UNIVERSITI TEKNIKAL MALAYSIA MELAKA

UNIVERSITI TEKNIKAL MALAYSIA MELAKA
PEPERIKSAAN AKHIR SEMESTER I
FINAL EXAMINATION SEMESTER I
SESI 2020/2021
***SESSION* 2020/2021**
FAKULTI TEKNOLOGI MAKLUMAT DAN KOMUNIKASI

KOD MATAPELAJARAN ***SUBJECT CODE***	:	**BITS 3463**
MATAPELAJARAN ***SUBJECT***	:	**KRIPTOGRAFI DAN TEORI INFORMASI** ***CRYPTOGRAPHY AND INFORMATION THEORY***
PENYELARAS ***COORDINATOR***	:	**PM DR. NUR AZMAN ABU**
KURSUS ***COURSE***	:	**BITZ**
MASA ***TIME***	:	**2:15 PETANG**
TEMPOH ***DURATION***	:	**3 HOURS**
TARIKH ***DATE***	:	**1 FEBUARY 2020**
TEMPAT ***VENUE***	:	**EXAM HALL 5**

ARAHAN KEPADA CALON
INSTRUCTION TO CANDIDATES

1. **KERTAS SOALAN INI TERDIRI DARI 4 SOALAN DALAM DWI BAHASA.**
   THIS EXAM CONSISTS OF FOUR*(4) *QUESTIONS IN TWO*(2) *VERSIONS.
2. **SOALAN DALAM BAHASA INGGERIS DARI MUKASURAT 2 SAMPAI 6 DAN DALAM BAHASA MELAYU DARI MUKASURAT 7 SAMPAI 11.**
   EXAM QUESTIONS IN ENGLISH ARE FROM PAGE 2 TO 6 DAN IN MALAY ARE FROM PAGE 7 TO 11.
3. **SILA JAWAB SEMUA SOALAN.**
   ANSWER ALL QUESTIONS
4. **TULISKAN JAWAPAN ANDA DIDALAM KERTAS A4 KOSONG.**
   WRITE YOUR ANWERS IN BLANK A4 PAPERS.

KERTAS SOALAN INI TERDIRI DARIPADA SEBELAS(11) MUKA SURAT SAHAJA TERMASUK MUKA SURAT HADAPAN
THIS QUESTION PAPER CONTAINS ELEVEN* (11) *PAGES INCLUSIVE OF THIS FRONT PAGE

INSTRUCTION: *Answer ALL Questions*

QUESTION 1 (20 MARKS)

Suppose you are given 8 symbols to encode. Given the probability distribution of each symbol follows Poisson distribution with parameter λ. Take *i* as the last digit of your matrix id number. Then take $\lambda = \pi + \frac{i}{100}$ where π is a popular constant near 3.14159.

a) Compute a probability density function $P(X=x) = \frac{\lambda^x \cdot e^{-\lambda}}{x!}$ accurate up to 3 decimals.

(2 marks)

Table 1: Probability distribution of 8 symbols

Symbol x	A	B	C	D	F	G	H	I
Numerical x	0	1	2	3	4	5	6	7
$P(X=x)$								

b) Sketch the graph of the probability distribution (pdf).

(2 marks)

c) Build the Huffman tree for the symbols according to the probability distribution.

(6 marks)

d) Assign the binary Huffman code to each symbol.

(2 marks)

e) Compute the average length of Huffman codes of the A-I symbols.

(2 marks)

f) Compute the entropy H_x of symbol x.

(4 marks)

g) Compare your answer in part e) and f). What can you conclude about the performance of the Huffman codes on the given symbols x?

(2 marks)

QUESTION 2 (30 MARKS)

a) Give **FOUR (4)** hierarchical keys in a cryptosystem.

(4 marks)

b) Ultimately, the keys are stored in the system and the entire system may depend on a single master key. Give **TWO (2)** reasons why a master key needs to be protected by a threshold scheme.

(4 marks)

In a Threshold Scheme using Newton Polynomial mod 257, let the policy is $m = 3$ of $n = 5$ shadow keys.

c) Compute 2^{-1} (mod 257) and 4^{-1} (mod 257)

(4 marks)

d) Given the master key K =199 as a_0, the coefficients a_1= 73 and a_2 = 79, generate the shadow keys $\{y_0, y_1, y_2, y_3, \ldots, y_{n-1}\}$ at $\{x_0, x_1, x_2, x_3, \ldots, x_{n-1}\} = \{101, 103, 105, 107, 109\}$ via a polynomial $A(x) = a_0 + a_1 \cdot x + a_2 \cdot x^2 + \ldots + a_{m-1} \cdot x^{m-1} \bmod 257$.

(10 marks)

e) Given three shadow keys; $(x_0, y_0) = (101, 46)$, $(x_1, y_1) = (103, 42)$ and $(x_2, y_2) = (105, 156)$. Generate the divided difference table for Newton interpolation.

(4 marks)

f) Recover the master key from the three shadow keys; $(x_0, y_0) = (101, 46)$, $(x_1, y_1) = (103, 42)$ and $(x_2, y_2) = (105, 156)$ via Newton interpolation at $x = 0$.

(4 marks)

QUESTION 3 (30 MARKS)

a) Refer to Figure 1. Describe **THREE (3)** steps of signature verification

(6 marks)

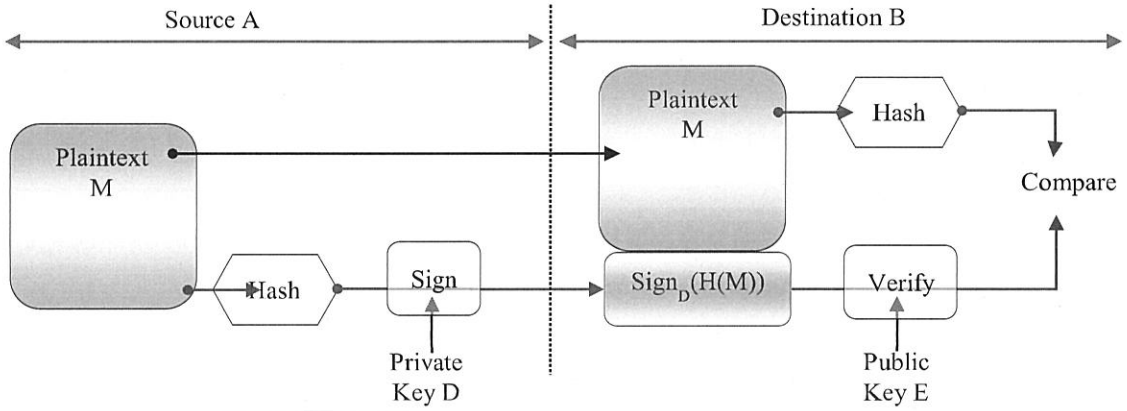


Figure 1: Basic Uses of Hash Functions: It shows the hash being signed with the sender's private key, thus forming a digital signature.

b) Take your matric id as 10 characters including the front letter B. Convert each character into an ASCII code. Pad your 10-character message into 512-bit message block as prescribed in SHA256. Write them in hexadecimals.

(6 marks)

c) There are six logical functions used in SHA-256. Each of these functions operates on 32-bit words and produces a 32-bit word as output. Each function is defined as follows:

$$\lambda(x, y, z) = (x \wedge y) \oplus (x \wedge z)$$
$$\mu(x, y, z) = (x \wedge y) \oplus (x \wedge z) \oplus (y \wedge z)$$
$$\Sigma_0(x) = S^2(x) \oplus S^{13}(x) \oplus S^{22}(x)$$
$$\Sigma_1(x) = S^6(x) \oplus S^{11}(x) \oplus S^{25}(x)$$
$$\sigma_0(x) = S^7(x) \oplus S^{18}(x) \oplus R^3(x)$$
$$\sigma_1(x) = S^{17}(x) \oplus S^{19}(x) \oplus R^{10}(x)$$

Describe each function λ, μ, Σ_0, and σ_1 in simple sentences without using any symbols.

(8 marks)

d) States **FOUR (4)** places a hash function is being used in a cryptosystem.

(4 marks)

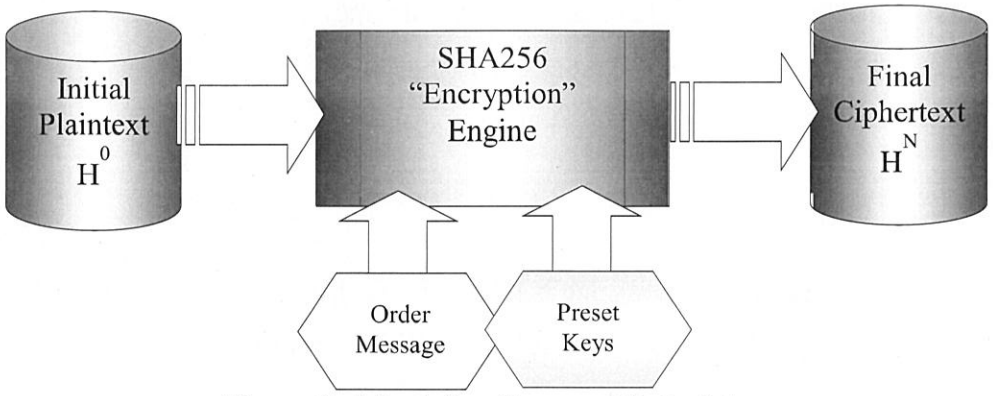


Figure 2: A hash function as a block cipher.

e) Refer to **Figure 2**, give **THREE(3)** steps in order to represent a hash function such as SHA2 as a block cipher.

(6 marks)

QUESTION 4 (20 MARKS)

Given n is the bit size of the plaintext and/or key. In general, the running time of AES, RSA, ECC and NTRU cryptosystems are given in the Table 2 below.

Table 2: Key sizes and the time complexities of 4 major cryptosystems

Algorithm	Key Size (in bits)	Running Encrypt Time	Running Decrypt Time
AES	128-256	$O(k_e \cdot n)$	$O(k_d \cdot n)$
RSA	1024-2048	$O(k_e \cdot n^3)$	$O(k_d \cdot n^3)$
ECC	160-256	$O(k_e \cdot n^3)$	$O(k_d \cdot n^3)$
NTRU	1841-6130	$O(k_e \cdot n^2)$	$O(k_d \cdot n^2)$

a) In general, ECC is faster than RSA and NTRU is faster than ECC. How these differences in speed are practically achieved on RSA, ECC and NTRU cryptosystems?

(2 marks)

b) Give **THREE (3)** latest updates on Quantum computers.

(6 marks)

c) Give **FOUR (4)** difficult mathematical problem on which modern cryptosystems rely on. For each difficult problem, give an example of the cryptosystem which uses it for each intractability.

(4 marks)

d) Give **TWO (2)** technical reasons on why ECC is preferred to an efficient RSA.

(2 marks)

e) Give **TWO (2)** technical reasons on why NTRU is preferred to an efficient ECC.

(2 marks)

f) What are devastating effects of having practical quantum computers on the security of each of the **FOUR (4)** cryptosystems above in Table 2?

(4 marks)

-END OF QUESTIONS-

ARAHAN: *Jawab **SEMUA** soalan*

SOALAN 1 (20 MARKAH)

Katakan terdapat 8 simbol untuk dikodkan. Diberi taburan kebarangkalian bagi setiap simbol berdasarkan Taburan Poisson dengan parameter λ. Ambil *i* sebagai digit terakhir nombor matrix anda. Kemudian ambil $\lambda = \pi + \frac{i}{100}$ dimana π adalah nilai terkenal mendekati 3.14159.

a) Kira taburan kebarangkalian berdasarkan formula $P(X=x) = \frac{\lambda^x \cdot e^{-\lambda}}{x!}$ tepat sehingga 3 titik perpuluhan.

(2 markah)

Jadual 1: Taburan kebarangkalian untuk 8 simbol.

Simbol x	A	B	C	D	F	G	H	I
Nilai x	0	1	2	3	4	5	6	7
$P(X=x)$								

b) Lakarkan graf taburan kebarangkalian (pdf). **(2 markah)**

c) Bina pokok Huffman untuk simbol-simbol tersebut mengikut taburan kebarangkalian. **(6 markah)**

d) Berikan kod Huffman binari kepada setiap simbol. **(2 markah)**

e) Kira purata panjang kod-kod Huffman bagi simbol-simbol A-J. **(2 markah)**

f) Kira nilai entropi H_x bagi simbol-simbol x. **(4 markah)**

g) Bandingkan jawapan anda di bahagian e) dan f). Apa yang boleh anda simpulkan mengenai prestasi kod Huffman pada simbol-simbol x?

(2 markah)

SOALAN 2 (30 MARKAH)

a) Berikan **EMPAT(4)** hierarki kekunci dalam sesebuah sistem kriptografi.

(4 markah)

b) Akhirnya, kekunci yang tersimpan di dalam seluruh sistem kriptografi hanya bergantung pada satu kekunci induk utama. Beri **DUA(2)** sebab mengapa kunci induk utama ini perlu dilindungi oleh skema ambang.

(4 markah)

Dalam sebuah Skema Ambang menggunakan Polinomial Newton modula 257, diberi dasar polisi keselamatannya adalah bersandarkan keberadaan $m = 3$ daripada $n = 5$ kekunci bayangan.

c) Kira 2^{-1} (mod 257) dan 4^{-1} (mod 257)

(4 markah)

d) Diberi kekunci induk utama K =199 sebagai pekali a_0, pekali-pekali a_1= 73 dan a_2 = 79, hasilkan kekunci bayangan $\{y_0, y_1, y_2, y_3, \ldots, y_{n-1}\}$ pada $\{x_0, x_1, x_2, x_3, \ldots, x_{n-1}\}$= {101, 103, 105, 107, 109} melalui sebuah polinomial $A(x) = a_0 + a_1 \cdot x + a_2 \cdot x^2 + \ldots + a_{m-1} \cdot x^{m-1}$ modula 257.

(10 markah)

e) Diberi tiga kekunci bayangan: (x_0, y_0) = (101, 46), (x_1, y_1) = (103, 42) dan (x_2, y_2) = (105, 156), hasilkan taburan *divided difference* table bagi interpolasi *Newton*.

(4 markah)

f) Keluarkan kekunci induk utama dari tiga kekunci bayangan:

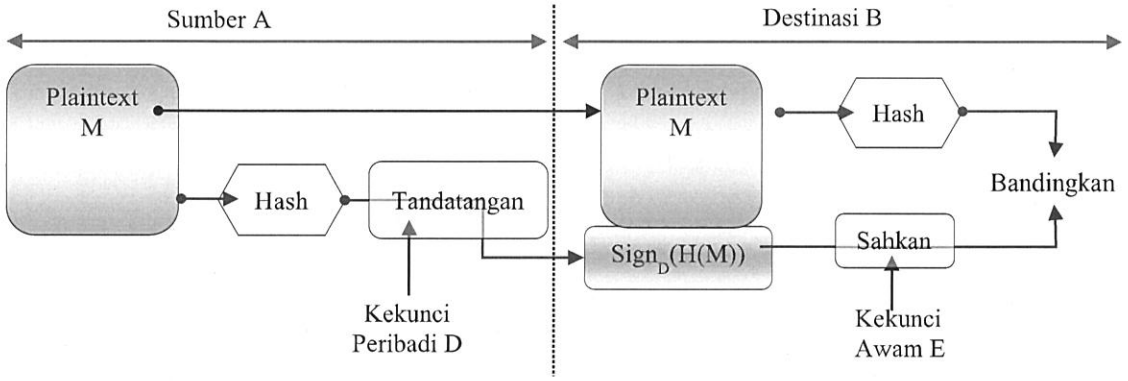
(x_0, y_0) = (101, 46), (x_1, y_1) = (103, 42) dan (x_2, y_2) = (105, 156) melalui interpolasi Newton pada nilai $x = 0$.

(4 markah)

SOALAN 3 (30 MARKAH)

a) Merujuk kepada **Rajah 1**. Jelaskan **TIGA(3)** langkah-langkah pengesahan tanda tangan digital.

(6 markah)



Rajah 1. Gambaran nilai hash ditandatangan dengan kekunci peribadi pengirim

b) Ambil nombor kad matrik anda sebagai 10 aksara termasuk huruf depan B. Tukarkan setiap aksara menjadi kod ASCII. Masukkan mesej 10 aksara anda ke dalam blok mesej 512-bit seperti yang ditetapkan dalam SHA256. Tuliskannya dalam hexa. Ambil id matrik anda sebagai 10 aksara termasuk huruf depan B. Tukarkan setiap aksara menjadi kod ascii. Masukkan mesej 10 aksara anda ke dalam blok mesej 512-bit seperti yang ditetapkan dalam SHA256. Tuliskan jawapan anda dalam hexa.

(6 markah)

c) Terdapat enam fungsi logik yang digunakan dalam SHA-256. Setiap fungsi ini beroperasi pada input 32-bit dan menghasilkan output 32-bit. Setiap fungsi ditakrifkan sebagai berikut:

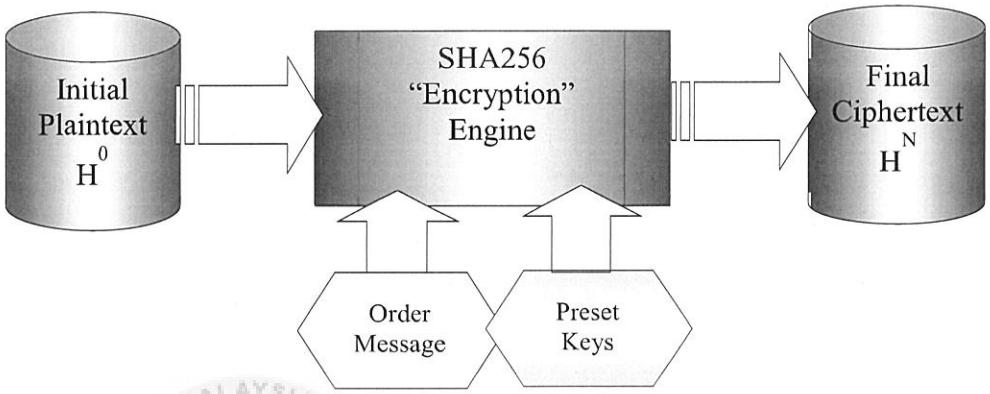
$$\lambda(x, y, z) = (x \wedge y) \oplus (x \wedge z)$$
$$\mu(x, y, z) = (x \wedge y) \oplus (x \wedge z) \oplus (y \wedge z)$$
$$\Sigma_0(x) = S^2(x) \oplus S^{13}(x) \oplus S^{22}(x)$$
$$\Sigma_1(x) = S^6(x) \oplus S^{11}(x) \oplus S^{25}(x)$$
$$\sigma_0(x) = S^7(x) \oplus S^{18}(x) \oplus R^3(x)$$
$$\sigma_1(x) = S^{17}(x) \oplus S^{19}(x) \oplus R^{10}(x)$$

Huraikan setiap fungsi λ, μ, Σ_0, dan σ_1 dalam ayat mudah difahami tanpa menggunakan apa-apa simbol.

(8 markah)

d) Nyatakan **EMPAT(4)** tempat fungsi hash digunakan dalam sesebuah sistem kriptografi.

(4 markah)



Rajah 2: A hash function as a block cipher.

e) Merujuk kepada **Rajah 2**, berikan **TIGA(3)** langkah atau elemen untuk mewakili fungsi hash seperti SHA2 sebagai sebuah sipher blok.

(6 markah)

SOALAN 4 (20 MARKAH)

Diberikan saiz pesanan terbuka dan/atau kekunci n. Secara umumnya, perjalanan masa pengiraan sistem kriptografi AES, RSA, ECC dan NTRU diberikan seperti dalam Jadual 2.

Jadual 2: Saiz kekunci dan pengolahan masa bagi 4 sisitem kripto ternama

Algorithma	Saiz Kekunci (dalam bit)	Pengolahan Masa Penyulitan	Pengolahan Masa Penyahsulitan
AES	128-256	$O(k_e \cdot n)$	$O(k_d \cdot n)$
RSA	1024-2048	$O(k_e \cdot n^3)$	$O(k_d \cdot n^3)$
ECC	160-256	$O(k_e \cdot n^3)$	$O(k_d \cdot n^3)$
NTRU	1841-6130	$O(k_e \cdot n^2)$	$O(k_d \cdot n^2)$

a) Secara umum, ECC lebih pantas daripada RSA dan NTRU lebih cepat daripada ECC. Bagaimana perbezaan kelajuan ini dapat dicapai secara praktikal pada sesebuah system kripto RSA, ECC dan NTRU? **(2 markah)**

b) Berikan **TIGA(3)** perkembangan terbaru dalam pembangunan computer Quantum. **(6 markah)**

c) Berikan **EMPAT(4)** permasalahan matematik sukar yang menjadi asas di dalam sistem kriptografi moden hari ini. Berikan contoh sistem kriptografi bagi setiap permasalahan matematik sukar yang digunakan. **(4 markah)**

d) Beri **DUA(2)** sebab teknikal mengapa ECC lebih digemari berbanding dengan RSA yang cekap. **(2 markah)**

e) Beri **DUA(2)** sebab teknikal mengapa NTRU lebih digemari berbanding dengan ECC yang agak laju. **(2 markah)**

f) Apakah kesan dari komputer Kuantum ke atas status keselamatan setiap **EMPAT(4)** sistem kriptografi diatas dalam Jadual 2? **(4 markah)**

- SOALAN TAMAT -