OLD DOMINION UNIVERSITY
CS 463

Homework 6

Madelene McFarlane

10/6/2023

#01096496

CS-463/563 Crytography for Cyber Security
Fall 2023
Homework Assignment #6

August 9, 2023

Points: 20

Question 1. Using Euclidean algorithm find GCD(378, 336). Show you work.

Question 2. Using Extended Euclidean algorithm find the multiplicative inverse of 9 in mod 37 domain. Show your work including the table.

i	r_i	q_{i-1}	s_i	t_i
0	37		1	0
1	9		0	1
2				
3				
4				
5				
6				

Question 3. Determine $\phi(3200)$. (Note that 1,2,3,5, 7, ... etc. are the primes). Show your work.

Question 4. Find the multiplicative inverse of 9 in GF(37) domain using Fermat's little theorem. Show your work. Question 5. Using Euler's theorem, find the following exponential: 7^{300} mod 31. Show how you have employed Euler's theorem here.

Bonus question [10 extra points]: Write a program (in any programming language) to implement Extended Euclidean algorithm with two input parameters a and b, and return the output as b^{-1} mod a. Run the program with $a = 47$ and $b = 7$ as input and print the results. Submit the source code and the output.

What to submit? Submit a single pdf file with your answers via Canvas. Show your work.

CS 463 HW 6

Madeleine McFarlane

■ : answer

(1)

GCD (378, 336)

$378 = 336 \cdot q + r$

$378 = 336 \cdot 1 + 42$

$\frac{378}{42} = 9$

$336 = 42 + 8$

$\frac{336}{42} = 8$

GCD(378, 336) = 42

CS 463 Madelene McFarlane

HW 6

= answer

(2)

i	r_i	q_{i-1}	s_i	t_i
0	37		1	0
1	9		0	1
2	$37 \bmod 9 = 1$	$37 - 1/9 = 4$	$1 - 4 \cdot 0 = 1$	$0 - 4 \cdot 1 = -4$
3	$9 \bmod 1 = 0$	$9 - 0/1 = 9$	$0 - 9 \cdot 1 = -9$	$1 - 9 \cdot -4 = 37$

$9^{-1} \bmod 37 = -4 \bmod 37 = \boxed{33}$

CS 463 Madeleine McFarlane

HW 6

■ = answer

(3) $\phi(n) = n \cdot (1 - \frac{1}{p_1}) \cdot (1 - \frac{1}{p_2}) \cdot \ldots \cdot (1 - \frac{1}{p_k})$

$3{,}200 = 2^7 \cdot 5^2$

$\phi(3{,}200) = 3{,}200 \cdot (1 - \frac{1}{2}) \cdot (1 - \frac{1}{5})$

$= 3{,}200 \cdot \frac{1}{2} \cdot \frac{4}{5}$

$= 1{,}280$

$\phi(3{,}200) = 1{,}280$

CS 463 Madelene McFarlane

HW 6

(4)

$a^{p-1} \cong 1 \pmod{p}$

inverse of 1 in GF(37)

$9^{37-1} \cong 1 \pmod{37}$

$9^{36} \cong 1 \pmod{37}$

$9^{35} \cdot 9^{-1} \cong 1 \cdot 9^{-1} \pmod{37}$

$9^{32 \cdot 2} \cdot 9^{-1} \cong 1 \cdot 9^{-1} \pmod{37}$

$1 \cdot 9^{-1} \cong 9^{-1} \pmod{37}$

$9^{-1} \cong 33$

$9 \cdot 33 \cong 1 \pmod{37}$

CS 463
HW 6

Madelene McFarlane

= answer

(5)

$$a^{\phi(n)} \cong 1 \pmod{n}$$

$$\phi(31) = 31 - 1 = 30$$

$$7^{30} \cong 1 \pmod{31}$$

$$7^{300} = 7^{10 \cdot 30}$$

$$(7^{30})^{10}$$

$$1^{10} \pmod{31}$$

$$= 1$$

$$7^{300} \bmod 31 = 1$$

main.py

```python
def extendedEuclideanAlgorithm(a, b):
    #if loop so that way the process will keep running until an answer is formed
    if a == 0:
        return b, 0, 1

    gcd, temp1, temp2 = extendedEuclideanAlgorithm(b % a, a)

    x = temp2 - (b // a) * temp1
    y = temp1

    return gcd, x, y

print("Please enter in your inputs for a and b")
#Enter in inputs in the following format a (space) b
#Example: 81 3
a, b = map(int, input().split())
output, x, y = extendedEuclideanAlgorithm(a, b)
print("The result is", output)
```

```
Please enter in your inputs for a and b
47 7
The result is 1

Process finished with exit code 0
```