CSCI361 Cryptography Written Test Practice

Question 1 (1 mark)
In cryptography, what does a perfect secrecy mean?

Question 2 (1 mark)
What is the relationship between MAC and one-way hash function?

Question 3 (1 mark)
Given a system where each character of the English alphabets is encoded using binary, and the true rate of English is 1.5 bits/character, what is the redundancy of English in this system?

Question 4 (2 marks)
Alice wishes to send the following message to Bob using the Affine cipher:

I LOVE UOW

Alice and Bob agreed to use a key a = 3 and b = 17. Encrypt the message.
You can assume the Affine cipher used in this encryption uses only 26 alphabetic characters, and you can ignore the spaces.

Question 5 (4 marks)

Compute the following by demonstrating the step-by-step calculation correctly.

(a) Compute gcd(12345, 67890) and find integers x and y such that $12345x + 67890y = \gcd(12345,67890)$.

(b) Compute $3221^{-1} \bmod 4019$

(c) Use the fast exponentiation algorithm described in lecture to determine 25^{166} mod 123.

(d) Given Z_{11}^*, and a primitive element 2, how many primitive elements (generators) are there and what are they?

Question 6 (2 marks)
What is blind signature scheme? Provide an example how this is achieved using RSA.

Question 7 (2 marks)

We consider a Cipher-Block Chaining Mode (CBC mode) for a block cipher which implements the encryption as $C_i = E(k, M_i \oplus C_{i-1})$ for i > 0 where $M_1, M_2, M_3 \ldots$ are the messages and C_0 is a randomly chosen initial vector.

(i) Explain how decryption is done, and give the mathematical expression for the decryption.
(ii) How does a bit error in the ciphertext influence decryption? (Assume that C_i is obtained corrupted because of a bit error. How does it affect the next decryption steps?)

Question 8 (2 marks)
Explain Diffie-Hellman key exchange. On what hard problem does its security depend? Describe the Diffie-Hellman key agreement protocol. Why is Diffie-Hellman susceptible to man-in-the-middle attacks? Name one way to prevent such attacks.

Question 1 (1 mark)
In cryptography, in particular digital signature context, explain the term nonrepudiation.

Question 2 (1 mark)
What is the difference between an unconditionally secure cipher and a computationally secure cipher?

Question 3 (2 marks)
What is factorization problem? Show an example of a signature scheme that relies on the security of factorization problem.

Question 4 (1 mark)

A user defines a cipher $Y = aX + b \ (mod\ 26)$ to encrypt a sequence of integers X ∈ [0, 25]. The user selects two non-negative integers a ∈ [0, 25] and b ∈ [0, 25] and then encrypts an integer X. How many pairs of (a, b) the user can choose so that a decryption always exists?

Question 5 (4 marks)

Compute the following by demonstrating the step-by-step calculation correctly.

(a) Compute gcd(830407,626303) and find integers x and y such that $830407x + 626303y = \gcd(830407,626303)$.

(b) Compute $591^{-1} mod\ 1823$

(c) Compute $1228^{460} mod\ 1147$ using fast exponentiation algorithm discussed in lecture and/or tutorial. Show all steps.

(d) For any positive integer n, what does Euler's Totient function $\phi(n)$ measure? What is the value of the Euler Phi function $\phi(n)$ if

(i) n = 181

(ii) n = 250

Question 6 (2 marks)
One issue with DES is the key size of 56-bit too short. To increase the key size, one approach is to double encrypt, and hence effectively increase the key size to 112 bits. However, this approach is not really the same as if there were a single DES of 112-bit. Explain why is it much less secure to implement a double DES.

Question 7 (2 marks)

A signature scheme introduced by David Chaum, allows a person to get a message signed by another party without revealing any information about the message to the other party. This signing protocol is known as blind signature. In general, this is what happens:

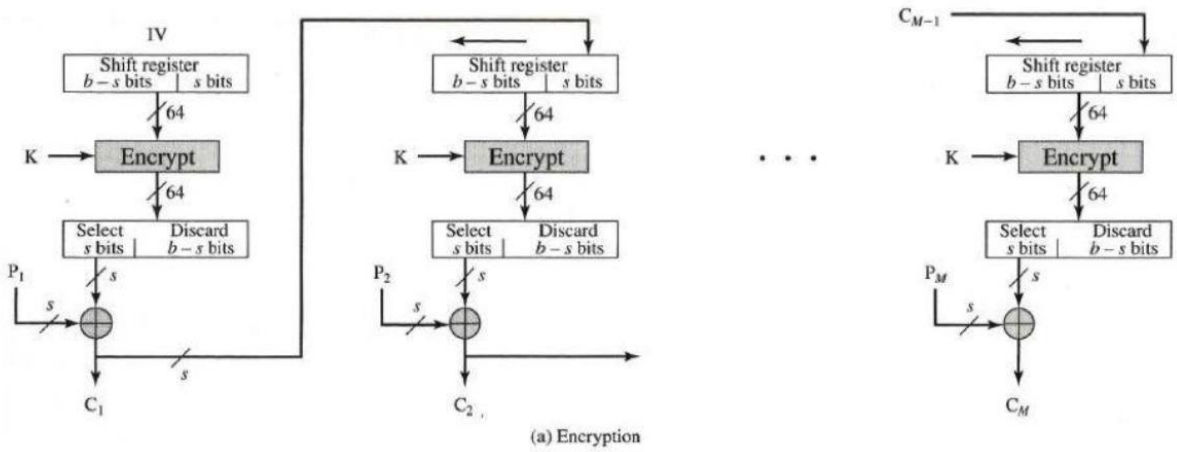
- The requester wants to obtain the signer's signature of message *m*.
- The requester doesn't want to reveal *m* to anyone, including the signer.
- The signer signs *m* blindly, not knowing what they are signing.
- The requester can then retrieve the signature.

(i) Using RSA as the digital signature scheme, describe how the blind signature is realized.

(ii) Show or explain that the requester can indeed verify that the signature of the signatory is valid or correct.

Question 8 (2 marks)

(i) 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. For the s-bit CFB (cipher feedback) mode, the encryption is depicted in the following diagram. **Draw the decryption block diagram** for the s-bit CFB mode shown below and **give the mathematical expression** for the decryption.



(ii) What are the advantages and disadvantages of the CFB mode of operation?

Question 1 (1 mark)
What is a trapdoor one-way function?

Question 2 (1 mark)
Define what a Message Authentication Code (MAC) system is and the properties it should have.

Question 3 (1 mark)
What are the roles of the public and private key?

Question 4 (2 marks)

The weakness of substitution cipher is the small key space. Alice decides to improve the security on the Caesar cipher by making the key space larger. She keeps the message $m = c = \{0, \cdots, 25\}$ as its original algorithm, but she increases the key space $k = \{0, \cdots, 49\}$ and defines a new cipher as follow:

$$E_k(m) = (k + m) mod\ 26$$

What is the security of Alice's new cipher as compared with the ordinary Caesar cipher? Justify your answers.

Question 5 (4 marks)

Compute the following by demonstrating the step-by-step calculation correctly.

(i) Compute $21^{221} mod\ 123$ using fast exponentiation algorithm discussed in lecture and/or tutorial. Show all steps.
(ii) Compute $3037^{-1} mod\ 4051$
(iii) Use Euclid's algorithm to find integers x and y such that $25x + 41y = 1$.
(iv) Find x such that the equation $18x = 11 \bmod 19$ is satisfied?

Question 6 (2 marks)
What is Discrete Logarithm problem? Show an example of a signature scheme that relies on the security of discrete logarithm problem.

Question 7 (2 marks)
Describe how encryption and decryption works for a cryptosystem built from a Feistel network

Question 8 (2 marks)

(i) Consider the RSA algorithm where $p = 11, q = 13,$ and $e = 11$. You receive the ciphertext c = 106. Find the plaintext or message m.
(ii) Adam and Barbie share the same modulus n for RSA to generate their encryption key e_A and e_B. Charlie sends them (Adam and Barbie) the same message m encrypted with e_A and e_B respectively. The resulting ciphertexts are c_A and c_B. Eve intercepts both c_A and c_B. Show how Eve can use the *common modulus attack* to compute the plaintext or the message m sent by Charlie?

Question 1 (1 mark)

What is a one-way function?

Question 2 (1 mark)

What is message authentication code (MAC), and how is it differing from a digital signature scheme?

Question 3 (1 mark)

If a bit error occurs in the transmission of a ciphertext character in 4-bit CFB mode, how far does the error propagate?

Question 4 (2 marks)

The Lehman's primality test can determine if a number is a prime number or a composite number. Describe Lehman's test algorithm.

Question 5 (4 marks)

Compute the following by demonstrating the step-by-step calculation correctly.

(i) Compute $21^{221} mod\ 123$ using fast exponentiation algorithm discussed in lecture and/or tutorial. Show all steps.
(ii) Compute $3037^{-1} mod\ 4051$
(iii) Does 337 have a multiplicative inverse modulo 1394? If yes, what is it?
(iv) What does it mean that g is a generator in Z_p^*?

Question 6 (2 marks)

What is factorization problem? Show an example of a signature scheme that relies on the security of factorization problem.

Question 7 (2 marks)

A message was encrypted using Affine transformation cipher. You have the ciphertext, and it is KRQWL. You also happen to know the plaintext starts with a letter P and ends with a letter Y; in other words, the plaintext letter P is encrypted to K, and the plaintext letter Y is encrypted to L. Decrypt the ciphertext KRQWL. You can assume the Affice cipher used in this ecnryption uses only 26 alphabetic characters, and the mapping of the alphabets to its numerical equivalent is as follow:

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Question 8 (2 marks)

In El Gamal encryption, the private key x in an element in Z_p^*. The public key is given by $y = g^x mod\ p$, where g is a primitive element in Z_p^*. To encrypt message m, one generates a random key $k < p - 1$, sets $c_1 = g^k\ mod\ p$, and $c_2 = m \times y^k\ mod\ p$, and output the ciphertext $c = c_1, c_2$. Describe the decryption process and show/prove that it always returns the encrypted message m.

Question 1 (1 mark)

What are the two main drawbacks with one-time pad?

Question 2 (1 mark)

Describe a practical use for a MAC.

Question 3 (1 mark)

In cryptography, in particular digital signature context, explain the term nonrepudiation.

Question 4 (2 marks)

Describe how to build a MAC system using a block cipher in CBC (chain-block cipher) or CFB (cipher- feedback Block) chain mode.

Question 5 (4 marks)

Compute the following by demonstrating the step-by-step calculation correctly.

(i) Compute $21^{221} mod\ 123$ using fast exponentiation algorithm discussed in lecture and/or tutorial. Show all steps.
(ii) Compute $3037^{-1} mod\ 4051$
(iii) Using the extended Euclidean algorithm, find the multiplicative inverse of 1234 and 4321.
(iv) Find x such that the equation $18x = 11 \bmod 19$ is satisfied?

Question 6 (2 marks)

DSA is a public key signature algorithm and is specified by the NIST's Digital Signature Standard. DSA is used to create a small, publicly verifable signature ! for a given message !. Describe how a message *M* is signed and verified using DSA. Show that the signing and verification algorithms are correct.

Question 7 (2 marks)

One issue with DES is the key size of 56-bit too short. To increase the key size, one approach is to double encrypt, and hence effectively increase the key size to 112 bits. However, this approach is not really the same as if there were a single DES of 112-bit. Explain why is it much less secure to implement a double DES.

Question 8 (2 marks)

(i) Consider the RSA algorithm where p = 7 and q = 19. What are the private and public keys?

(ii) Suppose Adam generates an RSA key pair with modulus n = p×q, but his private key is stolen (compromised). Rather than generating a new modulus, Adam decides to create a new key pair using the same modulus. Show to Adam that this is not safe.

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:

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

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

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 $P_1, P_2, P_3 \ldots$ are the messages and $C_1, C_2, C_3 \ldots$ 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 – $(89)_{hex} = (137)_{10}$

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

$= (11001001)$ xor (10010010) xor (00011011)

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

CSCI361 Cryptography Written Test Practice

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 $k \approx \sqrt{2 \times 2^{32} \times \ln\left(\frac{1}{1-0.3}\right)} \approx \sqrt{2 \times 4{,}294{,}967{,}296 \times 0.356675} \approx 55352.$

This study source was downloaded by 100000806118722 from CourseHero.com on 12-31-2024 19:43:47 GMT -06:00

https://www.coursehero.com/file/104720552/CSCI361-7PM-CLASS-TESTpdf/

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 e, which consists of

$$C = (y_1, e)$$

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

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, $C' = r \times e$.

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 $f_i(x,K) = (2i \times K)^{(x)_{10}} \bmod 19$, 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:

$L_0 = 1101, \quad R_0 = 0101$

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

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

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

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

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

$L_1 = R_0 = 1101$

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

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

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

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

$L_2 = R_1 = 1100$