|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **VIDYAVARDHAKA COLLEGE OF ENGINEERING**  **Autonomous Institute, Affiliated to Visvesvaraya Technological University, Belagavi**  **Gokulam, 3rd Stage, Mysuru 570 002** | | | | |
| **Fifth Semester B.E. Examinations** | | | | |
| **COURSE NAME: NUMBER THEORY AND CRYPTOGRAPHY** | | | | |
| **Duration: 3-hour Max. Mark: 100** | | | | |
| **INSTRUCTION TO STUDENTS**  **1) Answer One Full question from each module** | | | | |
| **Q. No.** | **Module-I** | **Marks** | **BL** | **CO** |
| **1. (a)** | Use Euclidean algorithm to obtain integers and satisfying: | **6** | **L3** | **2** |
| **1. (b)** | Determine all integer solutions of the following Diophantine equations: | **7** | **L3** | **2** |
| **1. (c)** | Use Chinese remainder theorem to solve the simultaneous congruence: | **7** | **L3** | **2** |
| **Module-II** | | | | |
| **2.(a)** | State and prove Euler’s theorem. | **6** | **L2** | **1** |
| **2.(b)** | Find the last two digits of | **7** | **L3** | **2** |
| **2.(c)** | Prove that is a finite field with respect to the binary operations addition and multiplication modulo 7. | **7** | **L4** | **3** |
| **Module-III** | | | | |
| **3.(a)** | Let the integer have order modulo . Then prove that if and only if . | **6** | **L2** | **1** |
| **3.(b)** | Show that if has a primitive root then it has precisely number of primitive roots. | **7** | **L3** | **2** |
| **3.(c)** | Determine the remainder when is divided by 17. | **7** | **L3** | **2** |
| **(OR)** | | | | |
| **4.(a)** | Write the definition of Legendre symbol and evaluate | **6** | **L2** | **1** |
| **4.(b)** | If is an odd prime and , prove that a is a quadratic residue modulo if and if | **7** | **L3** | **2** |
| **4.(c)** | Solve the following quadratic congruence | **7** | **L3** | **2** |
| **Module-IV** | | | | |
| **5.(a)** | Decipher **HPCCXAQ** if the encipherment function is . | **6** | **L3** | **2** |
| **5.(b)** | Use the Vigenère cipher formula to encrypt a plaintext **ATTACKATDAWN** using a keyword **LEMON.** | **7** | **L4** | **3** |
| **5.(c)** | Use a Hill cipher with key to encrypt the following message.  **‘’Agnes Driscoll worked for NSA’’**. | **7** | **L4** | **3** |
| **(OR)** | | | | |
| **6.(a)** | In a Diffie-Hellman Key Exchange, Alice and Bob have chosen prime value and primitive root is 5. If Alice’s secret key is 4 and Bob’s secret key is 6, what is the secret key they exchanged? | **6** | **L3** | **2** |
| **6.(b)** | Use RSA algorithm, find the public key and private key with respect to and . Also encrypt and decrypt the number | **7** | **L4** | **3** |
| **6.(c)** | Evaluate the discrete logarithm of 60 to the base 4 with prime | **7** | **L4** | **3** |
| **Module- V** | | | | |
| **7.(a)** | The cubic curve has the following points say compute the points and *.* | **6** | **L2** | **1** |
| **7.(b)** | Use Miller-Robin’s primality test to show that 561 is a composite number. | **7** | **L3** | **2** |
| **7.(c)** | Explain Elliptic curve Diffie Hellman key exchange. | **7** | **L3** | **2** |