Project 16 $p = 137, q = 241, e = 53$, and $a = 12345$

Step 1

Compute $n = pq = 137 \cdot 241 = 33017$

Step 2

Encrypt a: $c = a^e \; MOD \; n$

Modular Exponentiation

a	e	n
12345	53	33017
12345	53	12345
25570	26	
22266	13	7245
24501	6	
16924	3	22259
32318	1	24983

$c = 24983$

Step 3

Compute $\phi = (p-1)(q-1) = 136 \cdot 240 = 32640$

Step 4

Compute d: $\gcd(\phi, e)$

Greatest Common Denominator

a	b	q	r	s	t
32640	53	615	45	-20	12317
53	45	1	8	17	-20
45	8	5	5	-3	17
8	5	1	3	2	-3
5	3	1	2	-1	2
3	2	1	1	1	-1
2	1	2	0	0	1
1	0			1	0

$d = 12317$

Step 5

Decrypt c: $c^d \; MOD \; n$

Modular Exponentiation

c	d	n
24983	12317	33017
24983	12317	24983
29938	6158	
4362	3079	19746
9252	1539	6931
19440	769	29280
1018	384	
12797	192	
31906	96	
12692	48	
29938	24	
4362	12	
9252	6	
19440	3	23137
1018	1	12345