SIM GLOBAL EDUCATION

UNIVERSITY OF WOLLONGONG AUSTRALIA

SCIT
School of Computing and Information Technology

Family Name .....

First Name .....

Student Number .....

CSCI361

Cryptography & Secure Applications

This paper is for students studying at the Singapore Institute of Management Pte Ltd.

SESSION 1 2017 – CLASS TEST – PART TIME

(13 February 2017 – 8:00 pm – 10:00 pm)

Time Allowed:	2 hours
Number of Questions:	8 questions

DIRECTIONS TO CANDIDATES

1. Please attempt all questions as directed. Please answer in **consecutive order**.
2. Please write all answers neatly. Questions must be answered in the examination booklet provided. Please answer each question on *a new page* on the examination booklet. Clearly mark the number of the question attempted.
3. This test question must be submitted with your answer upon submission.
4. This paper is worth 15% of the total marks for the subject.

TEST MATERIALS/AIDS ALLOWED

Simple Non-Programmable Calculator Only

THIS TEST PAPER MUST NOT BE REMOVED FROM THE HALL

Version 2.0

Question 1 (1 mark)

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

Suggested answer:

Nonrepudiation provides protection against denial by one of the entities involved in communication of having participated in all or part of the communication. It is a service in digital signature that provides proof that the message was sent by the specified party as well as proof that the message was received by the specified party.

Question 2 (1 mark)

What is the difference between an unconditionally secure cipher and a computationally secure cipher?

Suggested answer:

An encryption scheme is unconditionally secure if the ciphertext generated by the scheme does NOT contain enough information to determine uniquely the corresponding plaintext, no matter how much ciphertext is available.

An encryption scheme is said to be computationally secure if the following two conditions are noticeable in the scheme:
1) The cost of breaking the cipher exceeds the value of the encrypted information, and
The time required to break the cipher exceeds the useful lifetime of the information.

Question 3 (2 marks)

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

Suggested answer:
Factorization refers to splitting of an integer number into a set of factors (a smaller set of prime numbers) which when multiplied together will get back the original integer. All integer numbers may be prime-factorized; i.e., expressed as a product of many prime numbers. When one has an integer number and wants to find the factors of these prime numbers, that can produce back the integer number, is difficult. This problem is known as factorization problem. Many public-key cryptosystems base on this factorization problem, including the RSA cryptosystem as well as RSA digital signature system.

RSA Digital Signature

Key generation:

- The key generation algorithm of RSA digital signature system is the same as the one employed by the RSA cryptosystem.
- Every user will generate his/her public key pair *(e, n)* and private key pair *(d, n)*. The user chooses two prime numbers *p* and *q* and compute the modulus $n = p \times q$.
- The user next chooses two more numbers, *e* and *d*. The number *e* is coprime (relatively prime) to *(p-1)(q-1)*. The number *d* is chosen such that $((e \times d) - 1)$ is divisible by *(p-1)(q-1)*.
- The *(e, n)* pair is the public key, and the *(d, n)* pair is private key.

Message signing:

- To sign a message, the sender signs the message using his/her private key; i.e., $S=m^d \bmod n$

Where

- S is the signature,
- m is the message,
- (d, n) the sender's private key.

- The sender sends the message *m* and the signature *S* to the recipient (receiver).

Signature verification:

- To verify that the message is indeed signed by the sender, the receiver verifies the message authentication using the sender's public key; i.e.,

  $m' = S^e \bmod n$

  where

  - m' is the message recovered by decrypting the digital signature.
  - S is the sender's digital signature
  - (e, n) pair is the sender's public key.

If the message received m is the same as the recovered message m', the receiver can be assured that the messages sent are authentic.

Question 4 (1 mark)

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

Suggested answer:

1. In order to have a decryption, the value of a must be relatively prime to 26; i.e., gcd(26, a) = 1. Thus the values 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, and 25 can be used for the value of a. Total possible values of a is 12.

2. The value b can be any value ∈ [0, 25]. Total possible values of b are 26.

   Thus the number of (a, b) pairs are 12 x 26 = 312 pairs. However, since when a = 1 and b = 0, the cipher produces exact copy of the plaintext, therefore the pair (1, 0) cannot be used because the pair does not hide the plaintext. With the pair (1, 0) excluded, the user can choose 311 (a, b) pairs that ensures decryption always exist.

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

Suggested answer:

a. gcd(830407, 626303) = 823 = (830407)(-224) + (626303)(297)

The student is expected to use Extended Euclidean Algorithm to compute as follow:

n1	n2	r	q	a1	b1	a2	b2
830407	626303	204104	1	1	0	0	1
626303	204104	13991	3	0	1	1	-1
204104	13991	8230	14	1	-1	-3	4

13991	8230	5761	1	-3	4	43	-57
8230	5761	2469	1	43	-57	-46	61
5761	2469	823	2	-46	61	89	-118
2469	823	0	3	89	-118	-224	297

$(830407)(-224) + (626303)(297) = 823.$

Hence x = -224, and y = 297.

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

591^{-1} mod 1823 = 401 mod 1823

The student is expected to use Extended Euclidean Algorithm to compute as follow:

n1	n2	r	Q	a1	b1	a2	b2
1823	591	50	3	1	0	0	1
591	50	41	11	0	1	1	-3
50	41	9	1	1	-3	-11	34
41	9	5	4	-11	34	12	-37
9	5	4	1	12	-37	-59	182
5	4	1	1	-59	182	71	-219
4	1	0	4	71	-219	-130	401

c. $1228^{460}\ mod\ 1147 = 118\ mod\ 1147$

460 (in decimal) = 111001100 (in binary)

2^0=1	0	$1228^1 mod\ 1147$	$81\ mod\ 1147$	81
2^1=2	0	$1228^2 mod\ 1147$	$6561\ mod\ 1147$	826
2^2=4	1	$1228^4 mod\ 1147$	$682276\ mod\ 1147$	958
2^3=8	1	$1228^8 mod\ 1147$	$917764\ mod\ 1147$	164
2^4=16	0	$1228^{16} mod\ 1147$	$26896\ mod\ 1147$	515
2^5=32	0	$1228^{32} mod\ 1147$	$265225\ mod\ 1147$	268
2^6=64	1	$1228^{64} mod\ 1147$	$71824\ mod\ 1147$	710
2^7=128	1	$1228^{128} mod\ 1147$	$504100\ mod\ 1147$	567
2^8=256	1	$1228^{256} mod\ 1147$	$321489\ mod\ 1147$	329
$1228^{460} = 1228^{4+8+64+128+256}\ mod\ 1147$				

$$= 1228^4 \times 1228^8 \times 1228^{64} \times 1228^{128} \times 1228^{256} \; mod \; 1147$$
$$= 958 \times 164 \times 710 \times 567 \times 329 \; mod \; 1147$$
$$= 118 \; mod \; 1147$$
$$= 118$$

$Thus, 1228^{460} \; mod \; 1147 = 118 \; mod \; 1147 = 118$

d. The Euler Phi function $\phi(n)$ counts the amount of numbers a with $1 \leq a \leq n$ such that $\gcd(a,n) = 1$. That is, it is the number of positive integers less than n that are relatively prime to n.

$$\phi(181) = n \times \prod_{p|n}\left(1 - \frac{1}{p}\right) = 181 \times \left(1 - \frac{1}{181}\right)$$
$$= 181 \times \left(\frac{180}{181}\right) = 181.$$

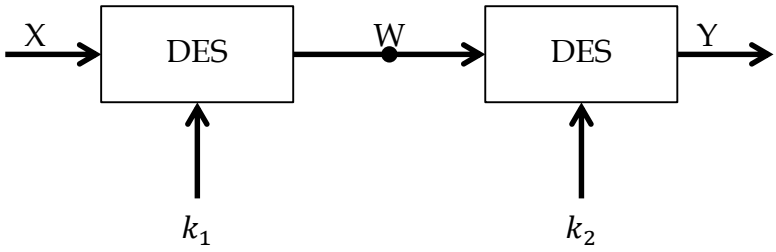
$$\phi(250) = n \times \prod_{p|n}\left(1 - \frac{1}{p}\right) = 250 \times \left(1 - \frac{1}{2}\right) \times \left(1 - \frac{1}{5}\right)$$
$$= 250 \times \left(\frac{1}{2}\right) \times \left(\frac{4}{5}\right) = 100.$$

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.

Suggested answer:

With double DES, the plaintext Y is encrypted two times, with different keys; $Y \longmapsto E_{k2}\big(E_{k1}(X)\big)$.



Since the plaintext *X* is encrypted two times with k_1 and k_2, the key-space size of double DES is basically $2^{56} \times 2^{56} = 2^{112}$. However, double DES can be attacked by "meet-in-the-middle", which takes not much more time than 2^{57}. With the "meet-in-the-middle" attack, the attacker knows a pair of plaintext and ciphertext (X, Y). The attacker tries to **decrypt** all 2^{56} values of permutations (identified as z'') and produces a list (w_i'', z_i'') where $w_i'' = DES_{z_i'}^{-1}(Y)$, and z_i'' is all 2^{56} values of permutation. The attacker then tries all 2^{56} values of permutation (identified as z') to **encrypt** X and produces a list (w_i', z_i') where $w_i' = DES_{z_i'}(X)$. The attacker then sorts the lists (w_i', z_i') in w_i' assending order, and (w_i'', z_i'') *in* w_i'' ascending order. The attacker is able to compare these two lists and determine the keys. If a match $(w_i' = w_i'')$ is found, then z_i'' is $k_2$and z_i' is k_1. With this attack, the number of operations is equal to the sum of the number of decryption $\left(w_i'' = DES_{z_i'}^{-1}(Y)\right)$ and the number of encryption $\left(w_i = DES_{z_i'}^{-1}(Y)\right)$. Hence the total number of operation required equals $2^{56} + 2^{56} = 2^{57}$. In order words, the effective key space is only 2^{57} bits and not 2^{112} bits.

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.

Suggested answer:

(i) Setup:

- Bob has (d, e), a (private, public) key pair, and $N=pq$, where p, q are large primes, associated with Bob.
- For a message m, that Alice wants Bob to sign, Alice constructs $\mu = mr^e mod\ N$, where $r \in_R Z_N^* \ and\ e\ is\ Bob's\ public\ key$, and sends μ to Bob. μ is known as the blinded message.
- Bob signs μ using his private key d, and sends his signature $s' = \mu^d\ mod\ N$ back to Alice. The signature s' that Alice receives is Bob's signature on the blinded message.
- Alice then verify that Bob actually sign the blinded message by dividing Bob's blind signature s' by r, such that $S = \frac{s'}{r}\ mod\ N = r^{-1}s'\ mod\ N$, to verify that it is correct.

(ii) Alice can verify that the message was signed by Bob by computing:

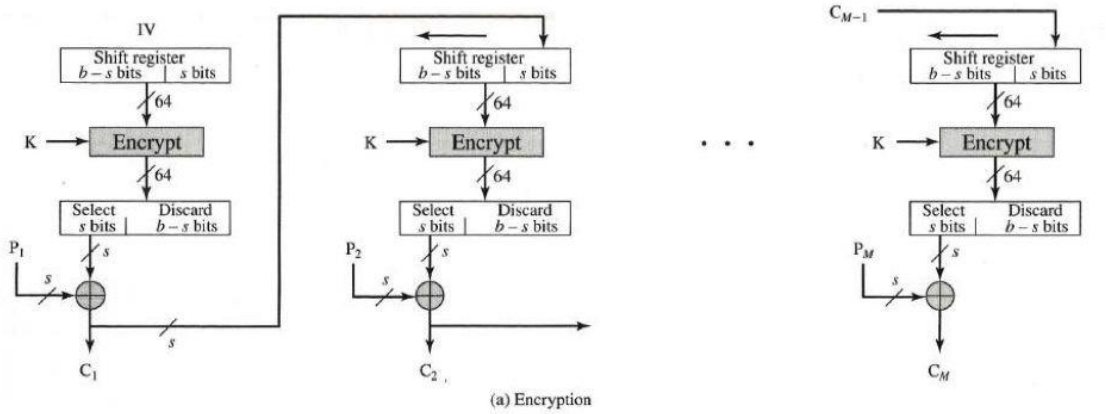
$$S = \frac{s'}{r}\ mod\ N$$
$$= \frac{\mu^d}{r}\ mod\ N$$
$$= \frac{(mr^e)^d}{r}\ mod\ N$$
$$= \frac{(m^d r^{ed})}{r}\ mod\ N \qquad \text{Since ed = 1 mod N,}$$
$$= \frac{m^d r}{r}\ mod\ N$$
$$S = m^d\ mod\ N$$

$$Hence,\ m = S^e\ mod\ N$$
$$= (m^d)^e\ mod\ N$$
$$m = m$$

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.

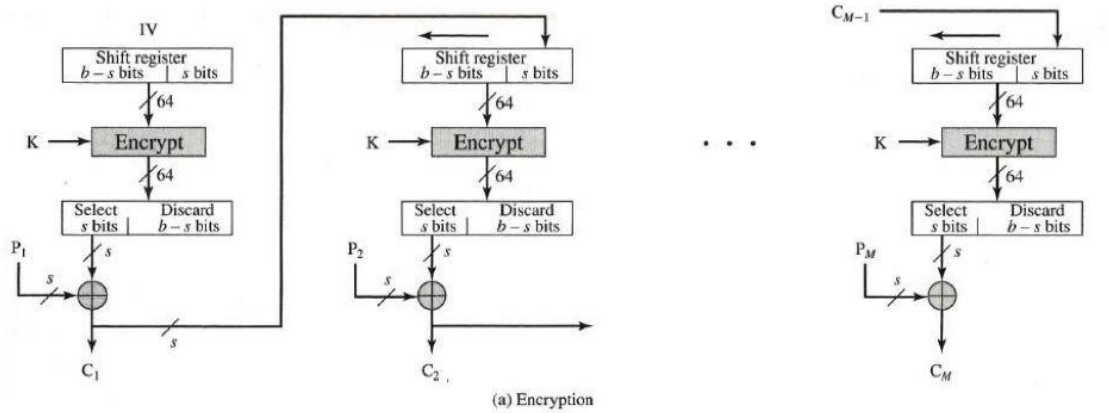


(ii) What are the advantages and disadvantages of the CFB mode of operation?

Suggested answer:

(i)

To decrypt, the same scheme is used, except that the received ciphertext unit is XORed with the output of the encryption function to produce the plaintext unit. The s-bit CFB decryption is as follow:



The mathematical formula to decrypt is

$$P_i = C_i \oplus S_s[E(K, C_{i-1})], \text{where } C_0 = IV \text{ (Initial Vector)}.$$

(ii)

Advantages:

- Same encryption function is used to encrypt and decrypt.
- The message (plaintext) does not need to be padded to a multiple of the cipher block size.
- Decryption can be done with just two adjacent cipher blocks, and hence decryption can be parallelized.

Disadvantages:

Due to the chaining of ciphertext, the encryption cannot be parallelized, however, the decryption is possible.

END OF TEST