Information Assurance and Security (IT352) Lab Program-9
For Reg. No 181560181IT245, 191300191IT101-191023191IT129

Write a program that should demonstrate RSA cryptosystem-based digital signature creation and verification. Program should consider the given P, Q and e values to generate the private key “d” value, then display the generated “d” value on to the terminal and also store the same onto the output file. Show RSA cryptosystem-based digital signature creation by displaying all intermediate results, Message and Digital Signature (Message, Signature) pair on the terminal and also store the same on to the output file. Further, show the digital signature verification steps by displaying all intermediate results on the terminal and also store them on the output file. Use ASCII value of the corresponding message in your computation.

Sample Test Case

1.	e= 313,	P=823,	Q=953,	Message = NITK-Surathkal
2.	e=527	P=43,	Q=47	Message = Good Friday

File name of the program : RegisterNo_IT352_P9 (P9 indicates Lab Program Number-9)

File name of the screenshot : RegisterNo_IT352_P9_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_P9_Output_TC1.txt

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

Date of Laboratory : 13th April 2022, Wednesday

Deadline of Submission : 13th April 2022, Wednesday on or before 7:00 PM

Submit program file, all six screenshots and all six output files (output.txt) to the Moodle under the web-link title “*IT352-Lab-Program-9-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-9
For Reg. No 191IT130 - 191IT201

Write a program that should demonstrate **RSA cryptosystem-based digital signature creation on MD5 message digest and also verification**. Program should consider the given P, Q and e values to generate the private key “d” value, then display the generated “d” value on to the terminal and also store the same onto the output file. Show RSA cryptosystem-based digital signature creation on MD5 message digest by displaying all intermediate results, Message and Digital Signature (Message, Signature) pair on the terminal and also store the same on to the output file. Further, show the digital signature verification steps by displaying all intermediate results on the terminal and also store them on the output file. Use ASCII value of the corresponding message in your computation.

Sample Test Case

1.	e= 313	P=823	Q=953	Message = Mangalore-575025
2.	e=527	P=43,	Q=47	Message = preservence0102

File name of the program : RegisterNo_IT352_P9 (P9 indicates Lab Program Number-9)

File name of the screenshot : RegisterNo_IT352_P9_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_P9_Output_TC1.txt

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

Date of Laboratory : 13th April 2022, Wednesday

Deadline of Submission : 13th April 2022, Wednesday on or before 7:00 PM

Submit program file, all six screenshots and all six output files (output.txt) to the Moodle under the web-link title “*IT352-Lab-Program-9-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-9
For Reg. No 191IT202 - 191IT231

Write a program that should demonstrate **ElGamal digital signature creation and verification**. Program should consider the given e_1, d and p values to generate the e_2 value, then display the generated e_2 value on to the terminal and also store the same onto the output file. Show **ElGamal digital signature creation** by displaying all intermediate results, Message and Digital Signature (Message, Signature) pair on the terminal and also store the same on to the output file. Further, show the digital signature verification steps by displaying all intermediate results on the terminal and also store them on the output file. **Use 00 to 25 to letters A to Z and 26 for the space.**

Sample Test Case

1.	e_1= 2	P=3119	d=127	r-5	Message = MANGALORE
2.	e_1= 2	P=3119	d=127	r=7	Message = BANGALORE

File name of the program : RegisterNo_IT352_P9 (P9 indicates Lab Program Number-9)

File name of the screenshot : RegisterNo_IT352_P9_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_P9_Output_TC1.txt

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

Date of Laboratory : 13th April 2022, Wednesday

Deadline of Submission : 13th April 2022, Wednesday on or before 7:00 PM

Submit program file, all six screenshots and all six output files (output.txt) to the Moodle under the web-link title "*IT352-Lab-Program-9-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-9
For Reg. No 191IT232 - 191IT258

Write a program that should demonstrate **Schnorr digital signature creation and verification**. Program should consider the given values to show the steps of **Schnorr digital signature creation** by displaying all intermediate results, Message and Digital Signature (Message, Signature) pair on the terminal and also store the same on to the output file. Further, show the digital signature verification steps by displaying all intermediate results on the terminal and also store them on the output file. **Use 00 to 25 to letters A to Z and 26 for the space.** Use SHA1 hash algorithm.

Sample Test Case

1. e_1= 354 P=2263 Q=103 d=30 r-5 Message= MANGALORE, e_2=1206

2. e_1= 354 P=2263 Q=103 d=30 r=7 Message = BANGALORE e_2=1206

File name of the program : RegisterNo_IT352_P9 (P9 indicates Lab Program Number-9)

File name of the screenshot : RegisterNo_IT352_P9_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_P9_Output_TC1.txt

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

Date of Laboratory : 13th April 2022, Wednesday

Deadline of Submission : 13th April 2022, Wednesday on or before 7:00 PM

Submit program file, all six screenshots and all six output files (output.txt) to the Moodle under the web-link title "*IT352-Lab-Program-9-Submisison Web Link*".

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