**UNIT – I**

**INTRODUCTION & NUMBER THEORY**

**PART-A**

1. **What is Network security?**
2. **List the types of primality testing?(APRIL/MAY 2011)**
3. **Define passive attack and active attack. (APRIL/MAY 2015) (APRIL/MAY 2011)** **(NOV/DEC 2011)**
4. **Mention the different types of security services.**
5. **Define cryptanalysis and cryptology.**
6. **Define the following terms:**
7. **What is Brute force attack?**
8. **Mention the various types of cryptanalytic attack.**
9. **Define the two basic building blocks of encryption techniques.**
10. **Mention few mono-alphabetic and poly-alphabetic ciphers.**
11. **What is steganography? Mention few techniques in it. (MAY/JUNE 2013)**
12. **Define Man-in-the-Middle.**
13. **Mention the various types of cryptanalytic attack.(NOV/DEC 2014)**
14. **What is Denial-of-service (DoS)?**
15. **What are computer security challenges?**
16. **Define Euclidean Algorithm.**
17. **Define Primality testing?(NOV/DEC 2011)**
18. **What is an abelian group?**
19. **What is a ring?**
20. **What is the primitive root of a number? (APRIL/MAY 2015)**
21. **What is a Field?(MAY/JUNE 2012)**
22. **What is Fermat’s Little Theorem.**
23. **State Euler’s Theorem.**
24. {\displaystyle a^{\varphi (n)}\equiv 1{\pmod {n}}}**What is the difference between diffusion and confusion? (NOV/DEC 2011)**
25. **Find the gcd (210,45) using Euclid’s algorithm. (MAY/JUNE 2013)**
26. **What is avalanche effect?** (NOV/DEC 2012)
27. **Define Replay attack? (NOV/DEC 2011)**

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |

{\displaystyle a^{p-1}\equiv 1{\pmod {p}}.**PART-B**

1. Explain the substitution encryption techniques in detail? (APRIL/MAY 2015)
2. State and derive i) Fermat’s Theorem ii) Euler’s Theorem (APRIL/MAY 2015) **(MAY/JUNE 2013)** (NOV/DEC 2012) . (NOV/DEC 2013) . (NOV/DEC 2014)
3. Discuss the classical cryptosystems and its types. (APRIL/MAY 2011) **(MAY/JUNE 2013)** (MAY/JUNE 2014)
4. Describe Euler’s theorem and Chinese remainder theorem. (APRIL/MAY 2011)(MAY/JUNE 2012) . (NOV/DEC 2014)
5. Explain any two types of Cipher technique in detail. (MAY/JUNE 2012)
6. Describe Finite Fields with their application in cryptography?(MAY/JUNE 2014)
7. Using playfair cipher algorithm encrypt the message using the key “MONARCHY” and explain.(NOV/DEC 2011)
8. Explain the ceasar cipher and monoalphabetic cipher? (NOV/DEC 2011)
9. What are the different types of attacks? Explain. (NOV/DEC 2013)
10. Find 321mod11 using Fermat’s theorem. (NOV/DEC 2013)
11. Encrypt the message “PAY” using Hill cipher with the following key matrix and show the decryption to get the original text.**[Nov/Dec 2014]**

K = 17 17 5

21 18 21

2 2 19

1. State Chinese Remainder theorem and find X for the given set of congruent equations using CRT.

X 1(mod 5)

X 2(mod 7)

X 3(mod 9)

X 4(mod 11) **[April/May 2017][Nov/Dec 2016]**

1. Explain briefly about Fermat’s and Euler’s theorem.**[Nov/Dec2012][May/June2013][Nov/Dec2016]**
2. Write about any two classical crypto systems (substitution and transposition) with suitable examples. **[May/June2013]**