UNIVERSITI TEKNIKAL MALAYSIA MELAKA

UNIVERSITI TEKNIKAL MALAYSIA MELAKA
PEPERIKSAAN AKHIR SEMESTER I
FINAL EXAMINATION SEMESTER I
SESI 2021/2022
***SESSION* 2021/2022**
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***	:	**9:00 – 11:30 PAGI**
TEMPOH ***DURATION***	:	**2 and ½ HOURS**
TARIKH ***DATE***	:	**24 JANUARY 2021**
TEMPAT ***VENUE***	:	**EXAM HALL 5**

ARAHAN KEPADA CALON
INSTRUCTION TO CANDIDATES

1. **KERTAS SOALAN INI TERDIRI DARI 5 SOALAN DALAM DWI BAHASA.**
   THIS EXAM CONSISTS OF FIVE*(5) *QUESTIONS IN TWO*(2) *VERSIONS.
2. **SOALAN DALAM BAHASA MELAYU DARI MUKASURAT 2 SAMPAI 6 DAN DALAM BAHASA INGGERIS DARI MUKASURAT 7 SAMPAI 11.**
   EXAM QUESTIONS IN MALAY ARE FROM PAGE 2 TO 6 DAN IN ENGLISH ARE FROM PAGE 7 TO 11.
3. **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

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 dan isikan ke dalam Jadual 1.

(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 dari Jadual 1.

(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-I.

(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 (20 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)

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

i. Diberi kekunci induk utama $K = 199$ sebagai pekali a_0, pekali-pekali $a_1 = 73$ dan $a_2 = 79$, hasilkan kekunci bayangan $\{y_2, y_3, \ldots, y_{n-1}\}$ pada $\{x_2, x_3, \ldots, x_{n-1}\} = \{105, 107, 109\}$ 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.

(6 markah)

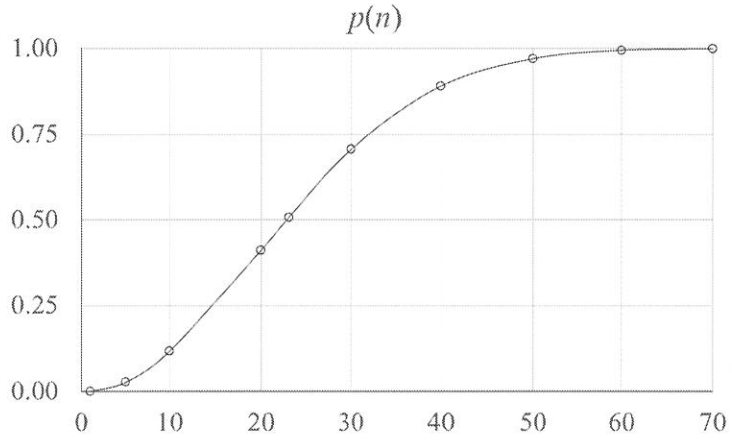
ii. Diberi tiga kekunci bayangan: $(x_0, y_0) = (101, 46)$, $(x_1, y_1) = (103, 42)$ dan $(x_2, y_2) = (105, 156)$, hasilkan taburan *divided difference* table bagi interpolasi *Newton*.

(4 markah)

iii. 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 $x = 0$.

(2 markah)

SOALAN 3 (20 MARKAH)



Rajah 1: Probabilities of at least two people sharing a birthday

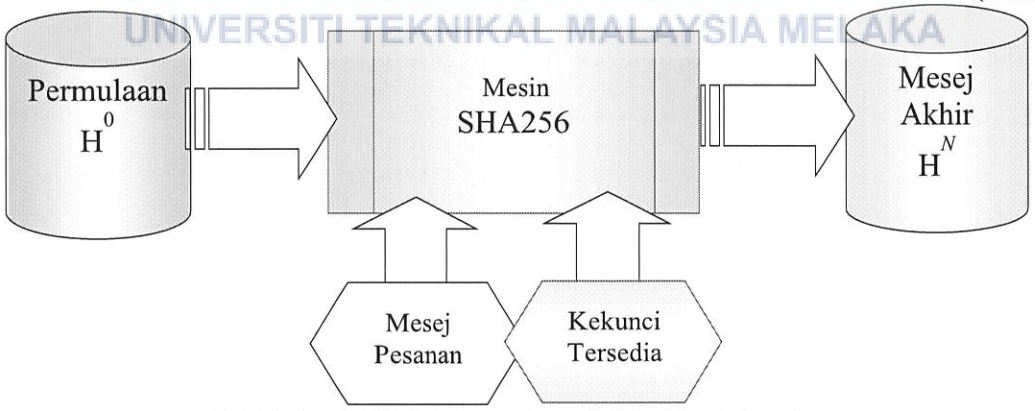
a) Merujuk kepada keberangkalian sekurang-kurang dua dari *n* orang berkongsi harjadi dalam Rajah 1, berikan **DUA (2)** penjelasan tentang *Paradox* Harijadi dikalangan 15 hingga 30 orang. **(4 markah)**

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

(4 markah)



Rajah 2: Fungsi cincang sebagai sebuah sipher blok.

d) 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 blok mesej dan/atau kekunci *n*. Sila rujuk perjalanan masa pengiraan sistem kriptografi AES, RSA, ECC dan NTRU yang 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	$O(k_e \cdot n^2)$	$O(k_d \cdot n^2)$

Menggunakan maklmat di dalam Jadual 2, jawap soalan-soalan berikut.

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 dalam Jadual 2?

(4 markah)

SOALAN 5 (20 MARKAH)

Diberi sebuah system kripto NTRU berparameter N=11, p=3 dan q=32. Kekunci awam Bob adalah

$$h(x) = 16x^{10} + 19x^9 + 12x^8 + 19x^7 + 15x^6 + 24x^5 + 12x^4 + 20x^3 + 22x^2 + 25x + 8$$

dan Kekunci Sulit Bob adalah

$$[f(x),\ f_p^{-1}(x)].$$

Ambil i = ID mod 16. Alice ingin menghantar mesej kepada Bob menggunakan kunci awam Bob $h(x)$. Dia mula-mula meletakkan mesejnya dalam bentuk polynomial,

$$m(x) = x^7 - x^6 - x^5 + i(x).$$

Seterusnya bagi mengaburi mesej, dia secara rawak memilih polinomial kecil yang lain,

$$r(x) = x^{10} + x^8 - x^6 + x^3 + x + 1.$$

a) Dalam process enkripsi, Alice perlu mengira *ciphertext* dengan cara

$$e(x) = \mathrm{r}(x) * h(x) + m(x) \text{ (modulo q)}.$$

Dimana polinomial e adalah mesej yang telah di enkripsi untuk Alice hantarkan kepada Bob.

i) Diberi $\mathrm{r}(x)*h(x)$

=[1 0 ,1 0,−1 0 0 1 0 1 1]*[16 19 12 19 15 24 12 20 22 25 8]

=[16 19 28 38 11 24 15 41 38 49 72 51 41 21 51 58 57 50 47 33 8]

Kira modulo q bagi mencapai $\mathrm{r}(x)*h(x)$ (mod q)

(2 markah)

ii) Ambil modulo $x^N - 1$ bagi mencapai $\mathrm{r}(x)*h(x)$ (mod $x^N - 1$)

(4 markah)

iii) Campurkan mesej dengan mengira $\mathrm{r}(x)*h(x) + m(x)$

(4 markah)

iv) Ambil modulo q bagi mencapai *ciphertext* $e(x)$

(2 markah)

b) Terangkan **EMPAT (4)** tatacara bagi proses dekripsi didalam system NTRU keatas *ciphertext e*.

(8 markah)

- SOALAN TAMAT –

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 an fill them in Table 1.

(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.

(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 (20 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)

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

i. Given the master key K =199 as a_0, the coefficients a_1= 73 and a_2 = 79, generate 3 shadow keys $\{y_2, y_3, y_4\}$ at $\{x_2, x_3, x_4\} = \{105, 107, 109\}$ via a polynomial $A(x) = a_0 + a_1 \cdot x + a_2 \cdot x^2 + \ldots + a_{m-1} \cdot x^{m-1} \bmod 257$.

(6 marks)

ii. Given $2^{-1} \equiv 129 \pmod{257}$ and $4^{-1} \equiv 193 \pmod{257}$, generate the divided difference table for Newton interpolation from three shadow keys: $(x_0, y_0) = (101, 46)$, $(x_1, y_1) = (103, 42)$ and $(x_2, y_2) = (105, 156)$.

(4 marks)

iii. 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 $x = 0$.

(2 marks)

QUESTION 3 (20 MARKS)

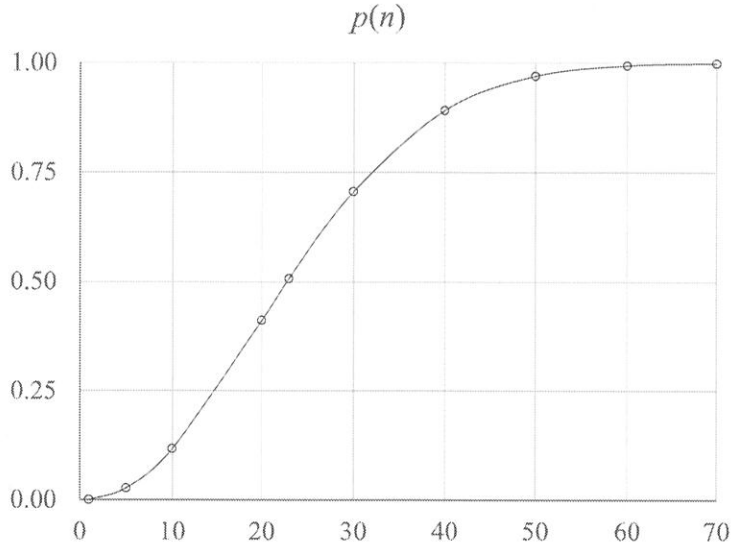


Figure 1: Probabilities of at least two people sharing a birthday

a) Refer to probabilities of at least two out of n people sharing a birthday in Figure 1, give **TWO (2)** description on Birthday Paradox among 15 to 30 people.

(4 marks)

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

(4 marks)

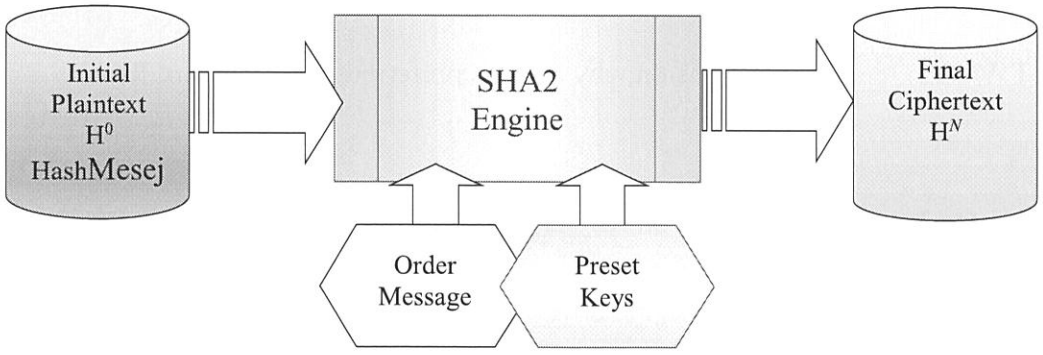


Figure 2: A hash function as a block cipher.

d) 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.

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

Algorithm	Block Size(in bits)	Running Encrypt Time	Running Decrypt Time
AES	128	$O(k_e \cdot n)$	$O(k_d \cdot n)$
RSA	2048, 4096	$O(k_e \cdot n^3)$	$O(k_d \cdot n^3)$
ECC	256	$O(k_e \cdot n^3)$	$O(k_d \cdot n^3)$
NTRU	347, 503	$O(k_e \cdot n^2)$	$O(k_d \cdot n^2)$

Using Table 2 as your reference, answer the following questions.

a) 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 the modern cryptosystems rely upon.

(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 stated in Table 2?

(4 marks)

QUESTION 5 (20 MARKS)

Given the NTRU parameters N=11, p=3 and q=32. Bob's Public Key is

$$h(x) = 16x^{10} + 19x^9 + 12x^8 + 19x^7 + 15x^6 + 24x^5 + 12x^4 + 20x^3 + 22x^2 + 25x + 8$$

and Bob's private key is

$$[f(x), f_p^{-1}(x)].$$

Take i = ID mod 16. Alice wants to send a message to Bob using Bob's public key $h(x)$. She first puts her message in the form of a polynomial,

$$m(x) = x^7 - x^6 - x^5 + i(x).$$

Next, she randomly chooses another small polynomial,

$$r(x) = x^{10} + x^8 - x^6 + x^3 + x + 1.$$

This blinding mode will obscure the message.

a) In an encryption process, Alice needs to compute a ciphertext,

$$e(x) = \mathrm{r}(x) * h(x) + m(x) \text{ (modulo q)}.$$

The polynomial e is the encrypted message which Alice sends to Bob.

i) Given $\mathrm{r}(x)*h(x)$

=[1 0 ,1 0,−1 0 0 1 0 1 1]*[16 19 12 19 15 24 12 20 22 25 8]

=[16 19 28 38 11 24 15 41 38 49 72 51 41 21 51 58 57 50 47 33 8]

Take modulo q to get $\mathrm{r}(x)*h(x)$ (mod q)

(2 marks)

ii) Take modulo $x^N - 1$ to get $\mathrm{r}(x)*h(x)$ (mod $x^N - 1$)

(4 marks)

iii) Add the message to compute $\mathrm{r}(x)*h(x) + m(x)$

(4 marks)

iv) Take modulo q to get $e(x)$

(2 marks)

b) Describe **FOUR (4)** steps on the decryption process in NTRU on the cipher text e.

(8 marks)

-END OF QUESTIONS-