Name:__________________

StudentNo:________________

The University of Newcastle
School of Electrical Engineering and Computer Science

COMP3260/6360 Data Security
Sample Midterm Test 1

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.

lg 26! $\approx$ 88.4	lg 3 $\approx$ 1.58
lg 25! $\approx$ 83.7	lg 26 $\approx$ 4.7

Name:_________________

StudentNo:_______________

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

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

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

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

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

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.

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

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

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

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

$\lg 26! \approx 88.4$	$\lg 3 \approx 1.58$
$\lg 25! \approx 83.7$	$\lg 26 \approx 4.7$

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

$\lg 26! \approx 88.4$ $\qquad$ $\lg 3 \approx 1.58$
$\lg 25! \approx 83.7$ $\qquad$ $\lg 26 \approx 4.7$

Name:__________________

StudentNo:________________

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

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

Name:_________________

StudentNo:_______________

5. ***(20 marks)*** Find a solution to the equation $7x \bmod 40 = 1$ 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): $a^{\Phi(n)} \bmod n = 1$, where $gcd(a,n)=1$

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

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

Name:_________________

StudentNo:_______________

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

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

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

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
```

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

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

Name:__________________

StudentNo:________________

$\lg 26! \approx 88.4$	$\lg 3 \approx 1.58$
$\lg 25! \approx 83.7$	$\lg 26 \approx 4.7$

Name:__________________

StudentNo:________________

$\lg 26! \approx 88.4$	$\lg 3 \approx 1.58$
$\lg 25! \approx 83.7$	$\lg 26 \approx 4.7$