Rajat M. Jain
SAMHITA
B6/17ISO31
Date: 11/4/2020

1.a) $n = 3599$

w.k.t : $\gcd(n, e) = 1$

~~$\gcd(3599,$~~

Let $e = 2$

$\gcd(3599, 2) = 1$

$\therefore$ Smallest value of $e = 2$.

1.b) Given $n = 3599$ $p = 59$ $q = 61$

$e = 13$

$n = p \times q$

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

$= (58)(60) = 3480$

Primes -

~~2, 3, 5, 7~~,

Since

$3600 = 60 \times 60$

$\therefore$ Try $59 \times 61$

$= 3599$

$\therefore p = 59$

$q = 61$

w.k.t $e \times d \equiv 1 \bmod \phi(n)$

$\therefore d = e^{-1} \bmod \phi(n)$

$\therefore d = 13^{-1} \bmod (3480)$

Kajal M. Jain
1BG17IS031
11/4/2020.

## Extended Euclid's – $b = b_1$ $c = c_1$

$r = 2$

| Iteration | $b'$ | $c'$ | $q$ | $r$ | $x_1$ | $x_2$ | $y_1$ | $y_2$ | $x * c + y * b$ |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 3480 | 13 | – | 2 | 1 | 0 | 0 | 1 | 3480 |
| 2 | 13 | 2 | 267 | 9 | 0 | 1 | 1 | 0 | |
| 3 | 2 | 9 | 6 | 1 | 1 | -267 | 0 | 1 | |
| 4 | | | | | | | | | |

Rajat M Jain
1BG17IS031
SAMRAT
Date 11/04/2020 Page

2.a) $5^{43} \bmod 77$

$43 = 101011$

| 1 | 0 | 1 | 0 | 1 | 1 |
|---|---|---|---|---|---|
| $5^{32} \bmod 77$ | $5^{16} \bmod 77$ | $5^{8} \bmod 77$ | $5^{4} \bmod 77$ | $5^{2} \bmod 77$ | $5 \bmod 77$ |
| 25 | 16 | 4 | 9 | 25 | 5 |

$(25 \times 4 \times 25 \times 5) \bmod 77$

$= \underline{26}$

Rajat M. Jain
1BG17IS031
11/4/2020

2.b) $p = 53$

$g = 2$

$a = 15$

$b = 33$

$X_A = (g)^a \bmod p$

$= (2)^{15} \bmod 53$

$= \underline{14}$ → A's public key

$X_B = (g)^b \bmod p$

$= (2)^{33} \bmod 53$

$= (2)^{15} (2)^{15} (2)^3 \bmod 53$

$= (14 \times 14 \times 8) \bmod 53$

$= \underline{31}$ → B's public key.

Secret key, $K = (g)^{ab} \bmod p$

$= (2)^{15 \times 33} \bmod p$

$= (2)^{15} \times (2)^{15} \times (2)^{15} \times (2)^3 \bmod 53$

$= (14^3 \times 8) \bmod 53 = 10$ //

17CS061
4