The University of Newcastle
School of Electrical Engineering and Computer Science

COMP3260 Data Security

GAME 3

21st March 2019

Number of Questions: 5
Time allowed: 30min
Total mark: 5

In order to score marks you need to show all the workings and not just the end result.

	Student Number	***Student Name***
Student 1		
Student 2		
Student 3		
Student 4		
Student 5		
Student 6		
Student 7		

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

Chinese Remainder Theorem: Let $d_1, \ldots, d_t$ be pairwise relatively prime, and let $n=d_1d_2 \ldots d_t$. Then the system of equations

$(x \bmod d_i) = x_i \quad (i = 1, \ldots, t)$

has a common solution x in the range $[0,n-1]$.

Euclid's Algorithm gcd(a,n)

```
//n ≥ a
      begin
      g0 := n;
      g1 := a;
      i := 1;
      while gi ≠ 0 do
        begin
          gi+1 := gi-1 mod gi;
          i := i + 1
        end;
      gcd := gi-1
end
```

Extended Euclid's Algorithm inv(a,n)

```
begin

     g0 := n; g1 := a; u0 = 1;  v0 := 0;  u1 := 0;  v1 := 1; i := 1;
     while gi ≠ 0 do "gi = uin + via"
       begin
         y := gi-1 div gi;   gi+1 := gi-1 - y × gi; //y:=10 div 4 = 2;
                                                   //gi+1 := 10 - 2×4=2
         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
```

Fast Exponentiation Algorithm fastexp(a, z, n)

```
begin "return x = a^z mod n"
  a1:= a; z1 :=z;  x := 1;
  while z1 ≠ 0 do
      begin
        while z1 mod 2 = 0 do
           begin "square a1 while z1 is even"
               z1 := z1 div 2; a1 := (a1*a1) mod n;
           end;
         z1 := z1 - 1; x := (x*a1) mod n;
       end;
   fastexp := x;
end
```

1. Use Fast Exponentiation to calculate $2^{57} \bmod 123$?

2. Find the inverse of 11 modulo 296 using CRT.

3. Find the inverse of 11 modulo 296 using Euler’s Theorem and Totient function.

4. Find the inverse of 11 modulo 296 using Extended Euclid’s Algorithm.

5. Consider GF(2^3) with the irreducible polynomial p(x)=1011 (x^3+x+1). Find the multiplicative inverse of *0 1 0*.