STUDENT PORTFOLIO

IAS 101 – Information Assurance and Security

2nd Term, A.Y. 2024-2025

Name: **Javier, Godfrey** **Year & Section:** **3D**

Activity: **1** **Subject:** **IAS101**

Topic: **Cryptography**

1. Choose one of the following cryptographic algorithms:

- SHA-1 (Secure Hash Algorithm 1)
- MD5 (Message Digest 5)
- DES (Data Encryption Standard)

2. Find a sample code written in either Java or Python that demonstrates the use of your chosen algorithm. You may:

- Search for open-source code on GitHub, tutorial sites, or documentation.
- Write your own simple implementation (optional for bonus points).

3. Copy the code into your document or attach it as a separate file. Be sure to:

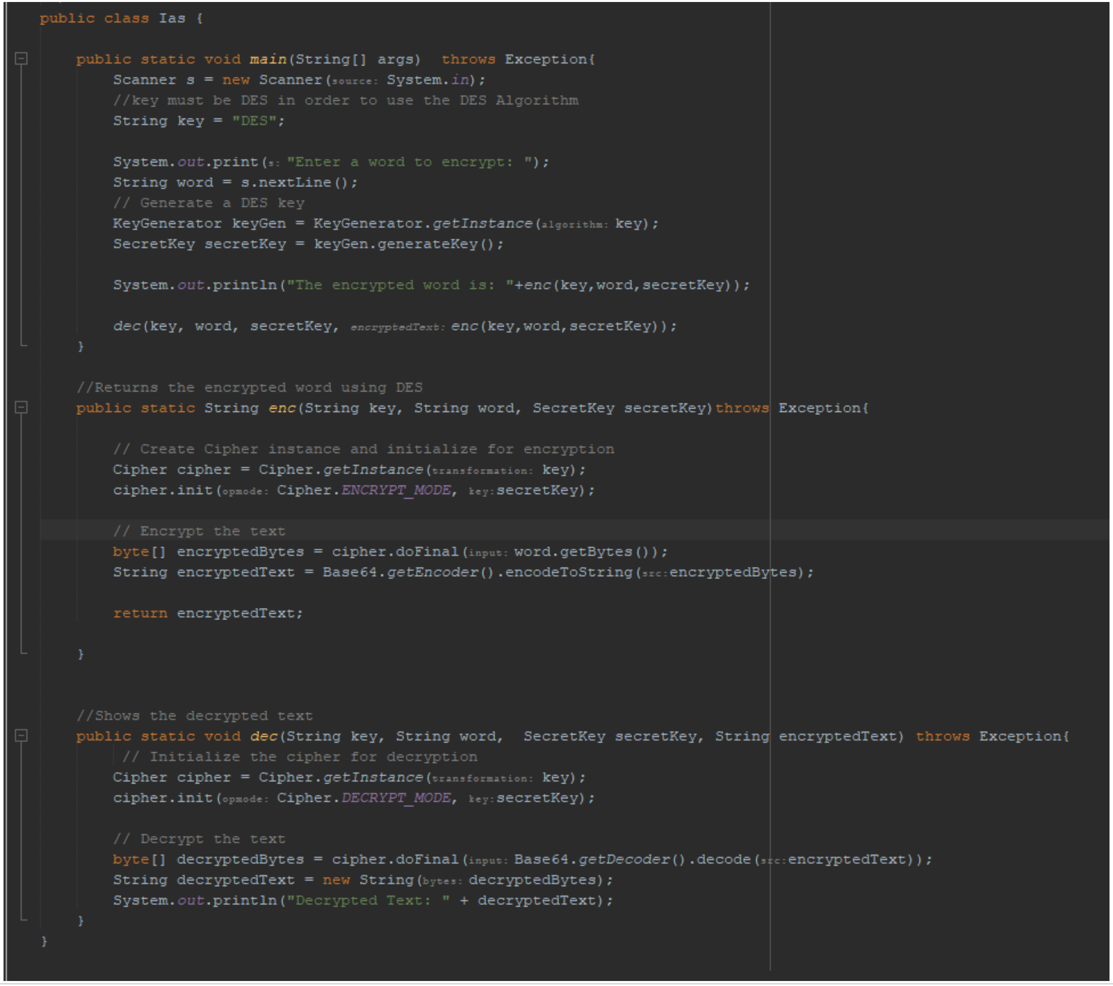
- Add brief comments to explain each step of the code (either your own or the one you found).
- Highlight which part is performing encryption, decryption, or hashing.

4. Answer the following questions below the code:

a) What does this code do?
b) What inputs are required and what outputs does it produce?
c) Why is this algorithm considered important in cryptography?
d) Are there any security concerns or limitations with this algorithm?

5. Cite your sources if you used any website, book, or article.

DATA ENCRYPTION STANDARD (Implemented by Godfrey)



```java
public class Ias {

    public static void main(String[] args)  throws Exception{
        Scanner s = new Scanner(source: System.in);
        //key must be DES in order to use the DES Algorithm
        String key = "DES";

        System.out.print(s: "Enter a word to encrypt: ");
        String word = s.nextLine();
        // Generate a DES key
        KeyGenerator keyGen = KeyGenerator.getInstance(algorithm: key);
        SecretKey secretKey = keyGen.generateKey();

        System.out.println("The encrypted word is: "+enc(key,word,secretKey));

        dec(key, word, secretKey, encryptedText: enc(key,word,secretKey));
    }

    //Returns the encrypted word using DES
    public static String enc(String key, String word, SecretKey secretKey)throws Exception{

        // Create Cipher instance and initialize for encryption
        Cipher cipher = Cipher.getInstance(transformation: key);
        cipher.init(opmode: Cipher.ENCRYPT_MODE, key:secretKey);

        // Encrypt the text
        byte[] encryptedBytes = cipher.doFinal(input: word.getBytes());
        String encryptedText = Base64.getEncoder().encodeToString(src:encryptedBytes);

        return encryptedText;

    }


    //Shows the decrypted text
    public static void dec(String key, String word,  SecretKey secretKey, String encryptedText) throws Exception{
         // Initialize the cipher for decryption
        Cipher cipher = Cipher.getInstance(transformation: key);
        cipher.init(opmode: Cipher.DECRYPT_MODE, key:secretKey);

        // Decrypt the text
        byte[] decryptedBytes = cipher.doFinal(input: Base64.getDecoder().decode(src:encryptedText));
        String decryptedText = new String(bytes: decryptedBytes);
        System.out.println("Decrypted Text: " + decryptedText);
    }
}
```

4.) Questions

a) What does this code do?

- This code can encrypt and decrypt the text input by user using Data Encryption Standard.

b) What inputs are required and what outputs does it produce?

- The required inputs here are the user message and the key must be “DES” in order to use the DES algorithm

c) Why is this algorithm considered important in cryptography?

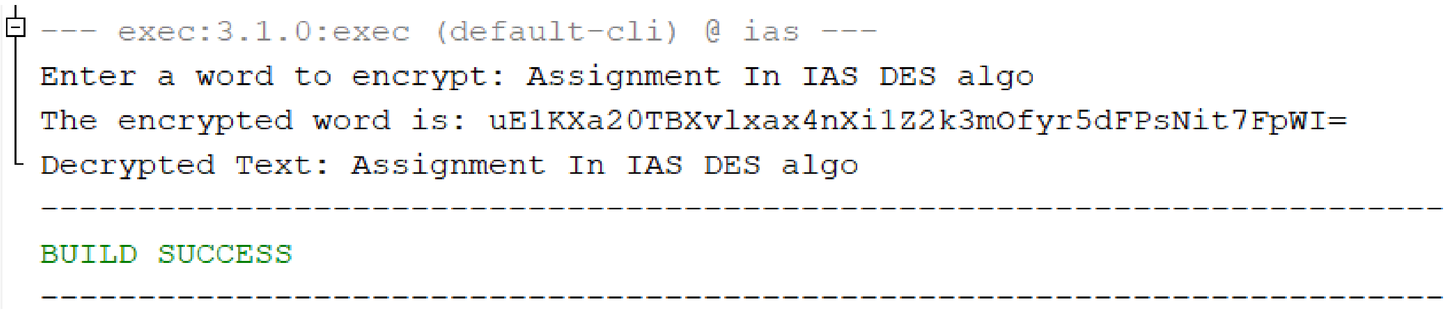
- DES was the first standardized encryption algorithm widely accepted and used by the U.S. government and commercial industries. It was adopted by NIST in 1977 as a federal standard.

d) Are there any security concerns or limitations with this algorithm?

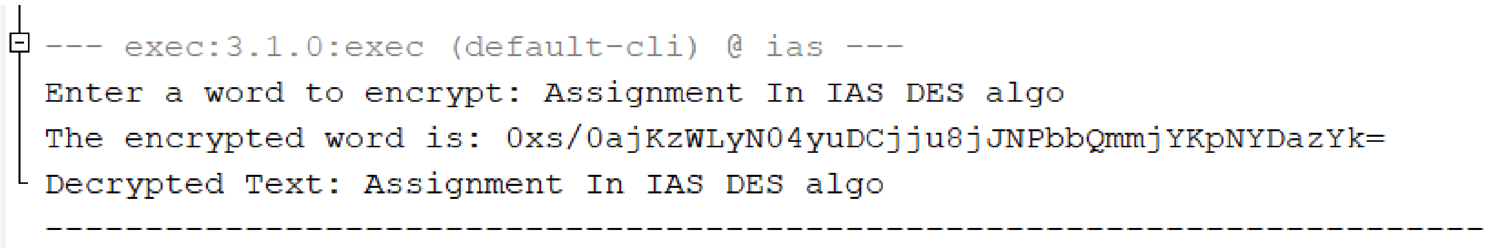
- Yes, first security concern is that there are only about 72 quadrillion possible keys in DES, modern computer can brute-force attack this in hours. Another reason is that DES is not good for encrypting large volumes of sensitive data due to short key size.

5.) Conceptualized and programmed with the help of ChatGPT.

Sample Output with same text input



```
--- exec:3.1.0:exec (default-cli) @ ias ---
Enter a word to encrypt: Assignment In IAS DES algo
The encrypted word is: uE1KXa20TBXvlxax4nXi1Z2k3mOfyr5dFPsNit7FpWI=
Decrypted Text: Assignment In IAS DES algo
------------------------------------------------------------------------
BUILD SUCCESS
------------------------------------------------------------------------
```



```
--- exec:3.1.0:exec (default-cli) @ ias ---
Enter a word to encrypt: Assignment In IAS DES algo
The encrypted word is: 0xs/0ajKzWLyN04yuDCjju8jJNPbbQmmjYKpNYDazYk=
Decrypted Text: Assignment In IAS DES algo
------------------------------------------------------------------------
```