

IS: Examples on Unit-II

1. Find $3^{110} \text{ mod } 13$
2. Find the smallest positive residue y in the given congruence: $7^{69} = y \text{ mod } 23$
3. To find the totient function of $n = 91$
4. If $n = 77$, find $\Phi(n)$.
5. If $n = 143$, find $\Phi(n)$.
6. If $n = 5488$, find $\Phi(n)$.
7. Compute $\text{GCD}(2071, 206)$ using Euclid's algorithm.
8. Compute $\text{GCD}(12345, 2345678)$ using Euclid's algorithm.
9. Find p and q such that $56p + 72q = 40$ and also find $\text{GCD}(56, 72)$
10. Find the multiplicative inverse of $35 \text{ mod } 11$, using extended Euclidean algorithm.
11. Find the multiplicative inverse of $-74 \text{ mod } 501$, using extended Euclidean algorithm.
12. If $p = 3$ and $q = 19$. Find out the possible public key and private key for RSA algorithm.
Also encrypt the message "6".
13. In a public key cryptosystem using RSA, given $N=187$, and the encryption key (e) has 17, find out the corresponding private key (d).
14. What is the value of d if $p=3$, $q=11$ and $e=7$. Use RSA algorithm.
15. For $p=11$, $q=19$ and $e=17$. What is the value of cipher text if message = 5. Use RSA algorithm.
16. What is the value of d if $p=11$, $q=13$ and $e=11$. Use RSA algorithm.
17. How many primitive roots the number 15 has? Calculate all possible primitive roots for 15.
18. How many primitive roots does 25 have?

Prof. U. K. Raut
IS- Course Coordinator