Name:__________________

StudentNo:________________

The University of Newcastle
School of Electrical Engineering and Computer Science

COMP3260/COMP6360 Data Security
Midterm Test 1

21 March 2018
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*

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

Name:___________________

StudentNo:_________________

1. ***(20 marks)*** Let M be a secret message revealing the recipient of a scholarship. Suppose there were one female applicant, Anne, and three male applicants, Bob, Doug and John. It was initially thought each applicant had the same chance of receiving scholarship; thus p(Anne) = p(Bob) = p(Doug) = p(John) = ¼. It was latter learned that the chances of a scholarship going to a female were ½. Letting S denote the message revealing the sex of the recipient, compute $H_S(M)$.

lg 26! ≈ 88.4

lg 25! ≈ 83.7

lg 3 ≈ 1.58

lg 26 ≈ 4.7

Name:_________________

StudentNo:_______________

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

a. Every integer in the range [1,28] has a multiplicative inverse modulo 29.

b. Every integer in the range [1,21] except 2 and 11 has a multiplicative inverse modulo 22.

c. Equation 3x mod 15 = 1 has more than one solution.

d. Equation 3x mod 15 = 9 has exactly one solution.

e. Computing in $GF(2^n)$ is less efficient than computing in $GF(p)$, as p is a prime number.

f. There is no efficient algorithm for computing greatest common divisors.

g. There exists an <u>efficient</u> algorithm for computing Euler's totient function.

h. There exists an <u>efficient</u> algorithm for computing a common solution of the system of equations of the form $x \bmod d_i = x_i$, $1 \leq i \leq k$, where d_i's are pairwise relatively prime.

i. 100 and 110 are multiplicative inverses in $GF(2^3)$ with irreducible polynomial $p(x) = x^3 + x + 1$.

j. 101 and 111 are additive inverses in $GF(2^3)$ with irreducible polynomial $p(x) = x^3 + x + 1$.

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

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

Name:__________________

StudentNo:________________

3. ***(20 marks)*** Find a solution to the equation $3x \bmod 20 = 1$ in the following *3* ways:

a) (6 marks) Euler's Theorem (by fast exponentiation): $a^{\Phi(n)} \bmod n = 1$, where $gcd(a,n)=1$

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

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

Name:___________________

StudentNo:_________________

b) (7 marks) 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 $(x \bmod d_i) = x_i \quad (i = 1, \ldots, t)$ has a common solution x in the range $[0, n-1]$. The common solution is

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

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

lg 26! ≈ 88.4

lg 25! ≈ 83.7

lg 3 ≈ 1.58

lg 26 ≈ 4.7

Name:___________________

StudentNo:_________________

c) (7 marks) 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
```

$\lg 26! \approx 88.4$

$\lg 25! \approx 83.7$

$\lg 3 \approx 1.58$

$\lg 26 \approx 4.7$

Name:__________________

StudentNo:________________

4. ***(20 marks)*** Let $a=101$. 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 $a \times a^{-1} \bmod p(x)=1$.

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

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

Name:__________________

StudentNo:________________

5. ***(20 marks)*** Give a definition and provide a formula for each of the following terms:

a. ***(6 marks)*** Entropy

b. ***(7 marks)*** Equivocation

c. ***(7 marks)*** Perfect secrecy

$\lg 26! \approx 88.4$

$\lg 25! \approx 83.7$

$\lg 3 \approx 1.58$

$\lg 26 \approx 4.7$