



Daffodil International University

Assignment Submission

Course Code: CS-509

Course Name: Cryptography

Topic Name: AES, RSA



Name: Dr. Rubaiyat Islam

Designation: Associate Professor

Department: Cyber security

Daffodil International University

Name: Md. Tanjim Mahmud Tuhin

ID: 251-56-012

Section: A

Semester: 3

Department: Cyber security

Daffodil International University

Submission Date: 12/12/2025

Answer 01

@ GCD of 198, 243

$$198 = 1 \times 198$$

$$= 2 \times 99$$

$$= 3 \times 66$$

$$= 6 \times 33 = 9 \times 22$$

$$= 11 \times 18$$

$$243 = 1 \times 243$$

$$= 3 \times 81$$

$$= 9 \times 27$$

common divisor = 3, 9

GCD = 9

(b)

1819 & 3587

$$1819 = 1 \times 1819$$

$$= 17 \times 107$$

$$3587 = 1 \times 3587$$

$$= 17 \times 211$$

Common divisor = 17

GCD = 17

② Find GCD using Euclid's Algo

③ 7469 & 2464

Q	a	b	r
3	7469	2464	77
32	2464	77	0
	77	0	x

$$\therefore \text{GCD} = 77$$

④ 2689 & 4001

Q	a	b	r
1	4001	2689	1312
2	2689	1312	65
20	1312	65	12
5	65	12	5
2	12	5	2
2	5	2	1
1	2	1	1
1	1	1	0
1	1	0	x

\therefore no GCD.

③ from euler's totient function.

$$1 \leq n < m$$

Given determine $\varphi(m)$ for $m = 12, 15, 26$

for $m = 12$

co prime one. 1, 5, 7, 11.

$$\gcd(n, 12) = 1$$

$$\therefore \varphi(12) = 4$$

for $m = 15$

co prime one 1, 2, 4, 7, 8, ~~10~~, ~~11~~, ~~13~~, ~~14~~

$$\varphi(15) = 8$$

for $m = 26$

co prime one 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25

$$\varphi(26) = 12$$

P Q

$$n = p \times q$$

$$\phi = (p-1)(q-1)$$

$$p = 31, q = 37, e = 17, y = 2$$

$$n = pq = 1147, \phi = 1080$$

NO	a	b	d	k
1	1	0	1080	-
2	0	1	17 (6,3)	
3	-1	3	9	1
4	-1	64	8	1
	2	127	(1)	
x				
y				

$$\begin{aligned} & \text{ant by } \text{gcd}(a, b) \\ & \phi \downarrow \quad e \downarrow \\ & 1080x + 17y = 1 \\ & \quad \downarrow \quad \downarrow \\ & \quad 2 \quad -127 \end{aligned}$$

$$\begin{aligned} a_4 &= a_2 - (a_3 * k_3) \\ b_4 &= b_2 - (b_3 * k_3) \\ a_3 &= a_1 - (a_2 * k_2) \end{aligned}$$

$$a_3 = a_1 - (a_2 * k_2)$$

$$\begin{array}{r} a + \phi \\ \hline -127 + 1080 \\ \hline 953 = d \end{array}$$

$$\text{rged } (\quad)$$

$$\begin{aligned} c &= y^e \pmod{n} \\ &= 2^{17} \pmod{1147} \\ &= 319 \end{aligned}$$

$$\begin{aligned} & \text{if } d \nmid \phi \\ & d \pmod{n} \end{aligned}$$

$$14^{27} \bmod 55$$

2^0
 2^1
 2^2
 2^3
 2^4
 2^5
 2^6
 2^7
 2^8
 2^9
 2^{10}
 2^{11}
 2^{12}
 2^{13}
 2^{14}
 2^{15}
 2^{16}
 2^{17}
 2^{18}
 2^{19}
 2^{20}
 2^{21}
 2^{22}
 2^{23}
 2^{24}
 2^{25}
 2^{26}
 2^{27}

$$\begin{array}{r} 16 \\ 8 \\ \hline 11 \end{array} \quad \begin{array}{r} 8 \\ 11 \\ \hline 1 \end{array}$$

$$14^1 \bmod 55 = 14$$

$$14^2 \bmod 55 = 31$$

$$14^4 \bmod 55 = 41$$

$$14^8 \bmod 55 = 41$$

$$14^6 \bmod 55 = 41$$

0
1
2
3
4
5
6
7
8
9

⑥ Answer:

$$p = 41 \quad q = 17 \quad \varphi = 40$$

$$n = p \cdot q = 41 \cdot 17 = 697$$

$$\varphi = (p-1)(q-1) = 640$$

$$ax + by = \gcd(a, b)$$

$$\varphi x + ey = \gcd(\varphi, e)$$

a	b	d	k
1	0	640	-
0	1	49	13
1	-13	3	16
-16	209	1	
	d		
	7		

7) Answer:

$$\gcd(67, 12)$$

a	b	ϕ	k
1	0	67	-
0	1	12	5
1	-5	7	1
-1	6	5	1
2	-11	2	2
-5	28	1	*

d
↓

$$d = a + b$$

$$0 + 21 -$$

$$21$$

Answer 8:

$$p=5 \quad q=11 \quad e=3 \quad m=9$$

$$n = 5 \times 11 = 55$$

$$\phi(n) = (5-1)(11-1) = 40$$

a	b	d	K
1	0	40	-
0	1	3	13
•13	•13	1	
		d	

as d negative

$$\begin{aligned} d + \phi \\ = -13 + 40 \\ = 27 \end{aligned}$$

Ciphertext:

$$C = x^e \bmod n$$

$$= 9^3 \bmod 55$$

$$= 14$$

Plaintext

$$P = C^d \bmod n$$

$$= 14^{27} \bmod 55$$

$$2^4 \quad 2^3 \quad 2^2 \quad 2^1 \quad 2^0$$

$$9^1 \mod 55 = 9$$

$$9^2 \mod 55 = 26$$

$$9^4 \mod 55 = 26 \times 26 \mod 55 = 16$$

$$16 \times 16 \mod 55 = 36$$

$$36 \times 36 \mod 55 = 31$$

$$\therefore (9 \times 26 \times 16 \times 36 \times 31) \mod 55 = 4$$

$$\therefore c = 14 \quad p = 4$$

Q.E.D.

(b) Ans:

$$p=31 \quad q=37 \quad e=17 \quad \gamma=m=2$$

$$n = p \times q = (31 \cdot 37) = 1147$$

$$\phi = (31-1)(37-1) = 1080$$

a	b	d	K
1	0	1080	-
0	1	17	63
0	1	-63	1
-10	64	8	
2	-127	1	
16			
	d		

As d is negative

$$d + \phi$$

$$= -127 + 1080$$

$$= 953$$

$$c = 2^{17} \pmod{1147}$$

$$= 314$$

$$p = 314^{953} \pmod{1147}$$

$$\begin{matrix} 2^9 & 2^8 & 2^7 & 2^6 & 2^5 & 2^4 & 2^3 & 2^2 & 2^1 & 2^0 \end{matrix}$$

$$314^1 \pmod{1147} = 314 -$$

$$314^2 \pmod{1147} = 1101$$

$$314^4 \pmod{1147} = 969$$

$$314^8 \pmod{1147} = 715 -$$

$$314^{16} \pmod{1147} = 810 -$$

$$314^{32} \pmod{1147} = 16 -$$

$$314^{64} \pmod{1147} = 256$$

$$314^{128} \pmod{1147} = 157 -$$

$$314^{256} \pmod{1147} = 562 -$$

$$314^{512} \pmod{1147} = 419 -$$

$$(314 \times 715 \times 810 \times 16 \times 157 \times 562 \times 419) \pmod{1147}$$

$$= 2$$

$$\therefore c = 314$$

$$p = 2$$

2
11