

Christian Wakim

Elena Ghazi

Karim Hatem

Rita Maria Charbel

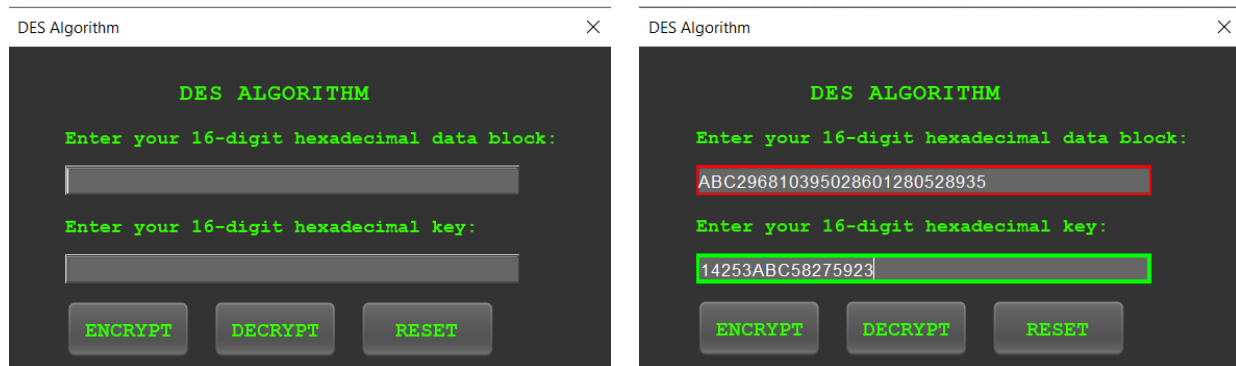
Project Report

Graphical User Interface:

We designed a GUI for DES encryption/decryption using Swing and Java.

The main page contains a field for the entry of the 16-digit (64-bit) hexadecimal plaintext/ciphertext and another field for the entry of the 16-digit (64-bit) hexadecimal key. When the correct size of the plaintext/ciphertext or key is input, the respective field turns green. Otherwise, it turns red. Then, the user has 3 options: encrypt, decrypt, or reset.

If the user has entered a plaintext with a key, he/she must click on encrypt to get the ciphertext. On the other hand, if the user enters a ciphertext with the key, he/she must click on decrypt to get the plaintext. The reset button clears the plaintext/ciphertext and key fields, allowing the user to change his/her input.



When the user clicks on either encrypt or decrypt, the main page closes, and the results page appears.

Encrypton:

Message: 21AB482389C59823
Key: 4AC5BAC314322334

OUTPUT

Go back

After performing 'Initial Permutation' on the Message:244020BB728B568A
After performing 'Permuted Choice 1' on the Key: 0E0BE4B6D92054

Round	LEFT(i-1)	RIGHT(i-1)	EXPANSION	XOR1	SBOX	PERMUTATION	XOR2	RESULT
Round 1	244020BB	728B568A	3A5456AAD454	EEB7FEA87203	0F14D2FF	6F3E5C31	4B7E7C8A	728B568A4B7E7C8A
Round 2	728B568A	4B7E7C8A	256BFC3F9454	C3E25ADF85DF	FF3C91C2	659AF257	1711A4DD	4B7E7C8A1711A4DD
Round 3	4B7E7C8A	1711A4DD	8AE8A3D096FA	3042A0D6A4D5	B83A0836	16CA0666	5DB47AEC	1711A4DD5DB47AEC
Round 4	1711A4DD	5DB47AEC	2FBDAB3F5758	068B92494EB8	0A02535F	6A7E2820	7D6F8CFD	5DB47AEC7D6F8CFD
Round 5	5DB47AEC	7D6F8CFD	BFAB5FC597FA	5BBF83C51E81	C5786651	06B5C8DC	5B01B230	7D6F8CFD5B01B230
Round 6	7D6F8CFD	5B01B230	2F6803DA41A0	79A2539DFD80	70377880	B4449287	C92B1E7A	5B01B230C92B1E7A
Round 7	5B01B230	C92B1E7A	6529568FC3F5	6BD064E6C68D	9ED9ACA7	D58B0DFB	8E8ABFCB	C92B1E7A8E8ABFCB
Round 8	C92B1E7A	8E8ABFCB	CSD4555FFE57	6BF11A562659	999CFE20	35AC55CA	FC874BB0	8E8ABFCBFC874BB0
Round 9	8E8ABFCB	FC874BB0	7F940EA57DA1	748399BD72C9	3651DE9A	FF27021B	71ADBDD0	FC874BB071ADBDD0
Round 10	FC874BB0	71ADBDD0	3A3D5BDFBEA0	472DB2474680	A8C154A0	A08D0709	5C0A4CB9	71ADBDD05C0A4CB9
Round 11	71ADBDD0	5C0A4CB9	AF80542595F2	3C40BC44F3C2	180855A2	200E244B	51A3999B	5C0A4CB951A3999B
Round 12	5C0A4CB9	51A3999B	AA3D07CF3CF6	3276917614FC	B1448435	03815E2A	5F8B1293	51A3999B5F8B1293
Round 13	51A3999B	5F8B1293	AFFC568A54A6	9BC75B2E06B0	82FA79A0	74C525C5	2566BC5E	5F8B12932566BC5E
Round 14	5F8B1293	2566BC5E	10AB0D5F82FC	139F584A401A	D07C5840	30949046	6F1E82D5	2566BC5E6F1E82D5

Key(1) 1C17C96DB240A8 D4E3A802A657
Key(2) 382F92CB648151 E689A6E0118B
Key(3) E0BE4B0D920546 BAAA0306322F
Key(4) 82F92C3648151B 29363A7619E0
Key(5) 0BE4B0E920546D E414DC00897B
Key(6) 2F92C3848151B6 56CA5047BC10
Key(7) BE4B0E020546D9 0EF932690578
Key(8) E97C3828151B64 AE754E09D80E

After shifting:71AF812EF8BCC81F
After PC1: 561333BBE2F1C8BC
CIPHER: 561333BBE2F1C8BC

Decryption:

Cipher: 561333BBE2F1C8BC
Key: 4AC5BAC314322334

OUTPUT

Go back

After performing 'Initial Permutation' on the Cipher:71AF812EF8BCC81F
After performing 'Permuted Choice 1' on the Key: 0E0BE4B6D92054Key(1) 1C17C96DB240A8 D4E3A802A657
Key(2) 382F92CB648151 E689A6E0118B
Key(3) E0BE4B0D920546 BAAA0306322F
Key(4) 82F92C3648151B 29363A7619E0
Key(5) 0BE4B0E920546D E414DC00897B
Key(6) 2F92C3848151B6 56CA5047BC10
Key(7) BE4B0E020546D9 0EF932690578
Key(8) E97C3828151B64 AE754E09D80EAfter shifting:244020BB728B568A
After PC1: 21AB482389C59823
MESSAGE: 21AB482389C59823

The results page displays every step of the encryption/decryption at every round of the process, and finally displays the ciphertext/plaintext. So, our interface shows the result of the message after each step in the encryption/decryption process at each and every round.

In addition to that, there is a “go back” button on the top right of the results page, so that when clicked, it takes the user back to the main page so that he/she inputs new plaintext/ciphertext and key for encryption/decryption.

EXPANSION	XOR1	SBOX	PERMUTATION	XOR2
3A5456AAD454	EEB7FEA87203	0F14D2FF	6F3E5C31	4B7E7C8A
256BFC3F9454	C3E25ADF85DF	FF3C91C2	659AF257	1711A4DD
8AE8A3D096FA	3042A0D6A4D5	B83A0836	16CA0666	5DB47AEC
2FBD83F5758	068B92494EB8	0A02535F	6A7E2820	7D6F8CFD
BFAB5FC597FA	5BBF83C51E81	C5786651	06B5C8DC	5B01B230
2F6803D4	Expansion Permutation is performed on the Right part of the output of the previous round through the use of the 'E table'.			E7A
6529568FC3F5	6BD064E6C68D	9ED9ACA7	D58B0DFB	8E8ABFCB
C5D4555FFE57	6BF11A562659	999CFE20	35AC55CA	FC874BB0
7F940EA57DA1	748399BD72C9	3651DE9A	FF27021B	71ADBDD0
3A3D5BDFBEA0	472DB24746B0	A8C154A0	A08D0709	5C0A4CB9
AF80542595F2	3C40BC44F3C2	180855A2	200E244B	51A3999B
AA3D07CF3CF6	3276917614FC	B1448435	03815E2A	5F8B1293
AFFC568A54A6	9BC75B2E06B0	82FA79A0	74C525C5	2566BC5E
10AB0DE582EC	130E684A001A	D02CE840	30040046	651E82DE

When hovering with the mouse over the elements of the table, the user gets a description of what the specific operation does.

Error Handling:

When the plaintext/ciphertext and key input match the required size, their respective fields turn green, indicating to the user that he/she has input the right length of key and plaintext/ciphertext.

However, if the user decides to click on encrypt/decrypt when the input is not of the right size, a dialog appears, indicating that the user has entered an invalid input.

Task Division:

For this project, we met and worked as a group on Zoom. Designing an interface was new to us, so we each did our research individually, then combined our knowledge into an interface when we met virtually. The DES encryption/decryption code was available online, but the hard part was linking our interface to the code.

Link to our demo video:

<https://www.youtube.com/watch?v=AydjFDb15xQ>

Acknowledgments:

We would like to thank Dr. Issa and Dr. Chehab for their continuous support and hard work. They were always available to answer our questions and help us through the process of developing the GUI.

References:

<https://www.geeksforgeeks.org/data-encryption-standard-des-set-1/>