Name:__________________

StudentNo:________________

The University of Newcastle
School of Electrical Engineering and Computer Science

COMP3260/6360 Data Security
Sample Midterm Test 1 Solutions

Test duration: 55 min
100 marks

In order to score marks, you must show all the workings!

STUDENT NUMBER:_______________________

STUDENT NAME:__________________________

PROGRAM ENROLLED:____________________

Question 1	***Question 2***	***Question 3***	***Question 4***	***Question 5***	***TOTAL***

$\lg 26! \approx 88.4$ $\lg 3 \approx 1.58$

$\lg 25! \approx 83.7$ $\lg 26 \approx 4.7$

Name:__________________

StudentNo:________________

1. ***(20 marks)*** Suppose that there are 5 possible messages, A, B, C, D and E, with probabilities p(A) = p(B) = p(C) = p(D) = 1/8 and p(E)=1/2.

- ***a.*** What is the expected number of bits needed to encode these messages in optimal encoding?
- ***b.*** Give an example of an optimal encoding.
- ***c.*** Calculate the average number of bits needed to encode the message using your encoding.

Solution:

a. The expected number of bits needed to encode these messages in optimal encoding is given by the entropy:

$$H(X) = p(A)lg\frac{1}{p(A)} + p(B)lg\frac{1}{p(B)} + p(C)lg\frac{1}{p(C)} + p(D)lg\frac{1}{p(D)} + p(E)lg\frac{1}{p(E)}$$

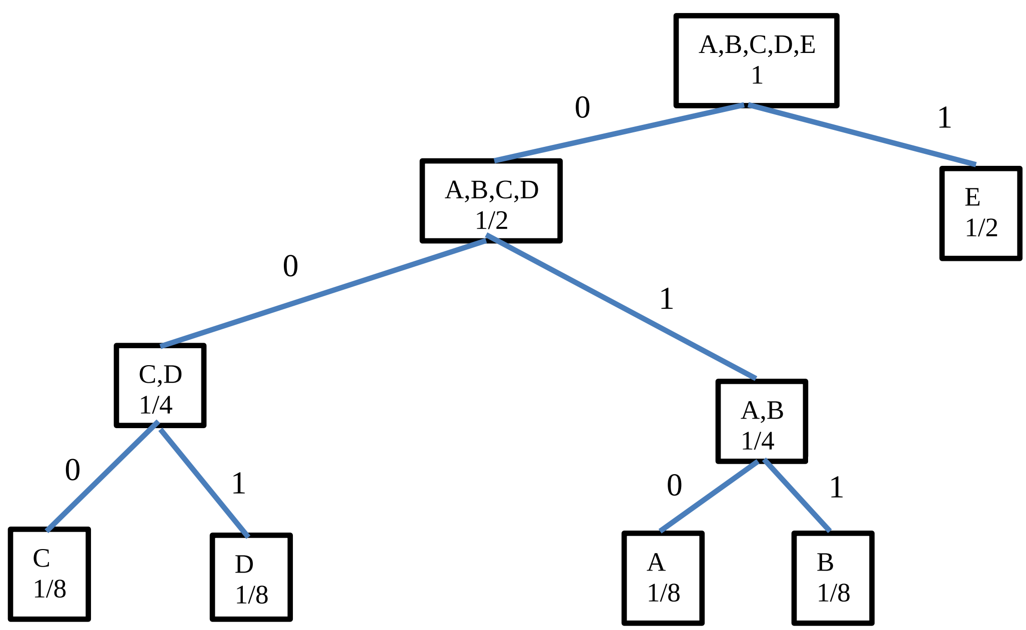
$$= 4 \times \frac{1}{8}lg\frac{1}{\frac{1}{8}} + \frac{1}{2}lg\frac{1}{\frac{1}{2}}$$

$$= \frac{1}{2}lg\,8 + \frac{1}{2}lg\,2$$

$$= \frac{3}{2} + \frac{1}{2}$$

$$= 2$$

b.



Then the optimal encoding is as follows:

lg 26! ≈ 88.4

lg 25! ≈ 83.7

lg 3 ≈ 1.58

lg 26 ≈ 4.7

A – 010
B – 011
C – 000
D – 001
E – 1

c. The average number of bits N_{av} for this encoding is:

$$\boldsymbol{N_{av} = 4 \times \frac{1}{8} \times 3 + \frac{1}{2} \times 1 = \frac{3}{2} + \frac{1}{2} = 2}$$

As N_{av} = H(X), we have achieved the optimal encoding.

2. ***(20 marks)*** True or false?

a. Every integer in the range [1,971] has a multiplicative inverse modulo 972.

Solution: FALSE – 972 is not a prime number, it is, for example, divisible by 2, so even integers in the range [1,971] do not have a multiplicative inverse modulo 972.

b. Every integer in the range [0,18] has a multiplicative inverse modulo 19.

Solution: FALSE – 0 does not have a multiplicative inverse.

c. Every integer in the range [1,34] except 5 and 7 has a multiplicative inverse modulo 35.

Solution: FALSE – multiples f 5 and 7 also do not have a multiplicative inverse modulo 35, for example, 15.

d. Equation 3x mod 15 = 12 has no solutions.

Solution: FALSE – since gcd(3,15)=3 and 12 is a multiple of 3, this equation has 3 solutions.

e. Computing in $GF(2^n)$ is less efficient than computing in $GF(p)$, as it is easier to work with integers than polynomials.

Solution: FALSE – computing with polynomials is more efficient as adition and subtraction are equivalent to bitwise exclusive OR.

f. There is an <u>efficient</u> algorithm for factoring large numbers, as to find factors of n, we only need to check if it is divisible by all prime numbers less than square root of n, thus the algorithm is sub-linear.

Solution: FALSE – this algorithm is correct but it is not efficient as it is sublinear in the number itself; the efficient algorithms for number inputs should be logarithmic.

g. There is an <u>efficient</u> algorithm for finding a greatest common divisor of any two integers.

Solution: TRUE – Euclid's algorithm.

h. There is no <u>efficient</u> algorithm for fast exponentiation.

Solution: FALSE – Fast Exponentiation algorithm is efficient.

i. 100 and 111are multiplicative inverses in $GF(2^3)$ with irreducible polynomial $p(x) = x^3 + x^2 + 1$.

Solution: FALSE – we multiply the polynomials and we get 111, not 001:

```
    100
x   111
______
    100
   100
  100
______
  11100
```

We divide 11100 by the irreducible polynomial 1101:

```
1101 ) 11100
       1101
       ______
       00111
```

lg 26! ≈ 88.4 lg 3 ≈ 1.58

lg 25! ≈ 83.7 lg 26 ≈ 4.7

j. 101 and 110 are additive inverses in GF(2^3) with irreducible polynomial p(x) = $x^3 + x^2 + 1$.

Solution: FALSE – we add the polynomials and we get 011, not 001:

$$\begin{array}{r} 101 \\ +\ 110 \\ \hline 011 \end{array}$$

lg 26! ≈ 88.4
lg 25! ≈ 83.7

lg 3 ≈ 1.58
lg 26 ≈ 4.7

Name:__________________

StudentNo:________________

3. Explain the following terms.

(a) ***(8 marks)*** Euler's Totient Function (also provide formula)
(b) ***(6 marks)*** Steganography (also give an example)
(c) ***(6 marks)*** Absolute Rate of Language

Solution:

(a) For every integer n, the Euler's totient function $\phi(n)$ is the number of positive integers less than n which are relatively prime to n. If the prime factorization of the number n is known, that is,

$$n = p_1^{e_1} p_2^{e_2} \dots p_t^{e_t}$$

Euler's totient function can be calculated as

$$\phi(n) = \prod_{i=1}^{t} p_i^{e_i - 1}(p_i - 1).$$

(b) Steganography is a study of hiding messages within other messages or some other medium. Thus, the purpose of steganography is to hide the existence of the message and not just its content as cryptography does.

An example of steganography is hiding a message in LSB (Least Significant Bit) in graphic image.

(c) The absolute rate of language, denoted R, is the maximum number of bits of information that could be encoded in each character assuming all possible sequences of characters are equally likely. The absolute rate R of the language is R = $\log_2$ L, where L is the number of characters in the language.

4. ***(20 mark)*** Let $a=100$. If $GF(2^3)$ with irreducible polynomial $p(x)= x^3 + x^2 + 1$, use Euler's theorem to find a^{-1} and then verify that $a \times a^{-1} \bmod p(x)=1$.

Solution:

$$a^{-1} = 011$$

In this context, the form of Euler's theorem to use is

$$a^{-1} = a^{\phi(p(x))-1} \bmod p(x).$$

We first need to know $\phi(p(x))$. Recall that Euler's totient function $\phi(p(x))$ counts the number of positive elements relatively prime to $p(x)$. Since $p(x)$ is irreducible, this is equivalent to the number of elements in $GF(2^3)$, minus the polynomial with only zero coefficients. The elements of $GF(2^3)$ (written as bit fields) are {000, 001, 010, 011, 100, 101, 110, 111}, so there are 7 elements relatively prime to $p(x)$. Equivalently, you could use the formula instead of enumerating the elements:

$$\phi(p(x)) = 2^n - 1$$

lg 26! ≈ 88.4	lg 3 ≈ 1.58
lg 25! ≈ 83.7	lg 26 ≈ 4.7

$$= 2^3 - 1$$
$$= 7.$$

We can now calculate the multiplicative inverse:

$$a^{-1} = a^{\phi(p(x))-1} \bmod p(x)$$
$$= a^{7-1} \bmod p(x)$$
$$= a^6 \bmod p(x)$$

To reduce the number of calculations required, we'll calculate $a^6 = a^2a^4$. First, we calculate $a^2 = 100 \times 100$ in polynomial arithmetic:

```
     100
x    100
     000
    000
   100
   10000
```

Now, we divide 10000 by $p(x) = 1101$

```
            11
1101 (   10000
         1101
         01010
          1101
          0111
```

so $a^2 = 111$. Next, we calculate $a^4 = a^2 \times a^2 = 111 \times 111$ in polynomial arithmetic:

```
     111
x    111
     111
    111
   111
   10101
```

Now, we divide 10101 by $p(x) = 1101$ to find 1101 mod $p(x)$:

```
            11
1101 (   10101
         1101
         01111
          1101
          0010
```

so $a^4 = 010$. Next, we calculate $a^6 = a^2 \times a^4 = 111 \times 010$ in polynomial arithmetic:

```
     111
x    010
     000
    111
   000
   01110
```

Now, we divide 1110 by $p(x) = 1101$ to find 1110 mod $p(x)$:

```
            1
1101 (  1110
        1101
        0011
```

So $a^6 = 011$, and $a^{-1} = a^6 \bmod p(x) = 011$.

The final requirement of the question is to verify $a \times a^{-1} \bmod p(x) = 1$. We start by calculating $a \times a^{-1} = 100 \times 011$:

```
     100
x     11
     100
    100
   01100
```

Now, we divide 1100 by $p(x) = 1101$ to find 1100 mod $p(x)$:

```
            1
1101 (  1100
        1101
        0001
```

So $a \times a^{-1} \bmod p(x) = 1$ as requested.

Name:__________________

StudentNo:________________

5. ***(20 marks)*** Find a solution to the equation *7x mod 40 = 1* in the following 3 ways. Note that you must show all the workings and/or trace the algorithm in order to score marks.

a) Euler's Theorem (by fast exponentiation): $a^{\Phi(n)}$ *mod n = 1*, where *gcd(a,n)=1*

Solution:

$$x = 23$$

First, we can re-arrange Euler's Theorem to be in terms of the multiplicative inverse:

$$a^{\phi(n)} \bmod n = 1$$
$$a^{\phi(n)-1} \bmod n = a^{-1}$$
$$a^{-1} = a^{\phi(n)-1} \bmod n.$$

In this case $a = 7, x = a^{-1}, n = 40$. We need to find the value of Euler's Totient function. Finding the prime factors yields $40 = 2^3 \times 5$, so we can find the value of the totient function using the formula:

$$\phi(n) = \prod_{i=1}^{t} {p_i}^{e_i - 1}(p_i - 1)$$
$$\phi(40) = [2^{3-1}(2-1)] \times [5^{1-1}(5-1)]$$
$$\phi(40) = 16.$$

Now we can use the fast exponentiation algorithm to find x:

$$\begin{aligned} x &= 7^{\phi(40)-1} \bmod 40 \\ &= 7^{15} \bmod 40 \\ &= 7 \times 7^{14} \bmod 40 \\ &= 7 \times (7^2)^7 \bmod 40 \\ &= 7 \times (49)^7 \bmod 40 \\ &= 7 \times (9)^7 \bmod 40 \\ &= 7 \times 9 \times (9)^6 \bmod 40 \\ &= 63 \times (9^2)^3 \bmod 40 \\ &= 23 \times (81)^3 \bmod 40 \\ &= 23 \times (1)^3 \bmod 40 \\ &= 23 \end{aligned}$$

lg 26! ≈ 88.4	lg 3 ≈ 1.58
lg 25! ≈ 83.7	lg 26 ≈ 4.7

Name:__________________

StudentNo:________________

b) Chinese Remainder Theorem: Let $d_1, \dots, d_t$ be pairwise relatively prime, and let $n = d_1 \times d_2 \times \dots \times d_t$. Then the system of equations $(x \bmod d_i) = x_i \ (i = 1, \dots, t)$ has a common solution x in the range $[0, n-1]$. The common solution is

$$x = \sum_{i=1}^{t} \frac{n}{d_i} y_i x_i \ mod\ n$$

where y_i is a solution of $(n/d_i)\, y_i \bmod d_i = 1,\ i = 1, \dots, t.$

Solution:

$$x = 23$$

First we need to find $d_1, \dots, d_t$. Now $40 = 5 \times 2^3$, so we have:

$$d_1 = 5$$
$$d_2 = 8$$

Next we can find $x_1, \dots, x_t$.

$$7x_1 \text{ mod } 5 = 1$$
$$2x_1 \text{ mod } 5 = 1 \Rightarrow x_1 = 3$$

$$7x_2 \text{ mod } 8 = 1 \Rightarrow x_2 = 7$$

And we can find $y_1, \dots, y_t$.

$$\frac{40}{5} y_1 \text{ mod } 5 = 1$$
$$8y_1 \text{ mod } 5 = 1$$
$$3y_1 \text{ mod } 5 = 1 \Rightarrow y_1 = 2$$

$$\frac{40}{8} y_2 \text{ mod } 8 = 1$$
$$5y_2 \text{ mod } 8 = 1 \Rightarrow y_2 = 5$$

Now we can find the common solution to the set of equations to get the multiplicative inverse by using the formula:

$$\begin{aligned} x &= \sum_{i=1}^{t} \frac{n}{d_i} y_i x_i \text{ mod } n \\ &= \left(\frac{40}{5} \times 2 \times 3 + \frac{40}{8} \times 5 \times 7\right) \text{ mod } 40 \\ &= (48 + 175) \text{ mod } 40 \\ &= (8 + 15) \text{ mod } 40 \\ &= 23 \end{aligned}$$

lg 26! ≈ 88.4	lg 3 ≈ 1.58
lg 25! ≈ 83.7	lg 26 ≈ 4.7

Name:____________________

StudentNo:__________________

c) Extended Euclid's algorithm:

```
Algorithm inv(a,n)
    begin
        g0 := n; g1 := a; u0 = 1;  v0 := 0;  u1 := 0;  v1 := 1; i := 1;
        while gi ≠ 0 do "gi = ui × n + vi × a"
            begin
                y := gi-1 div gi ;   gi+1 := gi-1 - y × gi ;
                ui+1 := ui-1 - y × ui ;  vi+1 := vi-1 - y × vi ;
                 i := i + 1
            end
         x := vi -1;
         if x ≥ 0 then inv := x else inv := x+n
    end
```

Solution:

i	y	g	u	v
0	-	40	1	0
1	-	7	0	1
2	5	5	1	-5
3	1	2	-1	6
4	2	1	3	-17
5	2	0	-	-

Now $x = v_4 = -17$, and inv $= x + n = -17 + 40 = 23$. Thus the multiplicative inverse of 7 modulo 40 is 23.

lg 26! ≈ 88.4

lg 25! ≈ 83.7

lg 3 ≈ 1.58

lg 26 ≈ 4.7