

1.a) $n = 3599$

w.k.t

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

~~$$\gcd(3599, 2)$$~~

Let

$$e = 2$$

$$\gcd(3599, 2) = 1$$

 \therefore Smallest value of $e = 2$.

1.b)

Given $n = 3599$ $p = 59$ $q = 61$
 $e = 13$

$$n = p \times q$$

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

$$= (58)(60) = 3480$$

w.k.t $e \times d \equiv 1 \pmod{\phi(n)}$

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

$$\therefore d = 13^{-1} \pmod{3480}$$

Primes -

~~2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 187, 191, 193, 197, 199, 211, 223, 227, 229, 233, 239, 241, 251, 257, 263, 269, 271, 277, 281, 283, 293, 307, 311, 313, 317, 331, 337, 347, 349, 353, 359, 367, 373, 379, 383, 389, 397, 401, 409, 419, 421, 431, 433, 439, 443, 449, 457, 461, 463, 467, 479, 487, 491, 499, 503, 509, 521, 523, 527, 539, 541, 547, 557, 563, 569, 571, 577, 587, 593, 599, 601, 607, 613, 617, 619, 623, 627, 631, 637, 641, 643, 647, 653, 659, 661, 667, 671, 673, 677, 683, 687, 691, 697, 701, 703, 707, 709, 713, 719, 727, 731, 733, 737, 739, 743, 747, 751, 757, 761, 763, 767, 769, 773, 777, 781, 787, 791, 793, 797, 799, 803, 807, 809, 811, 817, 821, 823, 827, 829, 833, 837, 839, 843, 847, 851, 853, 857, 859, 863, 867, 869, 871, 873, 877, 881, 883, 887, 891, 893, 897, 899, 903, 907, 909, 911, 913, 917, 919, 923, 927, 929, 931, 933, 937, 939, 941, 943, 947, 949, 953, 957, 959, 961, 963, 967, 969, 971, 973, 977, 979, 983, 987, 989, 991, 993, 997, 999~~

Since

$$3600 = 60 \times 60$$

$$\therefore \text{Try } 59 \times 61$$

$$= 3599$$

$$\therefore p = 59$$

$$q = 61$$

Kajal M. Jain
 18G17ISO31
 11/4/2020.

Extended Euclid's - $b = b'$ $c = c'$
 $n = 2$

Steps	b'	c'	q	r	x_1	x_2	y_1	y_2	$x \cdot c + y \cdot b$
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									

$(a) \phi \text{ term } 1 \equiv b \times 1$

$(a) \phi \text{ term } 2 \equiv b \times 2$

$(0 \times 1 + 2) \text{ term } 3 \equiv b \times 3$

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

$43 = 101011$

$$\begin{array}{ccccccc} 1 & 0 & 1 & 0 & 1 & 1 & \\ \hline 5^1 \mod 77 & 5^0 \mod 77 & 5^1 \mod 77 & 5^0 \mod 77 & 5^1 \mod 77 & 5^1 \mod 77 & 5^1 \mod 77 \\ 5 & 1 & 5 & 1 & 5 & 5 & 5 \end{array}$$

$$\begin{array}{ccccccc} 1 & 0 & 1 & 0 & 1 & 1 & \\ \hline 5^1 \mod 77 & 5^0 \mod 77 & 5^1 \mod 77 & 5^0 \mod 77 & 5^1 \mod 77 & 5^1 \mod 77 & 5^1 \mod 77 \\ 5 & 1 & 5 & 1 & 5 & 5 & 5 \end{array}$$

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

$= \underline{\underline{26}}$

Rajat M. Jain

18G1715031

11/4/2020

$$2.6) \quad p=53$$

$$g=2$$

$$a=15$$

$$b=33$$

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

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

$$= \underline{14} \rightarrow A's \text{ public key}$$

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

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

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

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

$$= \underline{31} \rightarrow B's \text{ public key}$$

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

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

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

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

17CS061
4