Amrita Vishwa Vidyapeetham
MCA
Fourth Semester
18CA314-Cryptography and Network Security
Assignment 1

Part A

1. $a \in \mathbb{Z}_p$ Prove that $(a+p)^n (mod\ p) \equiv a^n (mod\ p)$
2. Find the multiplicative inverse of all the elements in $\mathbb{Z}_5$ and $\mathbb{Z}_{11}$
3. Determine the gcd of 56245 and 43159
4. Compute $\Phi(n)$ for 3^4 and 2^{10}
5. Compute $3^{100} mod (31319)$

Part B -Programming Assignment

1. Write a program to implement Extended Euclidean Algorithm and find multiplicative inverse for following values.
   (a) $53947^{-1} mod\ 56211$
   (b) $19385^{-1} mod\ 43159$
2. In cryptography, a brute-force attack consists of an attacker submitting many passwords or passphrases with the hope of eventually guessing correctly.

   Implement a DES algorithm in any programming language(You are free to use language libraries). and decrypt the following cipher text using brute-force attack. Convert the hexadecimal value to string in the final stage.

   Cipher text: 0x4B518774A408E3E5
3. In real world, the commonly used RSA key size if 1024 bits, which is hard for cryptanalysis with limited resources. Implement a RSA algorithm with integer data type and show that you are able to decrypt the cipher text without knowing the private key.