



Daffodil
International
University

Assignment Submission

Course Code: CS-509

Course Name: Cryptography

Topic Name: AES, RSA

Submitted To

Name: Dr. Rubaiyat Islam

Designation: Associate Professor

Department: Cyber security

Daffodil International University

Submitted By

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

$$\text{GCD} = 9$$

(b)

1819 & 3587

$$1819 = 1 \times 1819$$

$$= 17 \times 107$$

$$3587 = 1 \times 3587$$

$$= 17 \times 211$$

Common divisor = 1, 17

$$\text{GCD} = 17$$

② Find GCD using Euclid's Algo

@ 7469 & 2464

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

$\therefore \text{GCD} = 77$

⑥ 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	0	x

$\therefore \text{no GCD.}$

③ from euler's totient function.
 $1 \leq n < m$

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

for $m=12$

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

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

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

for $m=15$

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

$$\phi(15) = 8$$

for $m=26$

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

$$\phi(26) = 12$$

$$n = p \times q$$

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

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

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

No	a	b	d	k
1	1	0	1080	-
2	0	1	17	(6.3)
3	-1	3	9	1
4	-1	6	8	1
	2	-17	1	

\swarrow \swarrow
 x $y = d$

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

$$1080x + 17y = 1$$

$$x = 2, y = -127$$

$$a_4 = a_2 - (a_3 \times k_3)$$

$$b_4 = b_2 - (b_3 \times k_3)$$

$$a_3 = a_1 - (a_2 \times k_2)$$

$$d + \phi$$

$$-127 + 1080$$

$$d = 953$$

$$e = y^e \bmod n$$

$$= 2^{17} \bmod 1147$$

$$= 314$$

if $d < \phi$
 d_{mod}

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

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

$$\begin{array}{r} 16 \quad 8 \quad 4 \quad 2 \quad 1 \\ \hline 1 \quad 1 \quad 0 \quad 1 \quad 1 \end{array}$$

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

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

$$14^4 \bmod 55 = 10$$

$$14^8 \bmod 55 = 1$$

$$14^6$$

$$(a, b) \bmod p = ra + sb$$

$$(c, d) \bmod p = rc + sd$$

$$r \quad b \quad d \quad 0$$

$$- \quad 0 \quad 0 \quad 1$$

$$1 \quad 0 \quad 1 \quad 0$$

$$1 \quad 1 \quad 1 \quad 1$$

$$1 \quad 0 \quad 0 \quad 1$$

$$\downarrow$$

$$1 \quad 0 \quad 0 \quad 1$$

$$\downarrow$$

$$1 \quad 0 \quad 0 \quad 1$$

$$1 \quad 0 \quad 0 \quad 1$$

$$\downarrow$$

$$1 \quad 0 \quad 0 \quad 1$$

$$\downarrow$$

$$1 \quad 0 \quad 0 \quad 1$$

$$\begin{array}{r} 14 \quad 14 \quad 14 \quad 14 \quad 14 \\ \hline 1 \quad 1 \quad 1 \quad 1 \quad 1 \end{array}$$

⑥ Answer:

$$p = 41 \quad q = 17 \quad e = 49$$

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

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

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

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

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

↓
d

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:

$$\begin{aligned} C &= x^e \bmod n \\ &= 9^3 \bmod 55 \\ &= 14 \end{aligned}$$

plaintext

$$\begin{aligned} P &= C^d \bmod n \\ &= 14^{27} \bmod 55 \end{aligned}$$

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

$$9^1 \bmod 55 = 9$$

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

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

$$16 \times 16 \bmod 55 = 36$$

$$36 \times 36 \bmod 55 = 31$$

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

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

Q.E.D.

⑥ Ans:

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

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

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

a	b	d	k
1	0	1080	-
0	1	17	63
1	-63	9	1
-10	64	8	1
2	-127		
	↓		
	d		

As d is negative

$$\begin{aligned} & d + \phi \\ &= -127 + 1080 \\ &= 953 \end{aligned}$$

$$C = 2^{17} \bmod 1147$$

$$= 314$$

$$P = 314^{953} \bmod 1147$$

$$2^{29} \quad 2^{28} \quad 2^{27} \quad 2^{26} \quad 2^{25} \quad 2^{24} \quad 2^{23} \quad 2^{22} \quad 2^{21} \quad 2^{20}$$

$$314^1 \bmod 1147 = 314 \text{ ---}$$

$$314^2 \bmod 1147 = 1101$$

$$314^4 \bmod 1147 = 969$$

$$314^8 \bmod 1147 = 715 \text{ ---}$$

$$314^{16} \bmod 1147 = 810 \text{ ---}$$

$$314^{32} \bmod 1147 = 16 \text{ ---}$$

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

$$314^{128} \bmod 1147 = 157 \text{ ---}$$

$$314^{256} \bmod 1147 = 562 \text{ ---}$$

$$314^{512} \bmod 1147 = 419 \text{ ---}$$

$$(314 \times 715 \times 810 \times 16 \times 157 \times 562 \times 419) \bmod 1147$$

$$= 2$$

$$\therefore C = 314$$

$$P = 2$$

2