Midterm

● Graded

Student

Joshua Mayhugh

Total Points

12.5 / 14 pts

Question 1

modes encryption

2 / 2 pts

✔ **– 0 pts** correct
a. which blocks can do parallel encryption (0.25 for mentioning each correct response)
b. inputs for each block (0.5 for each)
ECB-yes; CTR-yes; CBC-no
ECB: Plaintext block n and the key;
CTR: Plaintext block n, IV, block number, and the key
CBC: Plaintext block n, ciphertext block n-1 (or IV if n=1), and the key
If you have not mentioned anything about CBC, no points has been deducted.

– 0.05 pts attempted, incomplete response for what inputs needed for CTR.
Not mentioning any counter/ block number in CTR

– 0.25 pts Not mentioning all modes that be exeuted in parallel

– 0.25 pts attempted, incomplete response for what inputs needed for ecb

– 0.5 pts Not attempted any part

Question 2

modes decryption

Resolved **1.5** / 2 pts

+ 0.25 pts incomplete response for what blocks can use multiple processors
ECB-yes; CTR-yes; CBC-yes

+ 0.5 pts correct response for what blocks can use multiple processors
ECB-yes; CTR-yes; CBC-yes

✔ **+ 0.5 pts** correct response for what i/p need for cbc

CBC: Ciphertext block n, ciphertext block n-1 (or IV if n=1) and the key

✔ **+ 0.5 pts** correct response for what i/p need for ctr
CTR: Ciphertext block n, IV, block number, and the key

✔ **+ 0.5 pts** correct response for what i/p need for ecb
ECB: Ciphertext block n and the key

+ 0.45 pts attempted, incomplete response for what i/p need for ctr
missing item : block number

+ 0.45 pts attempted, incomplete response for what i/p need for CBC
missing item : previous block

no response on which of the modes can use multiple processors in parallel.

Regrade Request **Submitted on: Nov 01**

Question 2, it says i did not answer this correctly but i included all three correct blocks, ECB, CTR, CBC and explanations.

I do not see your response to the first part "in which of the modes can multiple processors be used in parallel". Hence (-0.5)
can you start a email thread if you need further discussion ? responding once in gradescope closes the request.

Reviewed on: Nov 01

Question 3

quantum 1

1 / 1 pt

✔ **– 0 pts** Correct
any two complex number with abs val of $1/sqrt(2)$
(a|00> + b|11> for make-up exam)

Question 4

quantum 2

1 / 1 pt

✔ **– 0 pts** Correct

Initialize each of the n qubits to zero (by reading them and complementing those that are read as one); then performing a **Hadamard gate** on each one.

– 0.5 pts reasonable attempt, no mention of hadamard

Question 5

quantum 3

1 / 2 pts

- ✔ **– 0 pts** Part 1Correct 2^n
- ✔ **– 0 pts** part 2 correct
  2^n
  2^ n values (all possible values for the first n and the ancilla bit set to 1
  if the first n are zero and 0 otherwise)
- **– 0 pts** Part 3 correct
  2^n -1
- ✔ **– 0 pts** part 4 correct
  1
  (full credit has been awarded for writing 0 superposed values, but the number of possible states is 1.)
- **– 0.5 pts** part 1 incorrect
- **– 0.5 pts** part 2 incorrct
- ✔ **– 0.5 pts** part 3 incorrect
- **– 0.5 pts** part 4 incorrect
- **+ 0.5 pts** attempted all part, but all incorrect
- 💬 **– 0.5 pts** part 1 (-0.25)
  part 2(-0.25)
  reasonable attempt, no of values not answered

Question 6

hash preimage

1 / 1 pt

- ✔ **– 0 pts** Correct

Question 7

hash collision

1 / 1 pt

- ✔ **– 0 pts** Correct

Question 8

RSA

3 / 3 pts

- ✔ **– 0 pts** A Correct
- ✔ **– 0 pts** B correct
- ✔ **– 0 pts** c correct

Question 9

multiplies

1 / 1 pt

- ✔ **– 0 pts** Correct
  correct answer is 17

Midterm October 11, 2024

Name: Joshua Mayhugh UIN 431004527

Total questions : 9 | Duration : 1 hr

1. In which of the encryption modes EBC, CTR, CBC can multiple processors be used to encrypt blocks in parallel? For each of those modes, what inputs are necessary to encrypt block n?

- ECB can be encrypted in parrallel , you need message block n and secret key K
- CTR for block n of the one time pad CTR, needs IV + n-1 encrypted using key K and the message block n

2. In which of the encryption modes EBC, CTR, CBC can multiple processors be used to decrypt blocks in parallel? For each of those modes, what inputs are required to decrypt ciphertext block n?

- ECB needs cipher text Cn and the secret key to decrypt
- CTR needs cipher block n as well as well as IV + n-1 (encrypted with K)
- CBC needs secret key and cipher text n-1 to decrypt Cipher n since C n-1 is ar computed it is okay

3. If a qubit is in a state where it's equally likely to be read as 0 or 1, what are two possible values for the coefficient of |1> in that state?

$\beta = \frac{1}{\sqrt{2}}, \frac{-1}{\sqrt{2}}$ where β is coefficient of 1

4. How do you initialize n qubits to be in an equal superposition of all 2^n possible classical values? perform hadamard gate on all n qubits

5. Suppose you have n+1 qubits. Let's call the $n+1^{st}$ qubit the "ancilla". Initialize the first n qubits to an equal superposition of all 2^n possible classical states and initialize the ancilla to zero.
For each of the following questions, explain your answer briefly.

a. How many values are superposed at this point on the n+1 qubits?
b. Now apply a quantum circuit that takes the first n qubits as input, and complements the ancilla if the first n bits are all zero. Otherwise, the circuit leaves the ancilla alone. How many values are superposed at this point on the n+1 qubits?
c. Now read the ancilla. Suppose you read 0. How many values are superposed at this point on the n+1 qubits?
d. Now assume that instead of reading a 0, you read a 1. How many values are superposed at this point on the n+1 qubits?

a. the first n qubits are in a superposed state because n+1st is 0

b. the first n qubits are still superimposed, no values have been revealed

c. since the ancilla is still 0, the first n bits cannot be all zero so one must be a value of 1 thus n-1 qubits are remaining superimposed

d. Now since all qubits are zero in the first n, there are no superimposed qubits

6. What is the work factor to find a preimage of a 512-bit hash function?

2^{512}

7. What is the work factor to find two messages that have the same 512-bit hash?

$2^{512/2} = 2^{256}$

8. Suppose Alice wants to create her own RSA key pair.
   a. How does she choose a modulus n?
   b. Let's say she uses 2^16+1 for her public exponent e. How does she calculate d?
   c. Why can't people who see her public key (e,n) calculate d?

a. She chooses two large primes p and q and $n = pq$

b. she calc $\phi(n) = (p-1)(q-1)$ and chooses d s.t $de \equiv 1 \mod(\phi(n))$

c. it is difficult for them to solve for factors of large number n in order to find e's exponentiative inverse mod $\phi(n)$

$X^{2^{16}+1}$

9. How many multiplies does it take to raise some number x to the power (2^16)+1, mod n? For each multiply, specify what values will be multiplied together.

17 multiplications

1. $x \cdot x = x^2$
2. $x^2 \cdot x^2 = x^4 = x^{2^2}$
3. $x^4 \cdot x^4 = x^8 = x^{2^3}$
4. $x^8 \cdot x^8 = x^{16} = x^{2^4}$
5. $x^{16} \cdot x^{16} = x^{32} = x^{2^5}$
6. $x^{2^5} \cdot x^{2^5} = x^{2^6}$
7. $x^{2^6} \cdot x^{2^6} = x^{2^7}$ — missed one: $x^{2^7} \cdot x^{2^7} = x^{2^8}$
8. $x^{2^8} \cdot x^{2^8} = x^{2^9}$
9. $x^{2^9} \cdot x^{2^9} = x^{2^{10}}$
10. $x^{2^{10}} \cdot x^{2^{10}} = x^{2^{11}}$
11. $x^{2^{11}} \cdot x^{2^{11}} = x^{2^{12}}$
12. $x^{2^{12}} \cdot x^{2^{12}} = x^{2^{13}}$
13. $x^{2^{13}} \cdot x^{2^{13}} = x^{2^{14}}$ +1
14. $x^{2^{14}} \cdot x^{2^{14}} = x^{2^{15}}$ +1
15. $x^{2^{15}} \cdot x^{2^{15}} = x^{2^{16}}$ +1
16. $x^{2^{16}} \cdot x = x^{2^{16}+1}$ +1