M 8167

Reg. No. : ....

Name : ....

VI Semester B.Sc. Degree (CCSS – Reg./Supple./Improv.) Examination, May 2015
CORE COURSE IN MATHEMATICS
6B14MAT : (5) Number Theory and Cryptography
(Elective)

Time : 3 Hours Max. Weightage : 30

1. Fill in the blanks : **(Weight 1)**
   a) If p is a prime, then $a^p \equiv$ __________ for any integer 'a'.
   b) $\tau(180) =$ __________
   c) A number-theoretic function f is said to be multiplicative if f (mn) = __________, whenever gcd (m, n) = 1.
   d) A block cipher with block length n and plain text and cipher space Z_m^n is called __________

Answer **any seven** from the following : **(Weightage 1 each)**

2. Find gcd (12378, 3054).
3. If p is a prime and p | ab, prove that p | a or p | b.
4. Prove that any absolute pseudoprime is square free.
5. Show that the function σ is a multiplicative function.
6. Prove that $\sum_{d/n} \mu(d) = 0$.
7. For u > 2, prove that $\phi(u)$ is an even integer.
8. If p is a prime, prove that $(p-1)! \equiv (-1) \pmod{p}$.

P.T.O.

9. Solve the linear congruence equation $18x \equiv 30 \pmod{42}$.

10. Define the following :
    a) Affine Cipher
    b) The Hill Cipher.

11. Define the following with examples :
    a) RSA modules
    b) encryption component.

Answer **any seven** from the following : **(Weightage 2 each)**

12. Determine all solutions in positive integers of $123x + 360y = 99$.

13. Solve the system of simultaneous congruences $x \equiv 1 (\text{mod } 3)$, $x \equiv 2 (\text{mod } 5)$, $x \equiv 3 (\text{mod } 7)$.

14. If p is a prime and suppose that $p \nmid a$, prove that $a^{p-1} \equiv 1 (\text{mod } p)$.

15. Let n be a composite square – free integer say $n = p_1, p_2, \ldots p_r$, where the p_i are distinct primes. If $p_{i-1} \mid u - 1$ for $i = 1, 2, \ldots, r$, prove that n is an absolute pseudoprime.

16. If f is a multiplicative function and F is defined by $F(u) = \sum_{d/u} f(d)$, prove that F is also multiplicative.

17. Let F and f be two number-theoretic functions related by the formula $F(u) = \sum_{d/u} f(d)$, prove that $f(u) = \sum_{d/n} \mu\left(\frac{\mu}{d}\right) F(d)$.

18. If the integer $u > 1$ has the prime factorization $u = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}$, prove that $\phi(u) = u\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \ldots \left(1 - \frac{1}{p_r}\right)$.

19. Find the remainders when 2^{50} and 41^{65} are divided by 7.

20. Which of the following schemes is a Crypto System ? What is the plain text space ? The Cipher text-space and the key space. Let $\varepsilon = 726$
    1) Each letter $\sigma \in \varepsilon$ is replaced by $k\sigma \mod 26$, $K \in \{1, 2, \ldots, 26\}$.

21. Show that in the RSA cryptosystem the decryption exponent d can be chosen such that $de \equiv 1 \mod \text{lcm}(p - 1, q - 1)$.

22. Verify that encryption and decryption are inverse operations.

Answer **any two** from the following : **(Weight 4 each)**

23. State and prove Chinese Remainder Theorem.

24. Prove that the quadratic congruence $x^2 + 1 \equiv 0 \pmod{p}$, where p is an odd prime, has a solution if and only if $p \equiv 1 \pmod{4}$.

25. Let (n, e) be a public RSA key and d, the corresponding private RSA key. Prove that $(m^e)^d \mod n \equiv m$ for any integer m with $0 \le m < n$.

____