UNIVERSITI TEKNIKAL MALAYSIA MELAKA

UNIVERSITI TEKNIKAL MALAYSIA MELAKA
PEPERIKSAAN AKHIR SEMESTER I
FINAL EXAMINATION SEMESTER I
SESI 2019/2020
SESSION 2019/2020

FAKULTI TEKNOLOGI MAKLUMAT DAN KOMUNIKASI

KOD MATAPELAJARAN ***SUBJECT CODE***	:	**BITS 3463**
MATAPELAJARAN ***SUBJECT***	:	**KRIPTOGRAFI DAN TEORI INFORMASI** ***CRYPTOGRAPHY AND INFORMATION THEORY***
PENYELARAS ***COORDINATOR***	:	**NUR AZMAN BIN ABU**
KURSUS ***COURSE***	:	**BITZ**
MASA ***TIME***	:	**2.15 PTG** ***2.15 PM***
TEMPOH ***DURATION***	:	**2 HOURS**
TARIKH ***DATE***	:	**2 JANUARI 2020** ***2 JANUARY 2020***
TEMPAT ***VENUE***	:	**B. KULIAH 5 PBPI** ***PBPI LECTURE ROOM 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 HINGGA 5 DAN DALAM BAHASA MELAYU DARI MUKASURAT 6 HINGGA 9.**
   EXAM QUESTIONS IN ENGLISH ARE FROM PAGE 2 TO 5 DAN IN MALAY ARE FROM PAGE 6 TO 9.
3. **SILA JAWAB SEMUA SOALAN.**
   ANSWER ALL QUESTIONS
4. **TULISKAN JAWAPAN ANDA DIDALAM BUKU JAWAPAN YANG DIBERIKAN.**
   WRITE YOUR ANWERS IN THE ANSWER BOOKLET PROVIDED.

KERTAS SOALAN INI TERDIRI DARIPADA SEMBILAN(9) MUKA SURAT SAHAJA TERMASUK MUKA SURAT HADAPAN
THIS QUESTION PAPER CONTAINS NINE(9) PAGES INCLUSIVE OF THIS FRONT PAGE

PERINGATAN
REMINDER:

PELAJAR TIDAK DIBENARKAN SAMA SEKALI MEMBAWA APA-APA BUKU, KERTAS, SURATAN, GAMBAR, NOTA, SEBARANG ALAT YANG DI DALAM ATAU DI ATASNYA TERDAPAT CATATAN BERTULIS, 'PROGRAMMABLE CALCULATOR', TELEFON MUDAH ALIH ATAU SEBARANG ALAT KECUALI YANG DIBENARKAN OLEH PENGAWAS KE DALAM ATAU KELUAR DARI SESUATU DEWAN PEPERIKSAAN ATAU MENERIMA APA-APA BUKU, KERTAS, SURATAN, GAMBAR, NOTA, SEBARANG ALAT YANG DI DALAM ATAU DI ATASNYA TERDAPAT CATATAN BERTULIS, 'PROGRAMMABLE CALCULATOR', TELEFON MUDAH ALIH ATAU SEBARANG ALAT DARI MANA-MANA ORANG LAIN SEMASA DI DALAM DEWAN PEPERIKSAAN KECUALI SESEORANG PELAJAR SEMASA IA BERADA DI DALAM DEWAN PEPERIKSAAN ITU MENERIMA DARIPADA PENGAWAS APA-APA BUKU, KERTAS, DOKUMEN/GAMBAR ATAU LAIN-LAIN ALAT YANG DIBENARKAN OLEH NAIB CANSELOR ATAS SYOR PEMERIKSA ATAU FAKULTI.

STUDENTS ARE NOT ALLOWED TO BRING IN ANY BOOKS, PAPERS, DOCUMENTS, PHOTOGRAPHS, NOTES, ANY TOOLS WHICH THERE ARE WRITTEN RECORDS, MOBILE PHONES, OR ANY OTHER DEVICES WITHOUT THE PRIOR PERMISSION OF THE INVIGILATORS INTO OR OUT OF THE EXAMINATION HALL, OR RECEIVE ANY PAPERS, BOOKS, DOCUMENTS, PHOTOGRAPHS, NOTES, ANY DEVICES IN OR ON WHICH THERE ARE WRITTEN RECORDS, 'PROGRAMMABLE CALCULATORS', OR TOOLS FROM OTHER PERSON(S) PRESENT IN THE EXAMINATION HALL; EXCEPT MATERIALS OR DEVICES PROVIDED BY THE INVIGILATORS AND PERMITTED BY THE VICE CHANCELLOR ON THE RECOMMENDATIONS OF THE EXAMINERS OR FACULTIES.

INSTRUCTION: *Answer ALL Questions*

QUESTION 1 (20 MARKS)

Suppose there are 9 symbols to encode. Given the probability distribution of the symbols as follows.

Symbol x	A	B	C	D	F	G	H	I	J
$P(X=x)$	0.03	0.12	0.19	0.23	0.17	0.13	0.07	0.04	0.02

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

(2 marks)

b) Sort the symbols and their pdfs in descending order according to 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-J 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)

Given the NTRU parameters N=11, p = 3 and q = 32. Bob's Public Key: $[h(x), N, p, q]$ and Bob's private Key: $[f(x), f_p^{-1}(x)]$.

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 $m(x) = x^7 - x^6 - x^5 + x^3 + x^2 + x + 1$. 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. Alice would like to compute ciphertext $e(x) = r(x) * h(x) + m(x)$ modulo q. The polynomial e is the encrypted message which Alice sends to Bob.

a) Compute $r(x)*h(x)$.

(8 marks)

b) Take modulo q to get $r(x)*h(x)$ (mod q)

(4 marks)

c) Take modulo $x^N - 1$ to get $r(x)*h(x)$ (mod $x^N - 1$)

(4 marks)

d) Add the message to compute $r(x)*h(x) + m(x)$

(4 marks)

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

(2 marks)

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

(8 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 1 below.

Table 1: Key sizes and the time complexities of 4 major cryptosystems

Algorithm	Key Size	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, an encryption run practically faster than decryption process. How this differences in speed is practically achieved on AES and RSA cryptosystems?

(2 marks)

b) Give an order on which cryptosystem is faster than the other. Give **THREE (3)** reasons on your answers.

(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 the effect from Quantum computers on the security of each of the **FOUR (4)** cryptosystems above?

(4 marks)

-END OF QUESTIONS-

ARAHAN: *Jawab **SEMUA** soalan*

SOALAN 1 (20 MARKAH)

Katakan terdapat 9 simbol untuk dikodkan. Taburan kebarangkalian simbol adalah disertakan seperti berikut.

Symbol x	A	B	C	D	F	G	H	I	J
$P(X=x)$	0.03	0.12	0.19	0.23	0.17	0.13	0.07	0.04	0.02

a) Lakarkan graf taburan kebarangkalian (pdf).

(2 markah)

b) Susunkan simbol-simbol tersebut dan pdf mereka dalam urutan menurun mengikut taburan kebarangkalian.

(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 system 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 Polynomial 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 polynomial $A(x) = a_0 + a_1 \cdot x + a_2 \cdot x^2 + \ldots + a_{m-1} \cdot x^{m-1}$ 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)

Diberi parameter NTRU N=11, p = 3 and q = 32. Kekunci awam Baba adalah $[h(x), N, p, q]$ dan kekunci peribadi Baba adalah $[f(x), f_p^{-1}(x)]$.

Ain ingin menghantar mesej kepada Baba menggunakan kunci awam Baba $h(x)$. Beliau mula-mula meletakkan mesejnya dalam bentuk polinomial $m(x) = x^7 - x^6 - x^5 + x^3 + x^2 + x + 1$. Kemudian dia secara rawak memilih polinomial kecil lain $r(x) = x^{10} + x^8 - x^6 + x^3 + x + 1$. Ini adalah nilai yang mengaburkan mesej. Ain ingin mengira teks cipher $e(x) = r(x) * h(x) + m(x)$ modula q. Polinomial e ialah mesej yang dienkripsi untuk dihantar oleh Ain kepada Baba.

a) Kira $r(x)*h(x)$.

(8 markah)

b) Guna modula q bagi mendapatkan $r(x)*h(x)$ (mod q).

(4 markah)

c) Sekali lagi gunakan modula $x^N - 1$ bagi mendapatkan $r(x)*h(x)$ (mod $x^N - 1$).

(4 markah)

d) Tambah mesej bagi mendapatkan $r(x)*h(x) + m(x)$.

(4 markah)

e) Guna modula q bagi mendapatkan teks cipher $e(x)$.

(2 markah)

f) Jelaskan **EMPAT(4)** langkah proses penyahsulitan di NTRU pada teks cipher e bagi mendapatkan mesej asal.

(8 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 1.

Jadual 1: Saiz kekunci dan pengolahan masa

Algorithma	Saiz Kekunci	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 praktikal dan umumnya, proses penyulitan enkripsi berjalan lebih pantas daripada proses penyahsulitan. Bagaimana perbezaan kelajuan ini dapat dicapai dalam sistem kriptografi AES dan RSA? **(2 markah)**

b) Berikan turutan kepantasan keatas keempat-empat sistem kriptografi diatas. Berikan **TIGA(3)** penjelasan ringkas sebab musabab berkaitan jawapan yang anda berikan. **(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? **(4 markah)**

- SOALAN TAMAT -