for $i > 0$, where P_1, P_2, P_3 ... are the messages and C_1, C_2, C_3 ... are the ciphertext. Given the ciphertext 11100111, the $key = [1,1,0]$, $C_0 = [1,1,1]$, and the following cipher:

Input	000	001	010	011	100	101	110	111
Output	110	111	100	101	010	011	000	001

Which one of the following is the plaintext, if the mode of operation is a **2-bit CFB** cipher?

A. $plaintext$: 11 00 10 00
B. $plaintext$: 11 00 10 01
C. $plaintext$: 11 10 01 00
D. $plaintext$: 11 00 10 10
E. $plaintext$: 11 10 10 00

Answer: Option C ($plaintext$: 11 10 01 00)

Explanation:

To decrypt in CFB mode, we need to XOR a plaintext with the previous block's ciphertext which has been feed-back to the following block cipher.

IV=111

Input (IV or C_0):	111	111	110	001
E(Input)/Output:	001	001	000	111
Ciphertext:	11	10	01	11
Plaintext:	11	10	01	00

Question 4 (1.0 mark)

What is $(C9 \times 03)$ performed in $GF(2^8)$?

A. $(25B)_{hex} = (603)_{10}$
B. $(DA)_{hex} = (218)_{10}$
C. $(E3)_{hex} = (227)_{10}$
D. $(89)_{hex} = (137)_{10}$
E. $(5D)_{hex} = (93)_{10}$

Answer: D – $(89)_{hex} = (137)_{10}$

$$(C8 \times 03) \quad = (C9) \oplus (C9 \times 02)$$

$$= (11001001) \text{ xor } (10010010) \text{ xor } (00011011)$$

$$= (10001001)_2 = (89)_{hex} = (137)_{10}$$

Question 5 (1.0 mark)

In your Assignment 2, you have implemented a simplified SHA hash function which output 32 bits of output (digest). How many attempts (round up to the nearest decimal) would you have to make to find two messages m and m' that are not the same, but have the same hash output, if you want your average success probability to be 0.3 or 30%?

Note: $\ln$ is log_e, and the value of e is approximately 2.719. (Hint: We discussed this in Lecture 7, slide 11 and 14.)

A. $k \approx 3{,}823$
B. $k \approx 4{,}168$
C. $k \approx 5{,}5352$
D. $k \approx 16{,}467{,}968$
E. $k \approx 6{,}356$

Answer: Option C ($k \approx 55352$)

Explanation: Using the formula $k \approx \sqrt{2m\, ln\left(\frac{1}{1-\varepsilon}\right)}$, where $m = 2^{32}$ and $\varepsilon = 30\% = 0.3$, we have $k \approx \sqrt{2 \times 2^{32} \times \ln\left(\frac{1}{1-0.3}\right)} \approx \sqrt{2 \times 4{,}294{,}967{,}296 \times 0.356675} \approx 55352.$

Question 6 (3.0 marks)

ElGamal is known to be insecure against chosen ciphertext attack. Show this.

Suggested answer:

An attacker wants to decrypt a target ciphertext message C, which consists of

$$C = (y_1, e)$$

$where\ y_1 = g^{k_1}\ mod\ p, and\ e = m \times y_2^{k_1}\ mod\ p$

to obtain the plaintext m.

Assumption:

The attacker has access to a decryption oracle and the decryption oracle is able to encrypt any ciphertext messages except of the ciphertext message C.

The attacker choses a random number r and multiplies r and e to obtain C', that is, $C' = r\ x\ e$.

The attacker then sends (y_1, C') to the decryption oracle to decrypt C' and obtain m'.

The attacker then computes

$$m' = \frac{C'}{y_1^{k_2}} = \frac{r \times e}{y_1^{k_2}}$$

$$\frac{m'}{r} = \frac{r \times m \times y_2^{k_1}}{r \times y_1^{k_2}}$$

$$= \frac{r \times m \times (g^{k_2})^{k_1}}{r \times (g^{k_1})^{k_2}}$$

$$= \frac{r \times m \times g^{k_2 k_1}}{r \times g^{k_2 k_1}}$$

$$= m.$$

Question 7 (2.0 marks)

Similar to the Assignment 1, but with a modified Feistel function $f_i(x,K) = (2i \times K)^{(x)_{10}} \; mod \; 19$, for $i = 1$ and 2 $(round\ 1\ and\ round\ 2)$, and K is a member of Z_{19} (meaning K is any number between 0 and $19-1$). $x = R_i$, that is the right 4 bits of a particular round, and $(x)_{10} = decimal\ form\ of\ x,\ e.g., x = 0111\ and\ (0111)_{10} = 7$. If $K = 7$ (for both rounds) and the plaintext is 11010101, what is the ciphertext? Draw the picture of the Feistel Cipher network to help you, and show your intermediate results.

Sample solution including but is not limited to the following:

$L_0 = 1101, \quad R_0 = 0101$

$i = 1, \quad x = (0101)_2 = (5)_{10}, \quad K = 7$

$F_i(x,K) = (2i \times K)^x \; mod \; 19$

$F_1(0101,7) = (2 \times 1 \times 7)^5 \; mod \; 19$

$= (14)^5 \; mod \; 19 = (1)_{10} = (0001)_2$

$R_1 = (F_1 \oplus L_0 = 0001 \oplus 1101 = 1100)$

$L_1 = R_0 = 1101$

$i = 2, \quad x = (1100)_2 = (12)_{10}, \quad K = 7$

$F_2(1100,7) = (2 \times 2 \times 7)^{12} \; mod \; 19$

$= (28)^{12} \; mod \; 19 = (7)_{10} = (0111)_2$

$R_2 = (F_2 \oplus L_1 = 0111 \oplus 1101 = 1010)$

$L_2 = R_1 = 1100$