Information Assurance and Security (IT352) Lab Program-8
For Reg. No 181560181IT245, 191300191IT101-191023191IT129

Write a program that should demonstrate Cyclic Attack of RSA cryptosystem. Program should use the given value of (e, N, C) to demonstrate Cyclic Attack where "C" represents ciphertext, (e, N) represents public key. Program should consider given "C" value during run-time. Store all the intermediate and end results in output file (.txt).) and also display on the terminal of the system. Program should use 100 iterations to derive plain text and if these iterations are insufficient then display error message on the terminal "INSUFFICIENT ITERATION" and store the same on the output file.

Sample Test Case

1. e= 3, N=35, C=22
2. e=5, N= 143, C=33

File name of the program	:	RegisterNo_IT352_P8 (P8 indicates Lab Program Number-8)
File name of the screenshot	:	RegisterNo_IT352_P8_TCS1

(TCS1 indicates screenshot for the first test case, similarly, for other test cases TCS2, TCS3, TCS4, TC5, TC6)

File name of the Output File : RegisterNo_IT352_P8_Output_TC1.txt

(TC1 indicates output for the first test case, similarly, for other test cases TC2, TC3, TC4, TC5, TC6)

Date of Laboratory	:	6th April 2022, Wednesday
Deadline of Submission	:	6th April 2022, Wednesday on or before 9:00PM

Submit program file, all six screenshots and all six output files (output.txt) to the Moodle under the web-link title "*IT352-Lab-Program-8-Submisison Web Link*".

Note : No/Zero marks for incomplete submission/late submission/incomplete program.
No email submission is considered for evaluation.

Information Assurance and Security (IT352) Lab Program-8
For Reg. No 191IT130 - 191IT201

Write a program that should demonstrate RSA crypto system as block cipher. Program should use the given public key, private key and given message during run-time. Demonstrate the encryption operation using public key, use the generated cipher text to demonstrate the decryption operation using private key. Store all the intermediate and end results in output file (.txt).) and also display on the terminal of the system. Use ASCII values message to get the integer value.

Sample Test Case

1.	e=13, d=37, N=77,	Message= HOW ARE YOU
2.	e=343, d=12007,	Message = This is Tough

File name of the program : RegisterNo_IT352_P8 (P8 indicates Lab Program Number-8)

File name of the screenshot : RegisterNo_IT352_P8_TCS1

(TCS1 indicates screenshot for the first test case, similarly, for other test cases TCS2, TCS3, TCS4, TC5, TC6)

File name of the Output File : RegisterNo_IT352_P8_Output_TC1.txt

(TC1 indicates output for the first test case, similarly, for other test cases TC2, TC3, TC4, TC5, TC6)

Date of Laboratory : 6th April 2022, Wednesday

Deadline of Submission : 6th April 2022, Wednesday on or before 9:00PM

Submit program file, all six screenshots and all six output files (output.txt) to the Moodle under the web-link title “*IT352-Lab-Program-8-Submisison Web Link*”.

Note : No/Zero marks for incomplete submission/late submission/incomplete program.
No email submission is considered for evaluation.

Information Assurance and Security (IT352) Lab Program-8
For Reg. No 191IT202 - 191IT231

Write a program that should demonstrate short-message attack of RSA crypto system. Program should use the given public key and the cipher-text during run-time. Store all the intermediate and end results in output file (.txt).) and also display on the terminal of the system. Assume that plaintext message is always 3-digit integer number.

.

Sample Test Case

e=13, N=77, Cipher Text = 26
e=13, N=77, Cipher Text = 35

File name of the program : RegisterNo_IT352_P8 (P8 indicates Lab Program Number-8)

File name of the screenshot : RegisterNo_IT352_P8_TCS1

(TCS1 indicates screenshot for the first test case, similarly, for other test cases TCS2, TCS3, TCS4, TC5, TC6)

File name of the Output File : RegisterNo_IT352_P8_Output_TC1.txt

(TC1 indicates output for the first test case, similarly, for other test cases TC2, TC3, TC4, TC5, TC6)

Date of Laboratory : 6th April 2022, Wednesday

Deadline of Submission : 6th April 2022, Wednesday on or before 9:00PM

Submit program file, all six screenshots and all six output files (output.txt) to the Moodle under the web-link title "*IT352-Lab-Program-8-Submisison Web Link*".

Note : No/Zero marks for incomplete submission/late submission/incomplete program.
No email submission is considered for evaluation.

Information Assurance and Security (IT352) Lab Program-8
For Reg. No 191IT232 - 191IT258

Write a program that should demonstrate key generation steps of RSA crypto system. Program should use the given P, Q and 'e' during run-time. Demonstrate all steps involved in generating key pairs of RSA crypto system. Store all the intermediate and end results in output file (.txt).) and also display on the terminal of the system. If key pair cannot be generated then print the error message "Key Pair Cannot Be Generate" on the terminal and also store on the output file.

Sample Test Case

1. P=13, Q=19, e=3
2. P=19, Q=29 e=5

File name of the program : RegisterNo_IT352_P8 (P8 indicates Lab Program Number-8)

File name of the screenshot : RegisterNo_IT352_P8_TCS1

(TCS1 indicates screenshot for the first test case, similarly, for other test cases TCS2, TCS3, TCS4, TC5, TC6)

File name of the Output File : RegisterNo_IT352_P8_Output_TC1.txt

(TC1 indicates output for the first test case, similarly, for other test cases TC2, TC3, TC4, TC5, TC6)

Date of Laboratory : 6th April 2022, Wednesday

Deadline of Submission : 6th April 2022, Wednesday on or before 9:00PM

Submit program file, all six screenshots and all six output files (output.txt) to the Moodle under the web-link title "*IT352-Lab-Program-8-Submisison Web Link*".

Note : No/Zero marks for incomplete submission/late submission/incomplete program.
No email submission is considered for evaluation.