Information Assurance and Security (IT352) Lab Program-7
For Reg. No 181560181IT245, 191300191IT101-191023191IT129

Use any one of the programming languages such as C/C++/Java/Python to implement steps involved in SSL in generating Cryptographic Secrets from Key Material that are computed by considering the given integer number input Pre-Master Secret (PM). Your program should generate two random numbers individually of size 32 bytes each and use them as Client Random Number (CR) and Server Random Number (SR). Use these data and follow the steps in involved in SSL to generate Master Secret (M). Use Hash-algorithm (MD5 and SHA-1) library in your program. Display the generated Client Random Number, Server Random Number and Master Secret on the terminal one after the other line-by-line and also store the same on the output file. Use the generated Master Secret and follow the steps involved in SSL to derive the Key Materials (six cryptographic secrete). Assume that each cryptographic secret of size is 8 bytes each. Display the generated six cryptographic secrets on the terminal on the one after the other line-by-line by pre-fixing appropriate key material name. Store the same on to the output file.

Sample Test Case

1. Pre-Master Secret : 123456789123456789
2. Pre-Master Secret : 987654321987654321

File name of the program : RegisterNo_IT352_P7 (P7 indicates Lab Program Number-7)

File name of the screenshot : RegisterNo_IT352_P7_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_P7_Output_TC1.txt

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

Date of Laboratory : 24^{tth} March 2022, Wednesday

Deadline of Submission : 25th March 2022, Friday on or before 7:00PM

Submit program file, all six screenshots and all six output files (output.txt) to the Moodle under the web-link title "*IT352-Lab-Program-7-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-7
For Reg. No 191IT130 - 191IT201

Use any one of the programming languages such as C/C++/Java/Python to implement Data Expansion Function of the TLS protocol. Your program should generate random number of size 32 bytes to use it as seed value. Consider generated seed value, given input secrete and use MD5 hash algorithm to generate expanded secrete of size 384 bits (48bytes). You may use the MD5 hash algorithm library in your program. Display the generated expanded secret on the terminal by pre-fixing word "Expanded Secrete is =" and store the same on to the output file.

Sample Test Case

1. Secret : 123456789123456789
2. Secret : 987654321987654321

File name of the program : RegisterNo_IT352_P7 (P7 indicates Lab Program Number-7)

File name of the screenshot : RegisterNo_IT352_P7_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_P7_Output_TC1.txt

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

Date of Laboratory : 24^{tth} March 2022, Wednesday

Deadline of Submission : 25th March 2022, Friday on or before 7:00PM

Submit program file, all six screenshots and all six output files (output.txt) to the Moodle under the web-link title "*IT352-Lab-Program-7-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-7
For Reg. No 191IT202 - 191IT231

Use any one of the programming languages such as C/C++/Java/Python to implement Data Pseudorandom Function (PRF) of the TLS protocol. Your program should generate random number of size 32 bytes to use it as seed value. Consider generated seed value, given input secrete and use label as "LABEL" to generate new secrete. You may use the MD5 and SHA1 hash algorithm libraries in your program. Display the generated new secret on the terminal by pre-fixing word "New Secrete is =" and store the same on to the output file.

.

Sample Test Case

1. Secret : 123456789123456789
2. Secret : 987654321987654321

File name of the program : RegisterNo_IT352_P7 (P7 indicates Lab Program Number-7)

File name of the screenshot : RegisterNo_IT352_P7_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_P7_Output_TC1.txt

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

Date of Laboratory : 24^{tth} March 2022, Wednesday

Deadline of Submission : 25th March 2022, Friday on or before 7:00PM

Submit program file, all six screenshots and all six output files (output.txt) to the Moodle under the web-link title "*IT352-Lab-Program-7-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-7
For Reg. No 191IT232 - 191IT258

Use any one of the programming languages such as C/C++/Java/Python to implement steps involved in TLS in generating Master Secrets by considering the given integer number input Pre-Master Secret (PM). Your program should generate two random numbers individually of size 32 bytes each and use them as Client Random Number (CR) and Server Random Number (SR). Use these data and follow the steps in involved in TLS to generate Master Secret (M) of size 160 bits (20 bytes). You may use hash algorithm (MD5 and SHA-1) libraries in your program. Display the generated Client Random Number, Server Random Number and Master Secret on the terminal one after the other line-by-line by pre-fixing appropriate name and also store the same on the output file.

Sample Test Case

3. Pre-Master Secret : 123456789123456789
4. Pre-Master Secret : 987654321987654321

File name of the program : RegisterNo_IT352_P7 (P7 indicates Lab Program Number-7)

File name of the screenshot : RegisterNo_IT352_P7_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_P7_Output_TC1.txt

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

Date of Laboratory : 24^{tth} March 2022, Wednesday

Deadline of Submission : 25th March 2022, Friday on or before 7:00PM

Submit program file, all six screenshots and all six output files (output.txt) to the Moodle under the web-link title "*IT352-Lab-Program-7-Submisison Web Link*".

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