The University of Newcastle
School of Electrical Engineering and Computer Science

COMP3260 Data Security

GAME 3 SOLUTIONS

21st March 2019

Number of Questions: 5
Time allowed: 50min
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***

1. Use Fast Exponentiation to calculate 2^{57} mod 123?

Solution: 2^{57} mod 123 = 77

Workings:

x	a	z
1	2	111001 (57)
2	2	111000 (56)
2	4	11100 (28)
2	16	1110 (14)
2	10	111 (7)
20	10	110 (6)
20	100	11 (3)
32	100	10 (2)
32	37	1 (1)
77	37	0 (0)

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

Solution:

We have

$n = 296$

$296 = 2^3 \times 37$

$n = d_1 \times d_2$, $d_1 = 8$, $d_2 = 37$

$11x_1 \bmod 8 = 1 \rightarrow 3x_1 \bmod 8 = 1$

$x_1 = 3$

$11x_2 \bmod 37 = 1 \rightarrow x_2 = 11^{35} \bmod 37 = 11\times 11^{34} \bmod 37 = 11\times (11^2)^{19} \bmod 37 = 11 \times (121)^{19} \bmod 37 = 11 \times 10^{19} \bmod 37 = 11 \times 10 \times 10^{18} \bmod 37 = 36 \times (10^2)^9 \bmod 37 = 36 \times 26^9 \bmod 37 = 36 \times 26 \times 26^8 \bmod 37 = 11 \times (26^2)^4 \bmod 37 = 11 \times 10^4 \bmod 37 = 11 \times (10^2)^2 \bmod 37 = 11 \times (26)^2 \bmod 37 = 11 \times 10^2 \bmod 37 = 11 \times 26 \bmod 37 = 27$

$x_2 = 27$

$x \bmod 8 = 3$

$x \bmod 37 = 27$

We now need to find y_1 and y_2 such that

$(296/8)\, y_1 \bmod 8 = 1$

$(296/37)\, y_2 \bmod 37 = 1$

$37y_1 \bmod 8 = 5y_1 \bmod 8 = 1 \rightarrow y_1 = 5^3 \bmod 8 = 5 \times 5^2 \bmod 8 = 5$

$8y_2 \bmod 37 = 1 \rightarrow y_2 = 8^{35} \bmod 37 = 8 \times 8^{34} \bmod 37 = 8 \times (8^2)^{17} \bmod 37 = 8 \times 27^{17} \bmod 37 = 8 \times 27 \times 27^{16} \bmod 37 = 31 \times (27^2)^8 \bmod 37 = 31 \times (26)^8 \bmod 37 = 31 \times (26^2)^4 \bmod 37 = 31 \times (10)^4 \bmod 37 = 31 \times (10^2)^2 \bmod 37 = 31 \times 26^2 \bmod 37 = 31 \times 10 \bmod 37 = 14$

We get **$y_1 = 5$** and **$y_2 = 14$**.

We now get the solution
$x = (37×3×5 + 8×27×14) \bmod 296 = 27$

Thus the multiplicative inverse of 11 modulo 296 is 194.

Check: $11 × 27 \bmod 296 = 297 \bmod 296 = 1$

3. Find the inverse of 11 modulo 296 using Euler's Totient function.

Solution:

We can use Euler's theorem:

$$x = 11^{\Phi(296)-1} \bmod 296$$

$$296 = 2^3 × 37$$

$$\Phi(296) = 2^2 × (37-1) = 4 × 36 = 144$$

$$x = 11^{\Phi(296)-1} \bmod 296 = 11^{144-1} \bmod 296 = 11^{143} \bmod 296$$

Using fast exponentiation, we get

$$\begin{aligned}
x &= 11^{143} \bmod 296 = 11×11^{142} \bmod 296 \\
&= 11×(11^2)^{71} \bmod 296 = 11×121^{71} \bmod 296 \\
&= 11×121×121^{70} \bmod 296 = 147×(121^2)^{35} \bmod 296 \\
&= 147×137^{35} \bmod 296 = 147×137×137^{34} \bmod 296 \\
&= 11×(137^2)^{17} \bmod 296 = 11×121^{17} \bmod 296 \\
&= 11×121×121^{16} \bmod 296 = 147×(121^2)^8 \bmod 296 \\
&= 147×137^8 \bmod 296 = 147×(137^2)^4 \bmod 296 \\
&= 147×121^4 \bmod 296 = 147×(121^2)^2 \bmod 296 \\
&= 147×137^2 \bmod 296 = 147×121 \bmod 296 = 27
\end{aligned}$$

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

Solution:

i	y	u	v	g
0		1	0	296
1		0	1	11
2	26	1	-26	10
3	1	-1	**27**	1
4	10	11	-296	0

x = 27

5. Consider GF(2^3) with the irreducible polynomial p(x)=1011 (x3+x+1). Find the multiplicative inverse of 0 1 0.

Solution:

a = 0 1 0

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

a^2:

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

Thus $a^2 = 1\ 0\ 0$

a^4:

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

Since the degree of a^4 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 0 0 0
         1 0 1 1
         -----------
         0 0 1 1 0
```

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

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

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

Since the degree of a^6 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_1
10 1 1 ) 1 1 0 0 0
           1 0 1 1
           -----------
           0 1 1 1 0
             1 0 1 1
        --------------
             0 1 0 1
```

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