The University of Newcastle
School of Electrical Engineering and Computer Science

COMP3260 Data Security

GAME 3 Solutions

Friday, 22nd 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 $n = d_1 d_2 \ldots d_t$. 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 3^{49} mod 170?

Solution: 3^{49} mod 170 = 3

Workings:

x	a	z
1	3	110001 (49)
3	3	110000 (48)
3	9	11000 (24)
3	81	1100 (12)
3	101	110 (6)
3	1	11 (3)
3	1	10 (2)
3	1	1 (1)
3	1	0 (0)

2. Find the inverse of 20 modulo 477 using CRT.

Solution:

We have

$n = 477$

$477 = 3^2 \times 53$

$n = d_1 \times d_2, \; d_1 = 9, d_2 = 53$

$20x_1 \, mod \, 9 = 1 \rightarrow 2x_1 \, mod \, 9 = 1$

$\underline{\boldsymbol{x_1 = 5}}$

$$
\begin{aligned}
20x_2 \, mod \, 53 = 1 \rightarrow \quad x_2 &= 20^{51} \, mod \, 53 \\
&= 20 \times 20^{50} \, mod \, 53 \\
&= 20 \times (20^2)^{25} \, mod \, 53 \\
&= 20 \times 29^{25} \, mod \, 37 \\
&= 20 \times 29 \times 29^{24} \, mod \, 53 \\
&= 50 \times (29^2)^{12} \, mod \, 53 \\
&= 50 \times 46^{12} \, mod \, 53 \\
&= 50 \times (46^2)^6 \, mod \, 53 \\
&= 50 \times 49^6 \, mod \, 53 \\
&= 50 \times (49^2)^3 \, mod \, 53 \\
&= 50 \times 16^3 mod \, 53 \\
&= 50 \times 16 \times 16^2 \, mod \, 53 \\
&= 5 \times 44 \, mod \, 53 \\
&= 8 \, mod \, 53 = 8
\end{aligned}
$$

$\underline{\boldsymbol{x_2 = 8}}$

$x \, mod \, 9 = 6$

$x \, mod \, 53 = 8$

We now need to find y_1 and y_2

$(477/9) \, y_1 \, mod \, 9 = 1$

$(477/53)\ y_2\ mod\ 53\ =\ 1$

$$53y_1\ mod\ 9\ =\ 8y_1\ mod\ 9\ =\ 1\ \rightarrow\ y_1\ =\ 8^5\ mod\ 9\ = 8 \times 8^4\ mod\ 9$$
$$=\ 8 \times 64^2\ mod\ 9 = 8 \times 1^2\ mod\ 9 = 8$$

$$9y_2\ mod\ 53\ =\ 1\ \rightarrow \quad y_2\ =\ 9^{51}\ mod\ 53$$
$$=\ 9\ \times\ 9^{50}\ mod\ 53$$
$$=\ 9\ \times\ (81)^{25}\ mod\ 53\ =\ 9\ \times\ 28^{25}\ mod\ 53$$
$$=\ 9\ \times\ 28\ \times\ 28^{24}\ mod\ 53$$
$$=\ 40\ \times\ (28^2)^{12}\ mod\ 53\ =\ 40\ \times\ 42^{12}\ mod\ 53$$
$$=\ 40\ \times\ (42^2)^6\ mod\ 53\ =\ 40\ \times\ 15^6\ mod\ 53$$
$$= 40\ \times\ (15^2)^3\ mod\ 53\ =\ 40\ \times\ 13^3\ mod\ 53$$
$$=\ 40 \times 13\ \times\ 13^2\ \ mod\ 53$$
$$= 43 \times 10\ mod\ 53$$
$$= 6\ mod\ 53 = 6$$

We get $\underline{\boldsymbol{y_1\ =\ 8}}$ and $\underline{\boldsymbol{y_2\ =\ 6}}$.

We now get the solution

$$x\ =\ (53 \times 5 \times 8\ +\ 9 \times 8 \times 6)\ mod\ 477\ =\ 167$$

Thus the multiplicative inverse of 20 modulo 477 is 167.

Check: 20 × 167 mod 477 = 2280 mod 477 = 1

3. Find the inverse of 20 modulo 477 using Euler’s Theorem and Totient function.

Solution:

We can use Euler's theorem:

$$x\ =\ 20^{\Phi(477)-1}\ mod\ 477$$

$$477\ =\ 3^2\ \times\ 53$$

$$\Phi(477)\ =\ 3^1\ \times (3-1) \times\ (53-1)\ =\ 6\ \times\ 52\ =\ 312$$

$$x\ =\ 20^{\Phi(477)-1}\ mod\ 477 =\ 20^{311}\ mod\ 477$$

Using fast exponentiation, we get

$$x\ =\ 20^{311}\ mod\ 477$$
$$=\ 20 \times 20^{310}\ mod\ 477$$
$$=\ 20 \times (20^2)^{155}\ \ mod\ 477$$
$$=\ 20 \times 400^{155}\ mod\ 477$$
$$=\ 20 \times 400 \times 400^{154}\ mod\ 477$$
$$=\ 368 \times (400^2)^{77}\ mod\ 477\ \ =\ 368 \times 205^{77}\ mod\ 477$$
$$=\ 368 \times 205 \times 205^{76}\ mod\ 477$$
$$= 74 \times (205^2)^{38}\ mod\ 477\ =\ 74 \times 49^{38}\ mod\ 477$$

$$= 74 \times (49^2)^{19} \; mod \; 477 \;=\; 74 \times 16^{19} \; mod \; 477$$
$$= 74 \times 16 \times (16^2)^{\,9} mod \; 477 \;=\; 230 \times 256^9 \; mod \; 477$$
$$= 230 \times 256 \times 256^8 \; mod \; 477$$
$$= 209 \times (256^2)^4 \; mod \; 477 \;=\; 209 \times 187^4 \; mod \; 477$$
$$= 209 \times (187^2)^2 \; mod \; 477 = 209 \times 148^2 \; mod \; 477$$
$$= 209 \times 439 \; mod \; 477$$
$$= 167$$

4. Find the inverse of 20 modulo 477 using Extended Euclid's Algorithm.

Solution:

i	y	u	v	g
0		1	0	477
1		0	1	20
2	23	1	-23	17
3	1	-1	24	3
4	5	6	-143	2
5	1	-7	**167**	1
6	2	20	477	0

x = 167

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

Solution:

a = 1 1 0

$a^{-1} = 1\,1\,0^{\,7-1} \; mod \; 1011 = 1\,1\,0^6 \; mod \; 1011$

a^2:

```
      1 1 0
     ×1 1 0
     -----------
      0 0 0
    1 1 0
  1 1 0
  ----------
  1 0 1 0 0
```

Since the degree of a^2 is greater than 2 (recall that all elements of GF(2^3) have degree at most 2) we need to divide it by the irreducible polynomial 1 0 1 1:

```
          ______1__
10 1 1 ) 1 0 1 0 0
         1 0 1 1
         -----------
         0 0 0 1 0
```

thus $a^2 = 0\,1\,0$

a^4:

```
        0 1 0
      × 0 1 0
      -----------
        0 0 0
      0 1 0
    0 0 0
  ----------
   0 0 1 0 0
```

thus $a^4 = 1\ 0\ 0$

Finally, we obtain a^6 as a^4 x a^2 :

```
        1 0 0
  ×     0 1 0
     -----------
        0 0 0
      1 0 0
    0 0 0
    ----------
  0 1 0 0 0
```

Since the degree of a^6 is greater than 2 we need to divide it by the irreducible polynomial 1 0 1 1:

```
         ______1_
10 1 1 ) 1 0 0 0
         1 0 1 1
         -----------
         0 0 1 1
```

thus $a^6 = a^{-1} = 0\ 1\ 1$