Information Assurance and Security (IT352) Lab Program-5
For Reg. No 181560181IT245, 191300191IT101-191023191IT129

Use any one of the programming languages such as C/C++/Java/Python to implement *Initial Permutation* and *Final Permutation* operations of DES cipher. Your program should consider only the run-time plaintext input. Take the ASCII value of the given plaintext then covert them into binary form. If the binary data size is greater than predefined block size 64bits, then divide the binary data into block of 64 bits then process each block individually. Show the block of 64 bits one after the another on the terminal and also store them onto the output file before Initial Permutation operation. After completion of the Initial Permutation operation, print the output on the terminal and also store them onto an output file by prefixing word "Output of Initial Permutation Operation". Use output of Initial Permutation operation as input to Final Permutation. After completion of the Final Permutation operation, print the output on the terminal and also store them onto an output file by prefixing word "Output of Final Permutation Operation".

Sample Text Cases

1. Plain Text : Today morning show movie
2. Plain Text : Best sandalwood film actor year 2020

File name of the program : RegisterNo_IT352_P5

(P5 indicates Lab Program Number-5)

File name of the screenshot : RegisterNo_IT352_P5_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_P5_Output_TC1.txt

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

Date of Online Laboratory : 9tth February 2022, Wednesday

Deadline of Submission : 9th February 2022, Wednesday on or before 4:00PM

Submit program file, all six screenshots and all six output files (output.txt) to the Moodle under the web-link title "*IT352-Lab-Program-5-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-5
For Reg. No 191IT130 - 191IT201

Use any one of the programming languages such as C/C++/Java/Python to implement Round Key generation of the DES cipher. Your program should consider only the run-time inputs such as “Key-value”. Take the ASCII value of the entered input then covert them into binary form. If the binary input size is greater than predefined block size 56 bits, then divide the binary data into block of 56 bits then consider only the first block of 56 bits as key-value and ignore rest of the blocks. Show the first 56 bits as key-value on the terminal and also store them onto the output file before Permutation Choice-1 operation. After completion of the Permutation Choice-I operation, print the output onto the terminal and also store them onto an output file by mentioning the word “Output of the Permutation Choice-I Operation”. After completion of the Permutation Choice-2 operation, print the output on the terminal and also store them onto an output file by mentioning the word “Round Key” with appropriate round key number. Show all the generated 16 round keys.

Sample Text Cases

Key	:	NITKsurathkal
Key	:	MANGALORE

File name of the program	:	RegisterNo_IT352_P5 (P5 indicates Lab Program Number-5)
File name of the screenshot	:	RegisterNo_IT352_P5_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_P5_Output_TC1.txt

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

Date of Online Laboratory	:	9th February 2022, Wednesday
Deadline of Submission	:	9th February 2022, Wednesday on or before 4:00PM

Submit program file, all six screenshots and all six output files (output.txt) to the Moodle under the web-link title “*IT352-Lab-Program-5-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-5
For Reg. No 191IT202 - 191IT231

Use any one of the programming languages such as C/C++/Java/Python to implement *Expansion Permutation Box* operations of DES cipher. Your program should consider only the run-time plaintext inputs”. Take the ASCII value of the plaintext character then covert them into binary form. If the input size is greater than predefined block size of 64 bits, then divide the binary data into blocks of 64 bits then process each block individually. Show the block of 64 bits one after the another on the terminal and also store them onto the output file before *Expansion Permutation Box* operation. Consider only the first block of 64 bits to divide into two sub-blocks such right-subblock and left-subblock. Use the right-subblock to demonstrate the *Expansion Permutation Box* operation. After completion of the *Expansion Permutation Box* operation, print the output on the terminal and also store them onto an output file by mentioning the word “Output of Expansion Permutation Box Operation”.

Sample Text Cases

Plain Text : nitk-surathkal

Plain Text : Surathkal-575025

File name of the program : RegisterNo_IT352_P5
(P5 indicates Lab Program Number-5)

File name of the screenshot : RegisterNo_IT352_P5_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_P5_Output_TC1.txt

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

Date of Online Laboratory : 9tth February 2022, Wednesday

Deadline of Submission : 9th February 2022, Wednesday on or before 4:00PM

Submit program file, all six screenshots and all six output files (output.txt) to the Moodle under the web-link title “*IT352-Lab-Program-5-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-5
For Reg. No 191IT232 - 191IT258

Use any one of the programming languages such as C/C++/Java/Python to implement S-1 box operation of the DES cipher. Your program should consider only the run-time input. Take the ASCII value of the given input then covert them into binary form. If the binary input size is greater than 48 bits, then divide the binary data into block of 48 bits then consider only the first block of 48 bits as input to S-1 box and ignore rest of them. Show the first 48 bits as input value to S-1 box on the terminal and also store them onto the output file before S-1 box operation. After completion of the S-1 box operation, print the output onto the terminal and also store them onto an output file by mentioning the word "Output of S-1 box Operation".

Sample Text Cases

Plain Text	:	nitk surathkal mangalore
Plain Text	:	Surathkal-575025

File name of the program	:	RegisterNo_IT352_P5 (P5 indicates Lab Program Number-5)
File name of the screenshot	:	RegisterNo_IT352_P5_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_P5_Output_TC1.txt

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

Date of Online Laboratory	:	9tth February 2022, Wednesday
Deadline of Submission	:	9th February 2022, Wednesday on or before 4:00PM

Submit program file, all six screenshots and all six output files (output.txt) to the Moodle under the web-link title "*IT352-Lab-Program-5-Submisison Web Link*".

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