Student Number

The University of Melbourne

Department of Computing and Information Systems

COMP90043-CRYPTOGRAPHY AND SECURITY

Practice Exam 2016

Exam Duration: 120 minutes.

Reading Time: 15 minutes.

Length: This paper has 9 pages including this cover page.

Authorised Materials: None.

Instructions to Students: Answer all the questions on the exam question paper. Total marks for the exam is 50. This exam is worth 40% of the final mark in the subject;

Calculators: No Calculators are permitted.

Library: This paper must be returned and not taken out of the exam hall.

continued on next page

1. (2 marks) This question contains several multiple choice questions. For each question, circle exactly one of the choices.

   (a) The science of breaking ciphers is called–

   i. Cryptography.
   ii. Cryptology.
   iii. Cryptanalysis.
   iv. Decryption.

   (b) CVE stands for–

   i. Common Vulnerability Exposure.
   ii. Critical Vulnerability Evaluation.
   iii. Critical Vulnerability Exposure.
   iv. None of the above.

   (c) If a and b are the secrets used by Alice and Bob respectively in Diffie-Hellman key exchange protocol, the common secret shared by Alice and Bob at the end of the protocol is –

   i. $a \cdot b$.
   ii. a^b.
   iii. b^a.
   iv. None of the above.

   (d) (1 mark) What is the use of Encryption?

   i. Integrity.
   ii. Non-repudiation.
   iii. Confidentiality.
   iv. All of the above.

2. (2 marks) Are the following statements true or false? Indicate your choice by printing "TRUE" or "FALSE" next to the statements.

T (a) The OSI security architecture provides a systematic framework for defining security attacks, mechanisms, and services.

T (b) Finite fields of size p can be defined using arithmetic mod p, where p is a prime number.

true F (c) The number 37 is prime so therefore all of the positive integers from 1 to 36 are relatively prime to 37.

F (d) Timing attacks are ciphertext attacks that are only applicable to RSA.

continued on next page

3. (10 marks) Fill in the blanks.

(a) x^{p-1} *mod* $p, x \neq 0, p$ is a prime $=$ 1 _____.

(b) x^{101} *mod* 101, $=$ x _____.

(c) $\phi(p) =$ p-1 _____-,
where p is a primes and ϕ is the Euler's function.

(d) Let $m \geq 1$, $(1 + 2 + 3 + 4 + ... + m)$ mod $(m + 1)$, $=$ 0 if m is even, or (m+1)/2 if m is odd _____-

(e) $(18 + 23)$ *mod* 26$=$ 15 _____-,

(f) 22^{-1} *mod* 23. 22

(g) $2^{144}3^{132}5^{100}$ *mod* 4 $=$ 0 _____-.

(h) Let $m \geq 1$, $(1 + 2 + 4 + 8 + ... + 2^{m-1})$ mod $(2^m) =$ -1 _____-

(i) In the context of network security, access control _____- is the ability to limit and control the access to host systems and applications via communications links.

non-repudiation

(j) digit signature _____- prevents either sender or receiver from denying a transmitted message. Thus, when a message is sent, the receiver can prove that the alleged sender in fact sent the message and when a message is received, the sender can prove that the alleged receiver in fact received the message.

4. (3 marks)

(a) What are the two important requirements of symmetric encryption as discussed in textbook?
1. a strong encrypt algorithm
2. key is only known to the sender and receiver

(b) Explain the workings of the classical substitution cipher. mono alphabetic cipher
substitute the letter in the plaintext with the kth letter before/after it

(c) How many possible keys exist in a classical substitution cipher?
25
26!

continued on next page

5(b)
1. it can hash arbitrary length of message
2. it produces a fixed length output
3. preimage resistance: it's cpt hard to find m such that h(m) equals to a specifiic hash value
4. second preimage resistance: cpt hard to find x != y such that h(x)=h(y)
5. collision resistance: cpt hard to find any two different messages such that have the same hash
6. it's should be a one-way function

5. (3 marks)

(a) Explain why CRC checksum used in network protocols cannot be used as a cryptographic hash function. 1.it doesn't have collision resistance 2. it's not a one-way function

(b) What are the five basic requirements for cryptographic hash functions?

(c) Explain the birthday attack for hash functions. What does this attack imply for the security of hash functions?

assume x is the message of length m which is to be signed, generate 2^(m-1) variations of x' with the correct meaning, and generate 2^(m-1) variations of y' which is the fraud message, compare x' and y' to find one pair with the same hash. get x' signed and replace it with y' it implies the collision resistance attack

6. (2 marks) What is a replay attack? Give an example of a reply attack and its counter measure.

replay attack is the case that the attacker copies the message which was valid in the past and resend it to the receiver.
for example, an attacker intercept the message from A with the valid signature, and resend it to B in the future pretending he's A.
the counter measure could be add timestamp to the message which is to be sent. or add sequence number to every message. or using challenge/respong scheme

7. (3 marks) Consider the finite field $GF(2^3)$ as poynomails modulo $1 + x^2 + x^3$.

i	Elements:x^i	As Polynomials	As Vectors
$-\infty$	0	0	$[0,0,0]$
0	1	1	$[1,0,0]$
1	x	x	$[0,1,0]$
2	x^2	x^2	$[0,0,1]$
3	x^3	1+x^2	[1,0,1]
4	x^4	1+x+x^2	[1,1,1]
5	x^5	1+x	[1,1,0]
6	x^6	x+x^2	[0,1,1]
7	x^7	1	$[1,0,0]$

Table 1: Elements of $GF(2^3)$ as powers of x

(a) Complete the polynomial representations of the missing elements of the table.

(b) Find y such that

$$y\ x^2 = 1.$$

x^5 = 1+x

(c) Solve the equation in y: $xy = x^3$. x^2

(d) Compute $x^3 + x^6 + x^5$; 0

continued on next page

8. (4 marks) This question is about computing the inverse of a number modulo n, where n a positive integer. Note: Inverse of a number a mod n is a number x such that $xa = 1 \bmod n$.

   (a) The Extended GCD algorithm ($XGCD$), also known as the Euclidean algorithm, takes two given integers a and b as inputs and returns three integers g, x and y such that

   $$a\ x + b\ y = g,$$

   where g is the greatest common divisor of the input integers.
   Write a pseudocode for the function **inverse modulo** n using the XGCD function given above. NOTE: There is no need for you write XGCD function.

inverse(a,n) g,x,y = a XGCD(x,n) g=1 x "doesn't exist".

   (b) You have been given the results from the XGCD function below:

   i. $XGCD(11137, 56799) = 1, 18916, -3709$

   ii. $XGCD(22, 67) = 1, -3, 1$

   iii. $XGCD(23, 37) = 1, -8, 5$

   Now determine the inverse of the following numbers:

   i. 22 mod 67 64

   ii. 11137 mod 56799 18916

   iii. 23 mod 37 29

   iv. 37 mod 23 doesn't exist 5

continued on next page

9. (4 marks) Consider the ElGamal crypto system over the prime field $GF(q)$ given in lectures. Let $y_A = a^{x_A} \bmod q$ be the public key of Alice, where $x_A, 1 < x_A < q-1$ is the private key and a is a primitive element in the field.

   (a) Define ElGamal encryption and decryption functions.

   (b) State the hard problems on which the scheme is based.

encryption:
choose a random number k where 1 < k < q-1,
the one-time key will be K = yA^k mod q,
C1 = a^k mod q-1, C2 = KM
send the encryption result as (C1, C2)

decryption:
get the key K from C1: K = C1^xA mod q-1
compute K^-1 mode q-1
decrypt the message from C2: M = C2K^-1

it is based on 1. the computational DH problem, which is that given g^a and g^b, it hard to compute g^ab
2. discrete logarithm problem

10. (4 marks) Alice and Bob exchange their authentic RSA key parameters. Let n_a, e_a and n_b, e_b be public RSA parameters of Alice and Bob respectively. Similarly let d_a and d_b be private RSA keys of Alice and Bob respectively. Let $E_k()$ and $D_k()$ be encryption and decryption functions of the popular symmetric key cipher AES. Bob wants to send a large file *FILE* to Alice as explained below:

    (a) Chooses a random session key k_s, and encrypts as $C = k_s^{e_a} \bmod n_a$.

    (b) Encrypts *FILE* using the AES cipher as: $ENC\_FILE = E_{k_s}(FILE)$.

    (c) Computes $h = \text{HASH}(FILE)$, where HASH is a public hash function.

    (d) Computes the signature as $S = h^{d_b} \bmod n_b$.

    (e) Sends (ENC_FILE, C, S) to Alice.

    Now complete the missing parameters in the following steps to be performed by Alice if the messages are error free and not tampered.

    (a) $k_s =$ C^da ..... $\bmod n_a$.

    (b) $FILE\_RECEIVED =$ Dks(ENC_FILE).....

    (c) $\hat{h} = \text{HASH}($FILE_RECEIVED.....$)$.

    (d) $S^{e_b} \bmod n_b =$ h_hat.....

continued on next page

11. (4 marks) The following equations and figure describe one of the standard modes of usage of symmetric key encryption.

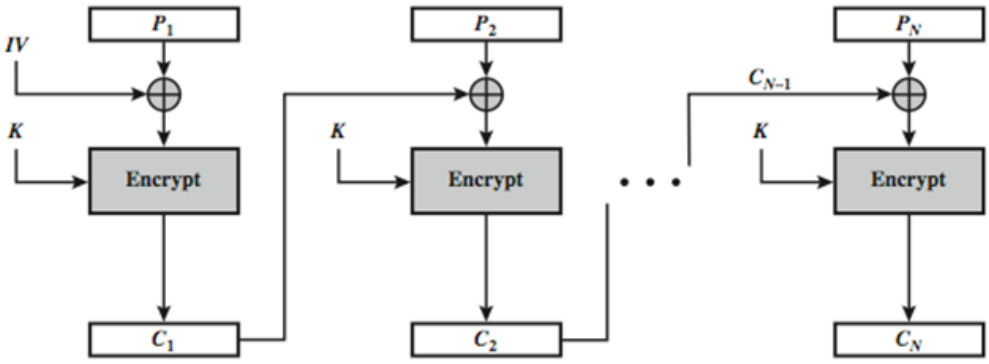

Figure 1: A Standard Mode of Encryption

Encryption:

$$C_1 = (E_K[IV \oplus P_1]).$$
$$C_j = (E_K[C_{j-1} \oplus P_j]), j > 1.$$

(a) What is the name of this mode?

CBC

(b) Expand the abbreviations and functions used in the equations:

i. IV = initial vector
ii. K = encryption key
iii. C_j = the jth block of ciphertext
iv. P_j = the jth block of plaintext
v. $E_y[x]$ = the encryption of x using the key y

(c) Complete the equations for decryption below:

Decryption:
P_1 = Dk[IV+C1].
P_j = Dk[Pj-1 + Cj], j > 1.

(d) What is the effect on the plain text of a one bit error in the transmission of an encrypted "block C_j"?

Pj and the following block Pj+1 will be affected

continued on next page

12. (4 marks)

DH key exchange
KDC

(a) List four general categories of schemes for the distribution of public keys. Briefly explain one of the schemes.

(b) Consider the hierarchy of Certificate Authorities (CAs) as in Figure 2. Show

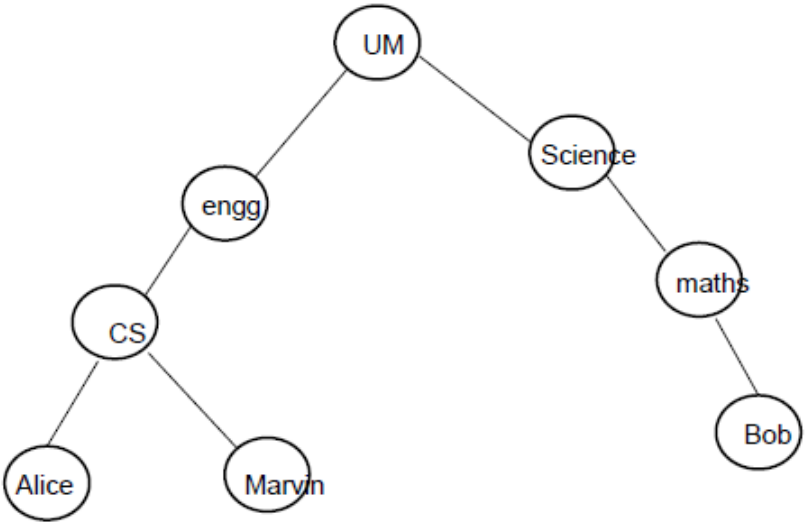

Figure 2: A Hierarchy of Certificate Authorities.

an example of certificates used to navigate the hierarchy. What is the chain of certificates that user Alice needs to obtain in order to establish a certificate path to Bob? You can use X.509 conventions for the certificate chain discussed in the book, for example the certificate for Alice by the CA CS is represented as CS <Alice>.

1. one-way function
2. input arbitrary length
3.output fixed length
4. preimage resistance
5. second preimage resistance
6. collision resistance

13. (5 marks) This question is about hash and MAC.

(a) What are the standard requirements of a cryptographic hash function?

(b) What is the main difference between hash functions and message authentication codes (MAC)? hash function cannot used as authentication by itself. it needs to be encrypted by an additional key
MAC uses a key

(c) Assume that Alice and Bob share a common key k. Then consider the following protocol:

1. Alice computes $\text{MAC}_k(M_s) = m_a$ on the message M_s
2. Alice $\rightarrow$ BoB : $< M_s \parallel m_a >$
3. Bob receives $< M_r \parallel m_a >$
4. Bob computes $\text{MAC}_k(M_r)$ and verifies if $m_a = \text{MAC}_k(M_r)$ holds.
5. Accepts M_r if 4 holds, else rejects.

Rewrite the above protocol using only a standard cryptographic hash function. Note: In the above protocol, $a \parallel b$ represents concatenation of a and b.

Alice encrypts the message EM = Ek(M)
Alice computes the hash of the message m=H(EM)
Alice sends Bob <EM II m>
Bob computes the hash of received message ms=H(EMs)
accepts EMs if ms = m

continued on next page

(d) (3 marks) In RSA, it is a normal practice to sign a $h(M)$, where h is an appropriate hash function instead of signing the message M directly. Explain why this is necessary.

with the hash function, can sign arbitrary length of message
and an appropriate hash function should have one-way property, preimage resistance,
second preimage resistance, and collision resistance. so it is cpt hard to find any other
message which is different from M with the same hash value

END OF EXAMINATION