 **جامعة الأزهر-غز**ة

**College of Engineering and Information Technology**

Software Engineering department

**Information Security Project**

Students are:

1. **Omar Mohammed al shaikh Khalil**

Supervised by

Dr. Ahmad Mahmoud

Semester 1 2022/2023

**Introduction**

* About Hill cipher:

The Hill cipher is a type of substitution cipher that is based on linear algebra. It was invented by Lester S. Hill in 1929. In the Hill cipher, each letter is represented by a number, which is then represented by a matrix. The encryption and decryption of the message is performed by performing matrix operations on the matrix representation of the message.

The Hill cipher is relatively easy to break, especially if the attacker knows part of the plaintext. As a result, it is not widely used in practice and has mostly been superseded by more secure encryption algorithms.

* About DES:

DES (Data Encryption Standard) is a symmetric-key algorithm for the encryption of electronic data. It was developed in the 1970s considered a powerful encryption algorithm and was widely used for secure data transmission. It uses a 56-bit key, which at the time it is developed thought to be large enough to be secure against brute force attacks.

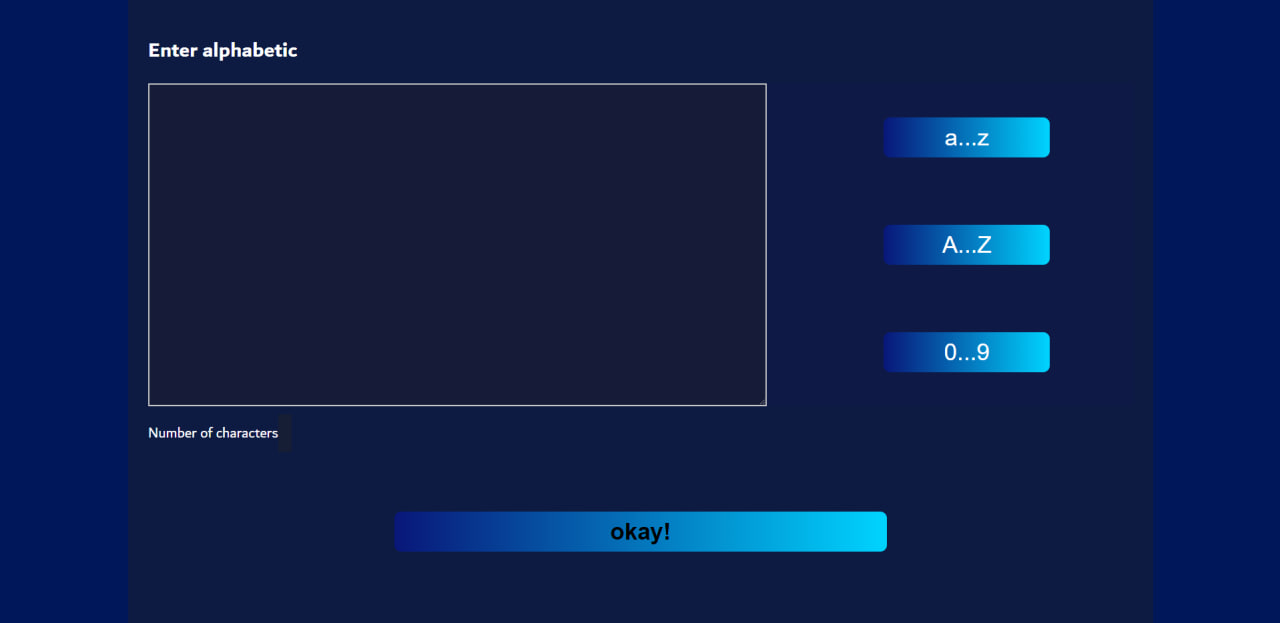
Although DES was once considered secure, it has since been broken by advances in computing power and is no longer considered secure for most applications. It has been replaced by more secure algorithms such as AES (Advanced Encryption Standard).

DES works by using the key to perform a series of transformations on the plaintext to produce the ciphertext. The transformations are designed to be reversible, so that the original plaintext can be recovered from the ciphertext by performing the same transformations in reverse.

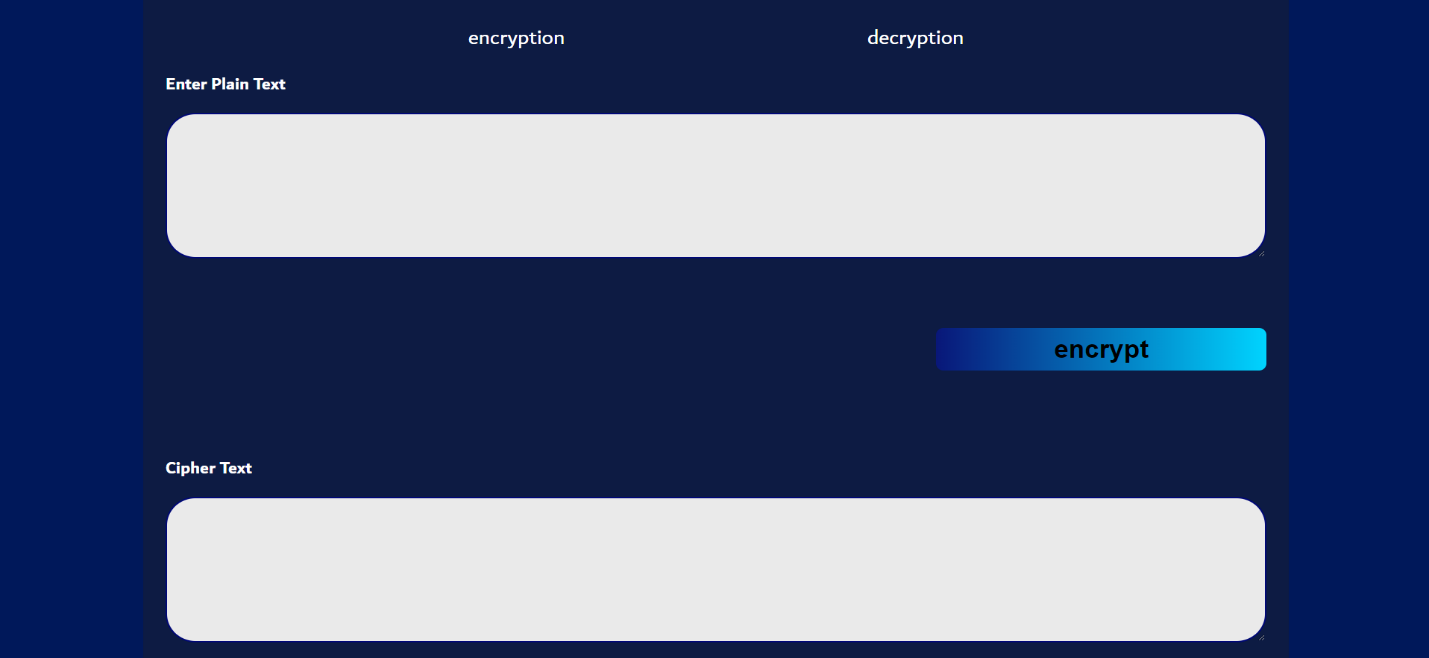
* **Algorithms we used:**

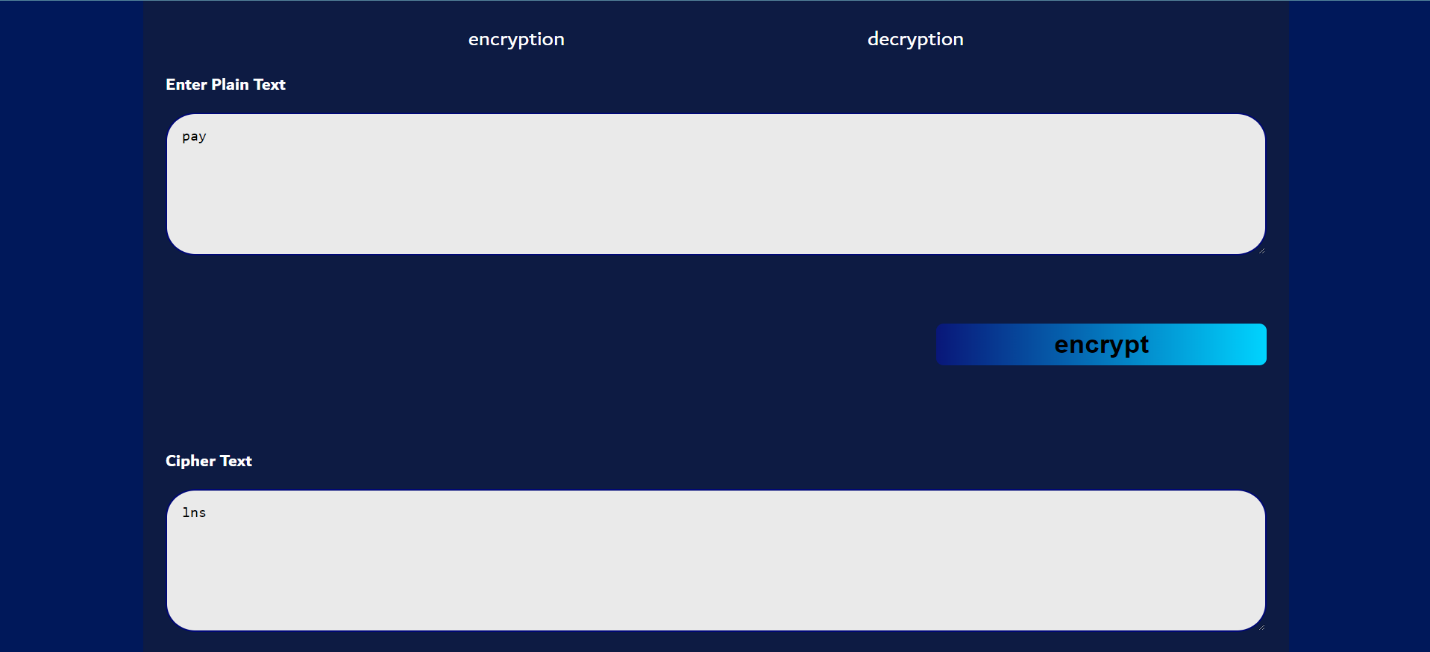
1. **Hill Cipher**
2. **DES Algorithm**

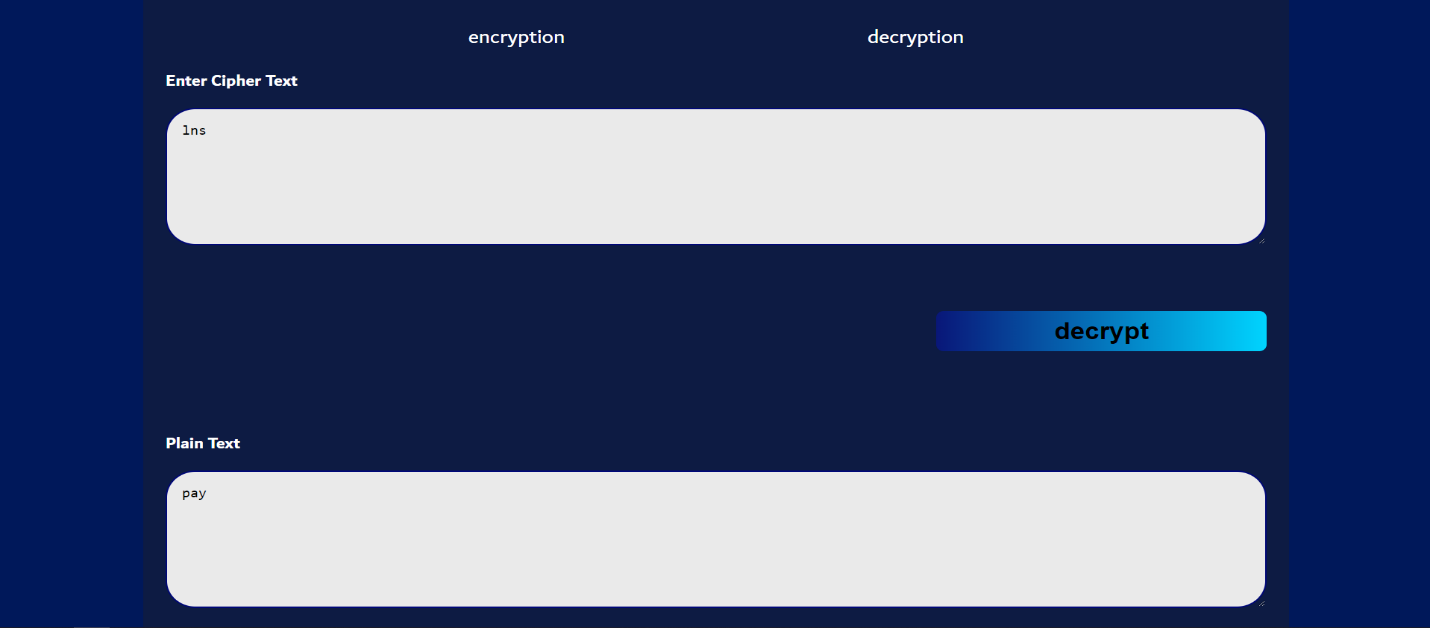
* **Mode we use:**
* **EBC Mode**
* **Videos**
* <https://youtu.be/cX9aQGvzk58> (DES)
* <https://youtu.be/JjaP3Vx3h7g> (Hill Cipher)
* **Screen shots of project**
* Hill Cipher



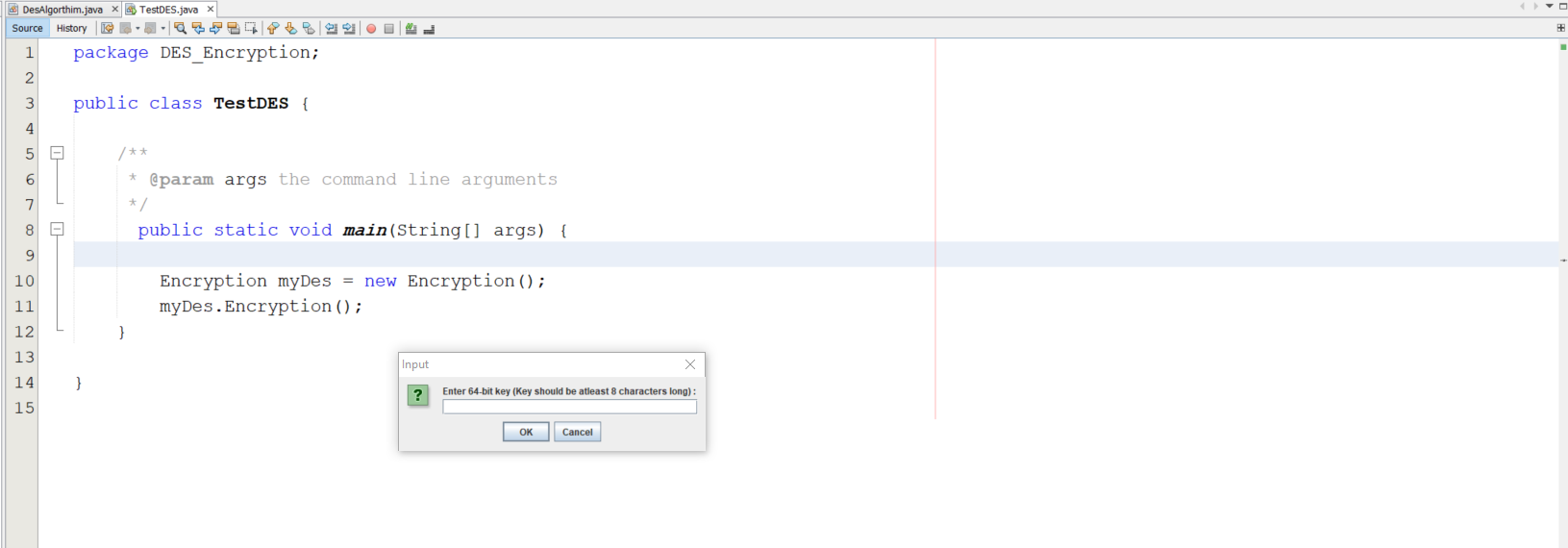


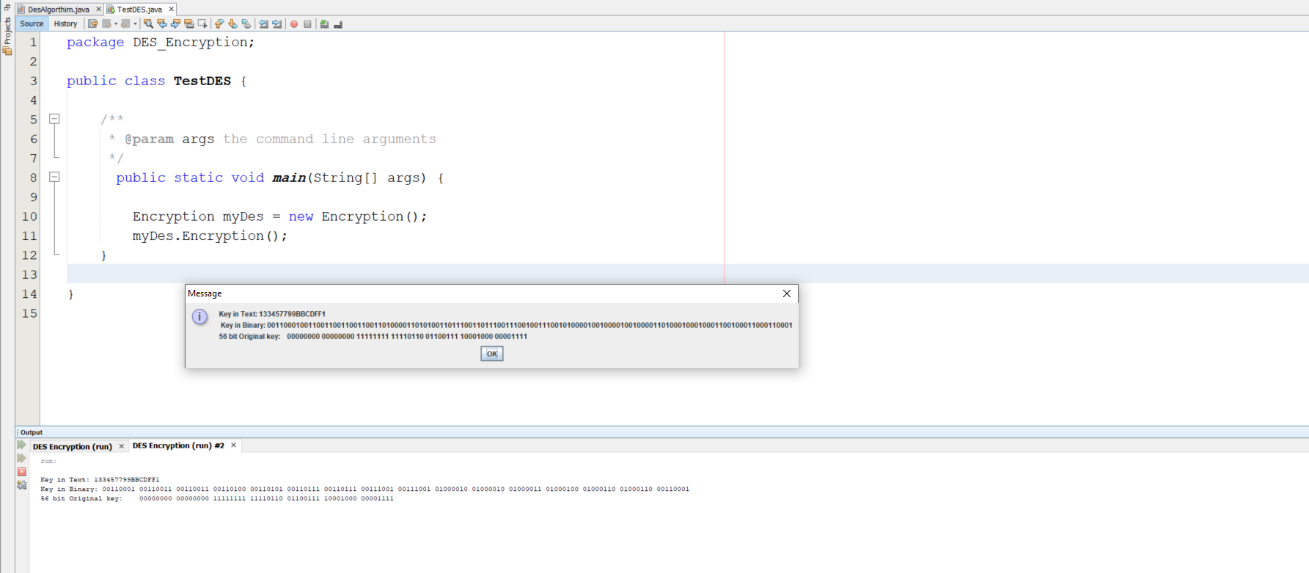


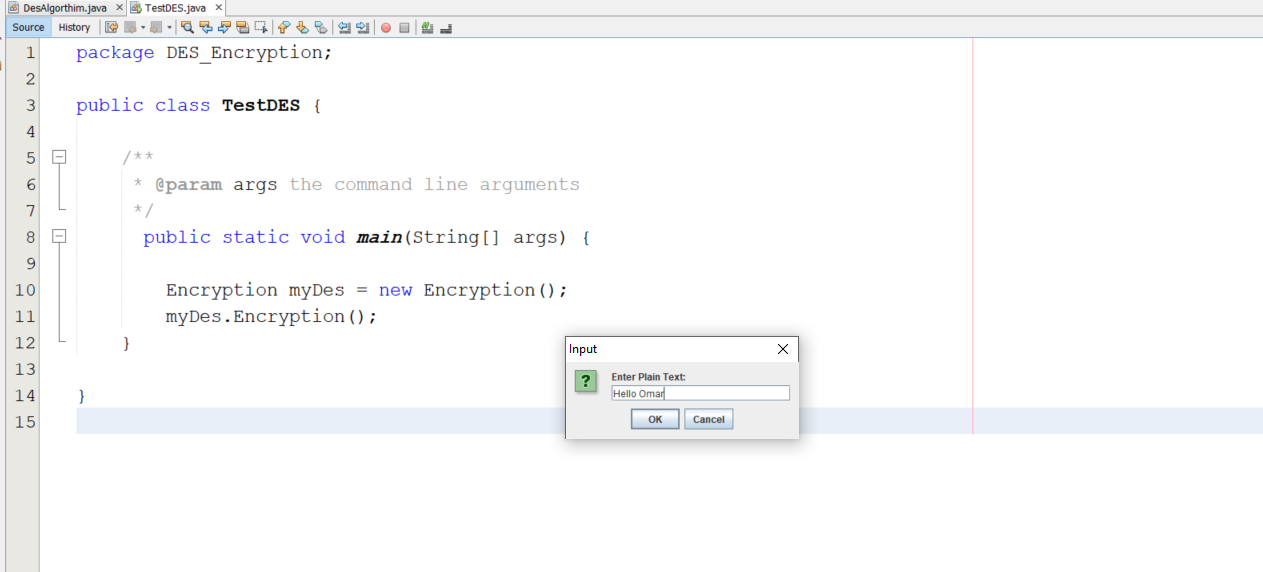


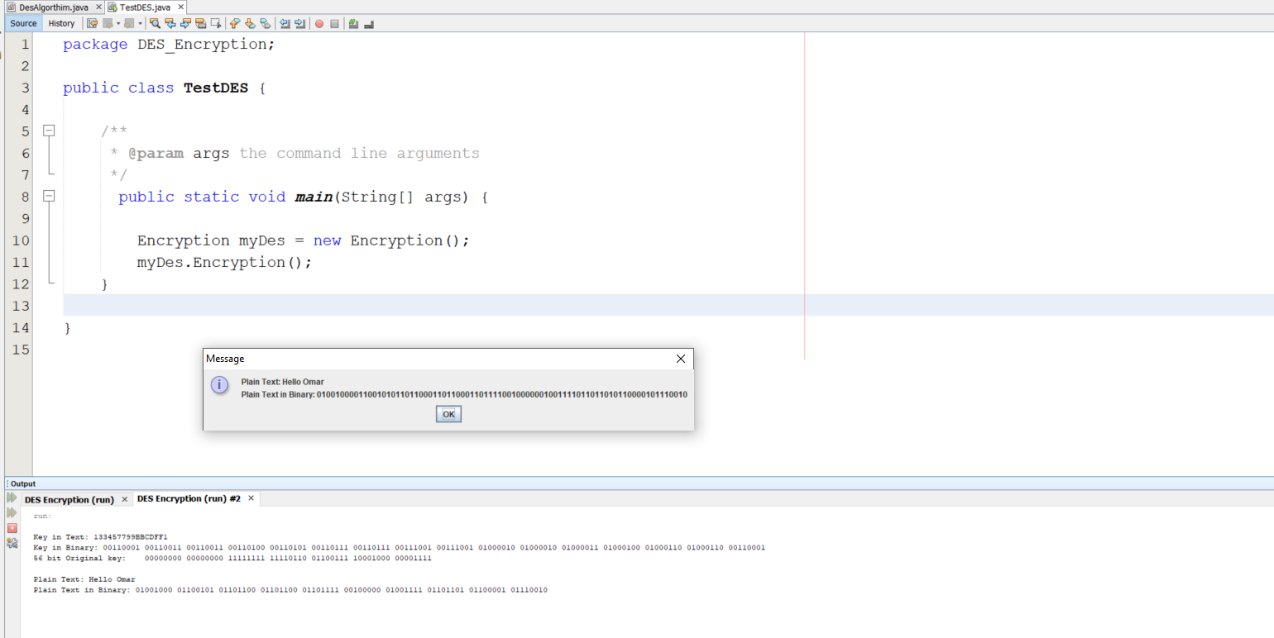


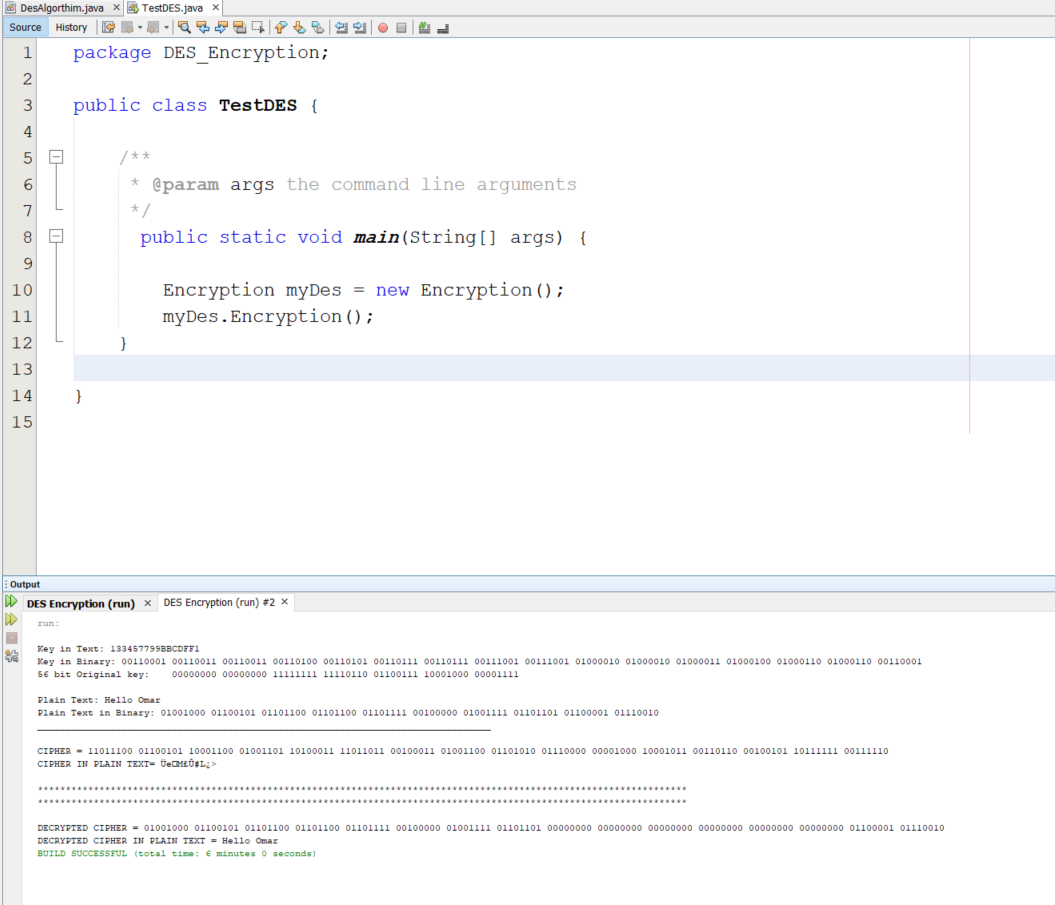
* DES

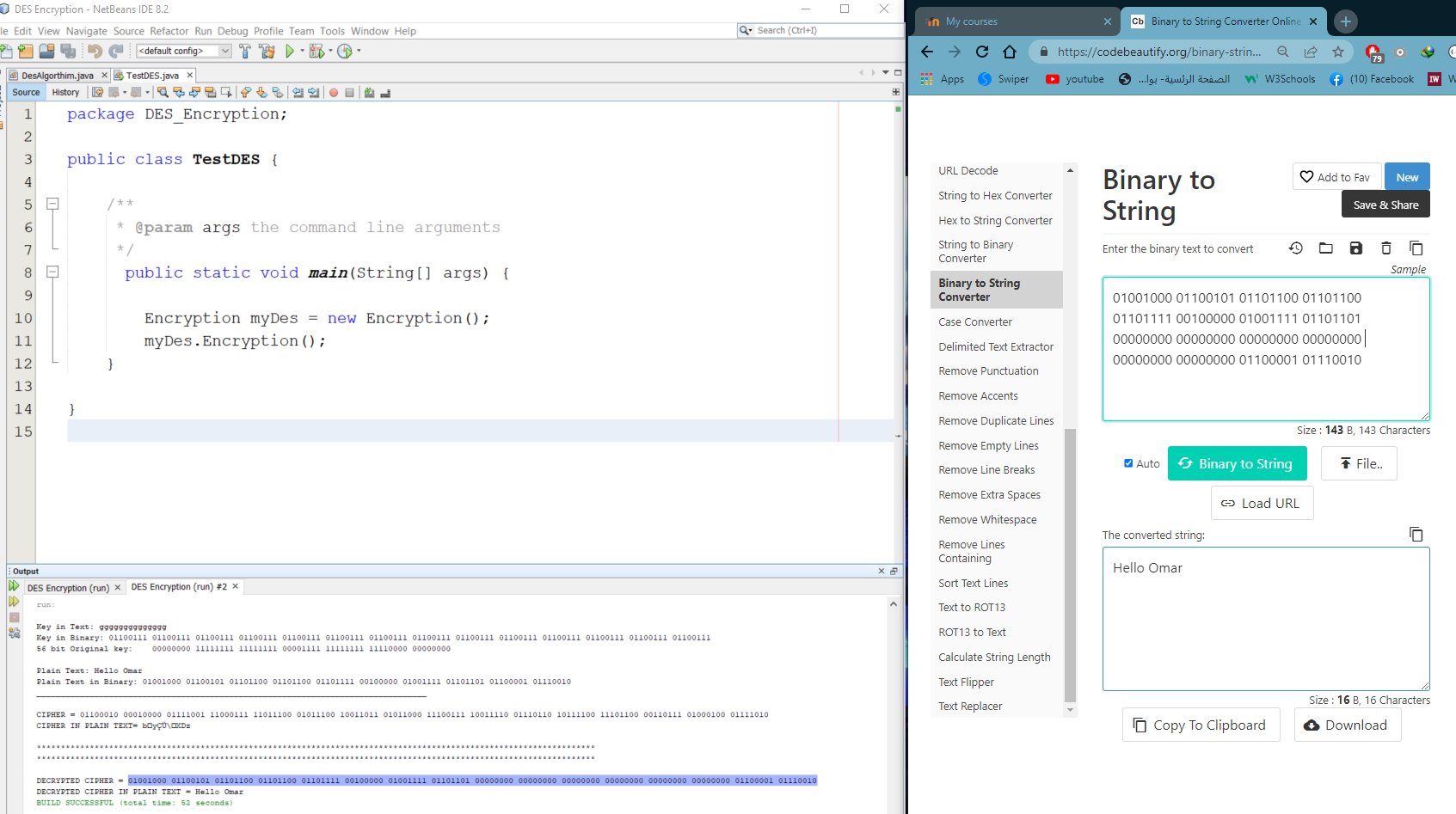






****





* **Simple Explanation:**
* We used the JavaScript language in the **Hill Cipher** encryption process and built a site using the HTML and CSS languages, and I asked the user to enter the value the Alphabet, then the key used in the encryption process and the decryption are shown, as it will check This matrix is whether it matches the conditions of the key principle or not, and then it is move to the encryption and decryption page, and everything will be shown in the video.
* We have been using the Java language to build a **DES** program:
* First, we asked to enter the key through which we will encrypt and then convert it into a number in the binary system, and then perform the Permit Choice process on it, and then print the previous data in a message.
* second request to enter the Plaintext to be encrypted and then convert it to the binary system and then print it.
* Thirdly, we do the Encryption process as it will be explained in the video and print the encrypted text as text and as a binary number.
* Finally, we do the Decryption process, print the number in the binary system, and print the Plaintext.

**References helped us:**

* <https://rb.gy/vleqni>
* <https://www.geeksforgeeks.org/data-encryption-standard-des-set-1/>
* <https://codebeautify.org/binary-string-converter>
* <https://morioh.com/p/c9f3eb99176f>