Information Assurance and Security(IT352) LabProgram-3(a)

Write appropriate diagrams, Equations and partial source code

Copy is not allowed. All copied submissions will he considered as Malpractice.

If any such submission is found, “FF” grade will be awarded for the course

Use any of the following programming languages: Python, Java, C++, or C to compute **Euler's totient function/Euler's phi function** by taking runtime prime numbers P and Q. Compute N =P×Q, and ϕ(n). Compute number from 1 to *n*-1 that are relatively prime to “n” by using extended Euclidean algorithm. Count the generated relatively prime numbers and compared with computed ϕ(n). Display all computed results on terminal and also store them on output file with a file name Rollnumber_IT352P3a.txt..

Upload the following files onto Moodle:

1. Source code file : Rollnumber_IT352P3a.filetype extension
2. Output file : Rollnumber_IT352P3a.txt
3. Screenshot of the results : Rollnumber_IT352P3ascreenshot.filetype Extension

----

Information Assurance and Security(IT352) LabProgram-3(b)

Write appropriate diagrams, Equations and partial source code

Copy is not allowed. All copied submissions will he considered as Malpractice.

If any such submission is found, “FF” grade will be awarded for the course

Use any of the following programming languages: Python, Java, C++, or C to implement **ELGAMAL CRYPTOSYSTEM** Key Generation, Encryption and Decryption operations by taking runtime input of large prime number “P” during key generation step.. Check primitive root condition and compute all primitive roots that are from 1 to “P-1”. Consider a runtime alpha numeric values as input for encryption, convert them into ASCII value and perform encryption operation (not as stream cipher). If any extraction condition is required, apply them and then perform encryption. Show that decryption operation is inverse of encryption operation. Show all computed results on terminal and also store the same onto an output file with a file name Rollnumber_IT352P3b.txt..

Upload the following files onto Moodle:

1. Source code file : Rollnumber_IT352P3b.filetype extension
2. Output file : Rollnumber_IT352P3b.txt
3. Screenshot of the results : Rollnumber_IT352P3bscreenshot.filetype extension

----

Information Assurance and Security(IT352) LabProgram-3(c)

Write appropriate diagrams, Equations and partial source code

Copy is not allowed. All copied submissions will he considered as Malpractice.

If any such submission is found, “FF” grade will be awarded for the course

Use any of the following programming languages: Python, Java, C++, or C to implement **Rabin Cryptosystem** Key Generation, Encryption and Decryption operations by taking runtime input of large prime number P and Q during key generation step. Check Quadratic Residue condition at the appropriate step and also any other extra condition is required to check at the time of key generation steps..Consider a runtime alpha numeric values as input for encryption, convert them into ASCII value and perform encryption operation (not as stream cipher). If any extraction condition is required, apply them and then perform encryption. Show the decryption operation is inverse of encryption operation. Use Chinese Remainder Theorem (CRT) to decrypt the cipher text. Show all computed results on terminal and also store them on output file with a file name Rollnumber_IT352P3c.txt..

Upload the following files onto Moodle:

1. Source code file : Rollnumber_IT352P3c.filetype extension
2. Output file : Rollnumber_IT352P3c.txt
3. Screenshot of the results : Rollnumber_IT352P3cscreenshot.filetype Extension

---

Information Assurance and Security(IT352) LabProgram-3(d)

Write appropriate diagrams, Equations and partial source code

Copy is not allowed. All copied submissions will he considered as Malpractice.

If any such submission is found, “FF” grade will be awarded for the course

Use any of the following programming languages: Python, Java, C++, or C to implement **RSA Cryptosystem** Key Generation, Encryption and Decryption operations by taking runtime input of large prime number P and Q for key generation. Consider a runtime alpha numeric values as input for encryption, convert them into ASCII value and then perform encryption operation (not as stream cipher). If any extraction condition is required, apply them and then perform encryption. Show the decryption operation is inverse of encryption operation. Show all computed results on terminal and also store them on output file with a file name Rollnumber_IT352P3d.txt..

Upload the following files onto Moodle:

1. Source code file : Rollnumber_IT352P3d.filetype extension
2. Output file : Rollnumber_IT352P3d.txt
3. Screenshot of the results : Rollnumber_IT352P3dscreenshot.filetype Extension

---

Information Assurance and Security(IT352) LabProgram-3(e)

Write appropriate diagrams, Equations and partial source code

Copy is not allowed. All copied submissions will he considered as Malpractice.

If any such submission is found, “FF” grade will be awarded for the course

Use any of the following programming languages: Python, Java, C++, or C to compute ***Quadratic Residue (QR) and Quadratic Non-Residue (QNR)for a given Z_n*.*** by taking runtime input ‘n’. Compute all QR and QNR from 1 to n. Display all computed results on terminal and also store them on output file with a file name Rollnumber_IT352P3e.txt..

Upload the following files onto Moodle:

1. Source code file	:	Rollnumber_IT352P3e.filetype extension
2. Output file	:	Rollnumber_IT352P3e.txt
3. Screenshot of the results	:	Rollnumber_IT352P3escreenshot.filetype extension

----
-