**Student Number**

The University of Melbourne

Department of Computing and Information Systems

# COMP90043-CRYPTOGRAPHY AND SECURITY

November, 2017

**Exam Duration:** 120 minutes.

**Reading Time:** 15 minutes.

**Length:** This paper has 18 pages including this cover page.

**Authorised Materials:** None.

**Instructions to Students:** Print your student number at the writing box given at the top of this page. Answer all questions in this exam booklet. 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.

**For Marking only:** The following table will be used to record the marks. Do not write anything in the table below.

| 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |

 *continued on next page*

1. (10 marks) Fill in the blanks.

   (a) $5^8$ *mod* 15 = .....10.....

   (b) $(14 + 18)$ *mod* 26= .....6.....

   (c) Let $p$ be a prime number. Then for any $x$, $x^p$ *mod* $p$ = .....X.....

   (d) $12^{-1}$ *mod* 13 = .....1.....

   (e) $2^{120}6^{12}5^{33}$ *mod* 7 = .....6.....

   (f) $\phi(p_1\ p_2)$ = .....$(p_1 - 1)(p_2 - 1)$.....
   where $p_1$ and $p_2$ are distinct primes and $\phi$ is the Euler's function.

   (g) The hash value of a message in the .....Digital Signature..... application is encrypted with a user's private key.

   (h) An .....active..... attack attempts to alter system resources or affect their operation.

   (i) The ticket-granting ticket is encrypted with a secret key known only to the Authentication Server (AS) and the .....Ticket-granting server ( TGS )

   (j) Public-key encryption schemes are secure only if the authenticity of the .....public key..... is assured.

 *continued on next page*

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

   (a) The three concepts that form what is often referred to as the CIA triad are ..... These three concepts embody the fundamental security objectives for both data and for information and computing services.

   i. confidentiality, integrity and availability.
   ii. communication, integrity and authentication.
   iii. confidentiality, integrity, access control.
   iv. communication, information and authenticity.

   (b) Two integers are ..... if their only common positive integer factor is 1.

   i. relatively prime
   ii. congruent modulo
   iii. polynomials
   iv. residual

   (c) A common item of authentication information associated with a user is a.....

   i. nonce
   ii. timestamp
   iii. ticket
   iv. password

   (d) Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to verify the source and integrity of the data unit and protect against forgery is

   i. a security audit trail.
   ii. a digital signature
   iii. an encipherment
   iv. an authentication exchange

 *continued on next page*

3. (2 marks) Are the following statements true or false? Indicate your choice by printing "TRUE" or "FALSE" next to the statements.

   (a) The data integrity service inserts bits into gaps in a data stream to frustrate traffic analysis attempts. F

   (b) With the use of symmetric encryption, the principal security problem is maintaining the secrecy of the key. T

   (c) Although public announcement of public keys is convenient, anyone can forge a public announcement. T

   (d) One means of forming a MAC is to combine a cryptographic hash function in some fashion with a secret key. T

4. (2 marks) This question is about authentication protocols.

   What are the four general means of authenticating a user's identity discussed in the course? Explain each means with an example.

① Something the individual knows: password, PIN

② Something the individual processes: smart cards, key cards

③ Something the individual is (static biometrics): fingerprint

④ Something the individual does (dynamic biometrics): recognition of voice pattern, handwriting characteristics, typing rhythm



*continued on next page*

5. Classical Ciphers (6 marks)

(a) The Vatsyana cipher is a specific version of a classical substitution cipher with the following two conditions:

i. A character $x$ is mapped to another distinct character $y$ and

ii. If a character $x$ is mapped to $y$, then the character $y$ will be mapped to $x$. In other words, substitution happens in pairs where the characters in each pair are mapped to each other.

How many possible keys are there when the cipher is defined over 26 English characters?

$25 \cdot 23 \cdot \cdots 1 = \prod_{i=0}^{12} (2i+1)$

$\therefore$ there are $\prod_{i=0}^{12} (2i+1)$ possible keys

(b) Consider the Vegenere cipher defined over the alphabet $\{0, 1, \cdots 25\}$. The key can be any string of length between $m_1$ to $m_2$ characters. What is the size of the key space?

$26^{m_1} + 26^{m_1+1} + \cdots + 26^{m_2} = 26^{m_1} \cdot \frac{1 - 26^{m_2 - m_1 + 1}}{1 - 26}$

 *continued on next page*

(c) Consider the following version of a classical cipher where plain text and cipher text elements are from integers from 0 to 25. The encryption function, which takes any plain text $p$ to a cipher text $c$, is given by

$$c = E_{[a,b]}(p) = (ap + b) \ mod \ 26,$$

where $a$ and $b$ are integers less than 26.

Show how an adversary can attack the system under the "Chosen Plaintext Attack" model.

① Consider each characters in the alphabet as a ciphertext and find the plaintext of it (or choose one ciphertext contains all the 26 characters in the alphebet and get the plaintext of it)

② generate a map using the result of step①

so we can easily decrept any cipher text



*continued on next page*

6. (5 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 $xa = 1 \bmod n$. In this semester, we studied methods for finding inverse modulo $n$ using the Extended GCD algorithm ($XGCD$) and Fermat's or Euler's theorems.

   (a) When $n$ is a prime number, write a pseudocode for the function inverse modulo $n$ using the properties of the Fermat's theorem.

Theory: $a^{n-2} \cdot a \equiv a^{n-1} \bmod n \equiv 1 \bmod n$

```
function inverse(a, n):
    if a, n relatively prime:
        return a^(n-2) mod n
    else:
        return "no inverse"
```

 *continued on next page*

(b) 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.

You have provided the results from the XGCD function and exponentiation modular identities below:

i. $XGCD(12986, 46799) = 1, 8905, -2471$

ii. $XGCD(12, 39) = 3, -3, 1$

iii. $XGCD(17, 29) = 1, 12, -7$

iv. $12^{29} \bmod 31 = 13$

v. $10^{29} \bmod 31 = 28$

Now determine the inverse of the following numbers:

i. 12 mod 39 no inverse

ii. 12986 mod 46799 8905

iii. 17 mod 29 12

iv. 12 mod 17 10

v. 12 mod 31 13

vi. 10 mod 31 28

 *continued on next page*

7. (3 marks) This question is about computations in a finite field. Consider $\mathbf{GF}(2^3) = \mathbf{GF}(2)[x]$ *mod* $(x^3 + x + 1)$, a field with 8 elements.

   (a) Express all the elements of $\mathbf{GF}(2^3) = \mathbf{GF}(2)[x]$ *mod* $(x^3+x+1)$ as powers of the element $x$.

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

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

   (b) What is the inverse of $x^3$ in the field?

inverse : $x^4 = x^2 + x$

   (c) Solve for $t$ and $w$ in the following simultaneous equations over the field.

$$x^2\ t + x^4 w = 1;$$

$$t + w = 1;$$

$\therefore\ t+w=1$

$w = t+1$

$x^2 \cdot t + x^4(t+1) = 1$

$(x^2+x^4)t + x^4 = 1$

$(x^2+x^2+x)t + x^2+x = 1$

$xt + x^2 + x = 1$

$xt + x = 1 + x^2$

$x(t+1) = x^6$

$t+1 = x^5$

$t+1 = x^2+x+1$

$t = x^2 + x$

$w = t+1 = x^2+x+1$



*continued on next page*

8. (4 marks) This question is about hash and MAC.

(a) What is the main difference between hash functions and message authentication codes (MAC)?

In MAC, user use a symmetric key to generate the hash value, which can guarantee both the integrity and authenticity of the message. But hash function can't not guarantee authenticity.

(b) Consider a version of the practical RSA signature algorithm discussed in the lectures. Let $n, e$ be Alice's RSA public key and $d$ be Alice's private key. The signature of a message $m, 0 < m < n - 1$ is given by

$$(m, s = (h(m))^d) \bmod n),$$

where $h$ is a hash function. Answer the following questions:

i. What is the verification equation?

$h(m) = s^e$ ?

or

$h(m) \stackrel{?}{=} s^e$

} which is better?

ii. Describe the "second preimage resistant" property of the hash functions.

For a given $x$, can't find any $y \neq x$ such that $h(x) = h(y)$.


*continued on next page*

iii. What is the consequence if the function $h$ used above satisfies all the requirements of cryptographic hash function except the second preimage resistant property?

How can this happen ?

break second preimage resistant would also break collision resistant right?

9. (3 mark) Assume the RSA signature parameters for this question. Marvin (an adversary) accidentally discovers the following message and signature pairs in Alice's computer.

$$(m_1, s_1) \text{ and } (m_2, s_2),$$

where $s_1 = (m_1)^d \ mod \ n$ and $s_2 = (m_2)^d \ mod \ n$. To his amazement, he discovers that the message he wanted to forge was exactly $m = (m_1^3 \, m_2) \ mod \ n$. Is it possible to forge Alice's signature on the message $m$? If so, describe how to construct a forged signature on the message. Note that in this question we assume the basic textbook RSA signature scheme which do not employ any hash function.

He can, since

$$(m_1^3 m_2)^d = m_1^{3d} \cdot m_2^d \mod n$$
$$= (m_1^d)^3 m_2^d \mod n$$
$$= s_1^3 \cdot s_2 \mod n$$

the signature he wants is $s_1^3 \cdot s_2$


*continued on next page*

10. (4 marks) Consider the ElGamal signature scheme over the prime field $GF(q)$ given in lectures. Let $H$ be a public hash function, $y_A = a^{x_A} \bmod q$ 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. Alice uses the following equation to define the ElGamal signature scheme:

$$k\ S_2 + x_A S_1 = m \bmod (q-1),$$

where $m = H(M)$, $M$ an arbitrary message and $k, S_1$ and $S_2$ are the signature parameters used in the scheme.

(a) What are the signing and verification equations?

Signing: $S_1 = \alpha^k \bmod q$

$S_2 = k^{-1}(m - x_A S_1) \bmod (q-1)$

in which $k^{-1}$ is the inverse of $k \bmod (q-1)$

verification: $V_1 = \alpha^m \bmod q$ $\quad V_1 \text{ eq } V_2 \ ?$

$V_2 = \gamma_A^{S_1} S_1^{S_2} \bmod q$

(b) What is the consequence of using same $k$ for signing two different messages?

Let $S_1'$ be the first messages $S_1$ signature

$S_1''$ be the second messages $S_1$ signature

$$k S_2' + x_A S_1' = m_1 \bmod (q-1)$$

$$k = S_2'^{-1}(m_1 - x_A S_1') \bmod (q-1)$$

$$k S_2'' + x_A S_1'' = m_2 \bmod (q-1)$$

$$S_2'^{-1}(m_1 - x_A S_1') S_2'' + x_A S_1'' = m_2 \bmod (q-1) \quad (1)$$

In formula (1), there is only one variable which means we can solve the equations and get the $x_A$, $S_0$ using the same $k$ would let other know your private key.

 *continued on next page*

11. (4 marks) Consider the following two protocols considered in the subject which are variations of Needham-Schroeder protocol:

**Protocol A (Denning's Protocol):**
1. A $\rightarrow$ KDC: $ID_A \;||\; ID_B$
2. KDC $\rightarrow$ A: $E(K_A, [K_s||ID_B||T||E(K_b, [K_s||ID_A||T])])$
3. A $\rightarrow$ B: $E(K_B, [K_s||ID_A||T])$
4. B $\rightarrow$A: $E(K_s, N_1)$
5. A $\rightarrow$ B $E(K_s, f(N_1))$

**Protocol B (An improvement to Denning's Protocol):**
1. A $\rightarrow$ B: $ID_A \;||\; N_a$
2. B $\rightarrow$ KDC: $ID_B||N_b||E(K_b, [ID_A||N_A||T_b])$
3. KDC $\rightarrow$ A: $E(K_A, [ID_B, N_a||K_s||T_b])||E(K_B, [ID_A, K_s||T_b])||N_b$
4. A $\rightarrow$B: $E(K_b, [ID_A||K_s||T_b])||E(K_s, N_b)$

(a) What is the role of $T$ in Protocol A?

Timestamp: assures fresh keys for A and B using to cope with reply attack.

(b) What is Suppress-Replay Attack?

When the sender's clock is ahead of the recipient's, an opponent can intercept a message from the sender and reply it later when the timestamp becomes current at the recipient's site.

(c) Is Protocol A susceptible to Suppress-Replay Attack? Explain your answer and suggest a remedy if your answer is yes.

Yes, when KDC's clock is ahead of B (recipient) the suppress attack happens.

 *continued on next page*

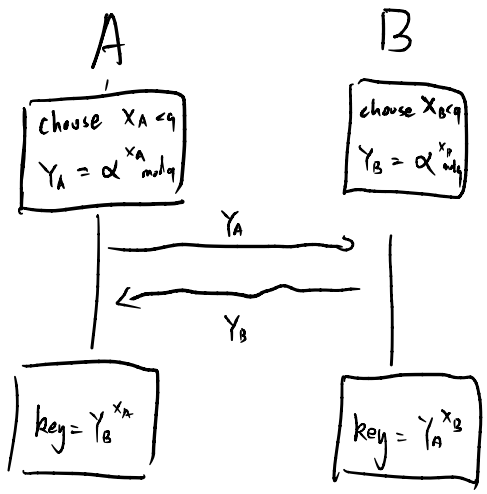
(d) Explain how Protocol B address the above susceptibility.

Since the timestamp (used) is generated by B (recipient) the opponent can't use the time different between A and B.

12. (5 marks)

(a) Describe the Diffie-Hellman (DH) key agreement protocol defined over the group of integers modulo $p$, where $p$ is a prime number. You are welcome to use any assumptions required to complete the statement of the protocol. Your answer should include the public parameters of the scheme and series of messages exchanged between the users A and B.

what is primitive element?




① Assume that A and B share the $p$ and $\alpha$, in which $\alpha < q$ and $\alpha$ is a primitive element

② A generates a private key $X_A$ and a public key $Y_A = \alpha^{X_A} \bmod q$

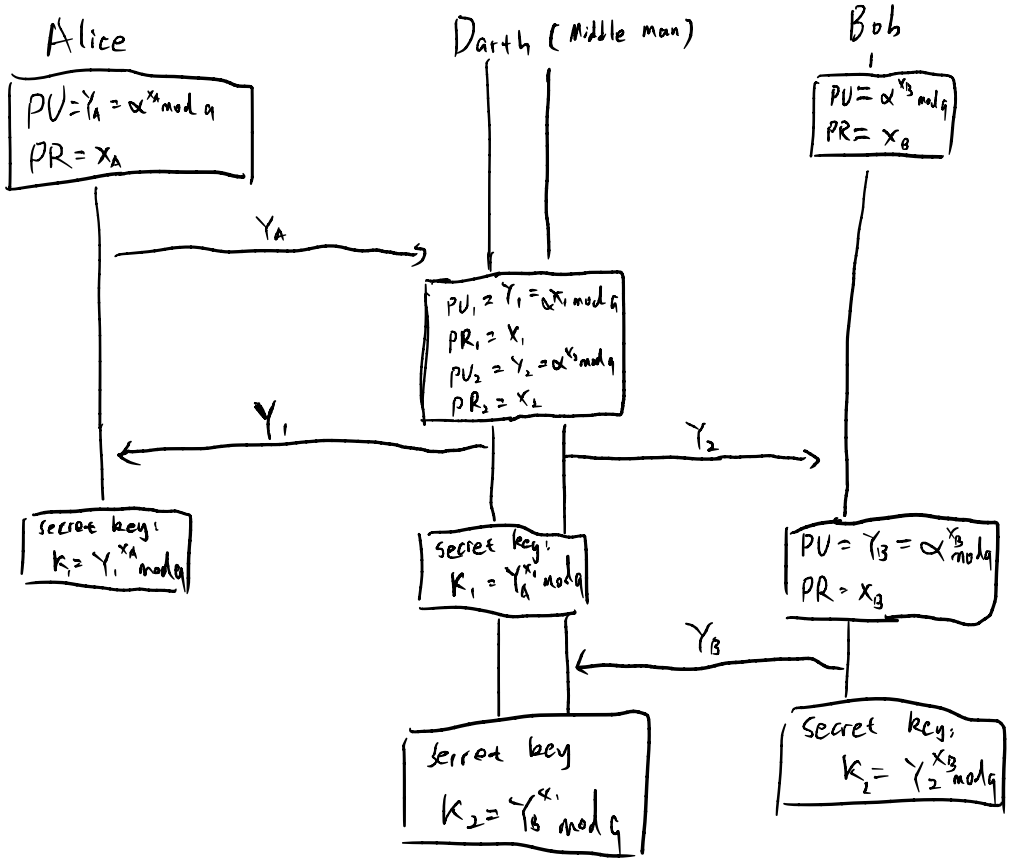
B generates a private key $X_B$ and a public key $Y_B = \alpha^{X_B} \bmod q$

③ they exchange their public key

④ A calculate the shared key by $Y_B^{X_A}$, B calculate the shared key by $Y_A^{X_B}$


*continued on next page*

(b) Show how this protocol is susceptible to a man-in-the-middle attack.

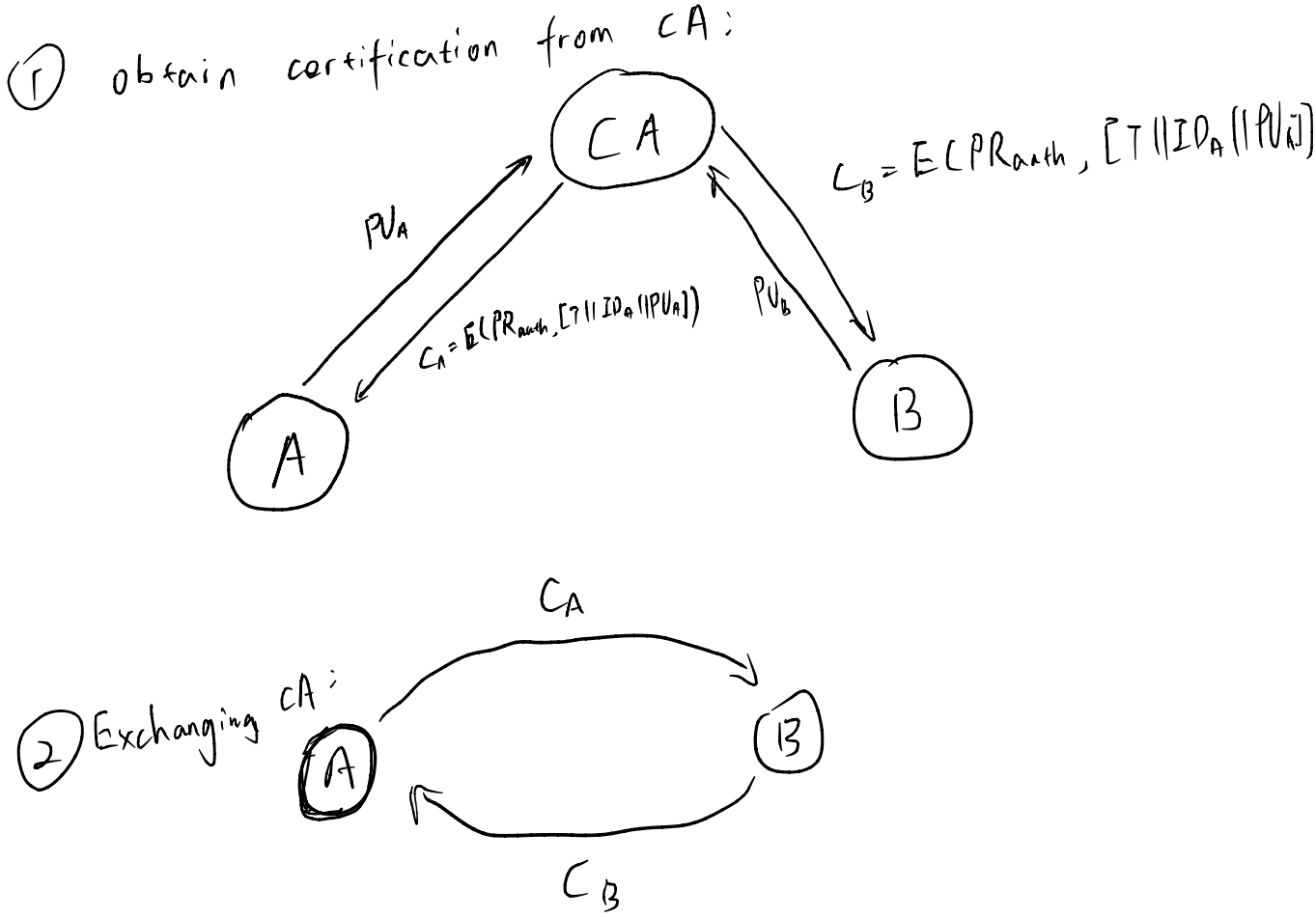



The figure above show how the attack happens.

 *continued on next page*

(c) Modify the protocol in part (a) so that it is secure against the vulnerability found in part (b) using the public key certificate scheme as defined in this subject. Briefly justify your solution. For your benefit, some relevant details about the certificate scheme are given below. You may have to fill in missing details if required.

- Let $[PU_{auth}, PR_{auth}]$ be the public and private key pair of the certificate authority.
- Let $E(PU, .)$ and $D(PR, .)$ be the public key encryption and decryption functions used in the scheme.
- The format of the certificate for a user A is given as $C_A = E(PR_{auth}, [T \parallel ID_A \parallel PU_A])$, where $T$ is a timestamp.




 *continued on next page*