Information Assurance and Security (IT352) Lab Program-6
For Reg. No 181560181IT245, 191300191IT101-191023191IT129

Use any one of the programming languages such as C/C++/Java/Python to implement **Electronic Code Book (ECB) mode** of data transmission with Hill Cipher as cryptosystem. Your program should consider only the run-time plaintext input. Take the corresponding 8-bit ASCII value for the given plaintext then divide them into fixed size blocks as per the given Hill Cipher cryptosystem, process each block individually to perform Encryption and Decryption operations. Show the created blocks one after the another on the terminal and also store them onto the output file. Read the given Key-value, check its inverse exist or not, if not, terminate the program by displaying an error message “Key-inverse does not exist” on the terminal and also store the same onto an output file. If Key-inverse exists then use the Key and Key-inverse values to perform Encryption and Decryption operations, respectively. For each input block perform Encryption and Decryption operations separately. After completion of each Encryption operation, print the plaintext and the corresponding ciphertext on the terminal and also store the same onto an output file. Furthermore, perform decryption operation for the generated ciphertext block and show the output of decryption operation by displaying ciphertext and output of the decryption operation on the terminal and also store the same onto the output file.

1. Plain Text : Phishing
   Key Value : $\begin{matrix} 2 & 3 \\ 4 & 5 \end{matrix}$
2. Plain Text : SBINITKS
   Key Value : $\begin{matrix} 3 & 3 \\ 4 & 4 \end{matrix}$

File name of the program : RegisterNo_IT352_P6 (P6 indicates Lab Program Number-6)

File name of the screenshot : RegisterNo_IT352_P6_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_P6_Output_TC1.txt

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

Date of Laboratory : 16tth March 2022, Wednesday

Deadline of Submission : 17th March 2022, Thursday 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-6-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-6
For Reg. No 191IT130 - 191IT201

Use any one of the programming languages such as C/C++/Java/Python to implement **Cipher Block Chaining (CBC) mode** of data transmission with Hill Cipher as cryptosystem. Your program should consider only the run-time plaintext input. Take the corresponding 8-bit ASCII value for the given plaintext then divide them into fixed size blocks as per the given Hill Cipher cryptosystem, process each block individually to perform Encryption and Decryption operations. Show the created blocks one after the another on the terminal and also store them onto the output file. Read the given Key-value, check its inverse exist or not, if not, terminate the program by displaying an error message "Key-inverse does not exist" on the terminal and also store the same onto an output file. If Key-inverse exists then use the Key and Key-inverse values to perform Encryption and Decryption operations, respectively. For each input block perform Encryption and Decryption operations separately. After completion of each Encryption operation, print the plaintext and the corresponding ciphertext on the terminal and also store the same onto an output file. Furthermore, perform decryption operation for the generated ciphertext block and show the output of decryption operation by displaying ciphertext and output of the decryption operation on the terminal and also store the same onto the output file.

1.	Plain Text	:	Phishing				
	Key Value	:	2	3	IV Value	4	5
			4	5		7	8
2.	Plain Text	:	SBINITKS				
	Key Value	:	3	3	IV Value	3	8
			4	4		3	7

File name of the program : RegisterNo_IT352_P6 (P6 indicates Lab Program Number-6)

File name of the screenshot : RegisterNo_IT352_P6_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_P6_Output_TC1.txt

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

Date of Laboratory : 16tth March 2022, Wednesday

Deadline of Submission : 17th March 2022, Thursday 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-6-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-6
For Reg. No 191IT202 - 191IT231

Use any one of the programming languages such as C/C++/Java/Python to implement **Cipher Feedback (CFB) mode** of data transmission with Hill Cipher as cryptosystem. Your program should consider only the run-time plaintext input. Take the corresponding 8-bit ASCII value for the given plaintext to perform Encryption and Decryption operations on each of the 8-bit ASCII value individually. Show the ASCII values for the given plaintext on the terminal and also store them onto the output file. Read the given Key-value, check its inverse exist or not, if not, terminate the program by displaying an error message “Key-inverse does not exist” on the terminal and also store the same onto an output file. If Key-inverse exists then use the Key and Key-inverse values to perform Encryption and Decryption operations, respectively. Read the given IV value and show perform the Encryption and Decryption operations separately. After completion of each Encryption operation, print the plaintext and the corresponding ciphertext on the terminal and also store the same onto an output file. Furthermore, perform decryption operation for the generated ciphertext and show the output of decryption operation by displaying ciphertext and output of the decryption operation on the terminal and also store the same onto the output file.

3.	Plain Text	:	Phishing				
	Key Value	:	2	3	IV Value	4	5
			4	5		7	8
4.	Plain Text	:	SBINITKS				
	Key Value	:	3	3	IV Value	3	8
			4	4		3	7

File name of the program : RegisterNo_IT352_P6 (P6 indicates Lab Program Number-6)

File name of the screenshot : RegisterNo_IT352_P6_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_P6_Output_TC1.txt

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

Date of Laboratory : 16tth March 2022, Wednesday

Deadline of Submission : 17th March 2022, Thursday 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-6-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-6
For Reg. No 191IT232 - 191IT258

Use any one of the programming languages such as C/C++/Java/Python to implement **Output Feedback (OFB) mode** of data transmission with Hill Cipher as cryptosystem. Your program should consider only the run-time plaintext input. Take the corresponding 8-bit ASCII value for the given plaintext to perform Encryption and Decryption operations on each of the 8-bit ASCII value individually. Show the ASCII values for the given plaintext on the terminal and also store them onto the output file. Read the given Key-value, check its inverse exist or not, if not, terminate the program by displaying an error message “Key-inverse does not exist” on the terminal and also store the same onto an output file. If Key-inverse exists then use the Key and Key-inverse values to perform Encryption and Decryption operations, respectively. Read the given IV value and show perform the Encryption and Decryption operations separately. After completion of each Encryption operation, print the plaintext and the corresponding ciphertext on the terminal and also store the same onto an output file. Furthermore, perform decryption operation for the generated ciphertext and show the output of decryption operation by displaying ciphertext and output of the decryption operation on the terminal and also store the same onto the output file.

5.	Plain Text	:	Phishing			
	Key Value	:	2 3	IV Value	4	5
			4 5		7	8
6.	Plain Text	:	SBINITKS			
	Key Value	:	3 3	IV Value	3	8
			4 4		3	7

File name of the program : RegisterNo_IT352_P6 (P6 indicates Lab Program Number-6)

File name of the screenshot : RegisterNo_IT352_P6_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_P6_Output_TC1.txt

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

Date of Laboratory : 16tth March 2022, Wednesday

Deadline of Submission : 17th March 2022, Thursday 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-6-Submisison Web Link*”.

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