Name: _____ **Student ID:**_____

You will need:
A computer with internet access to CyberChef (https://gchq.github.io/CyberChef/)

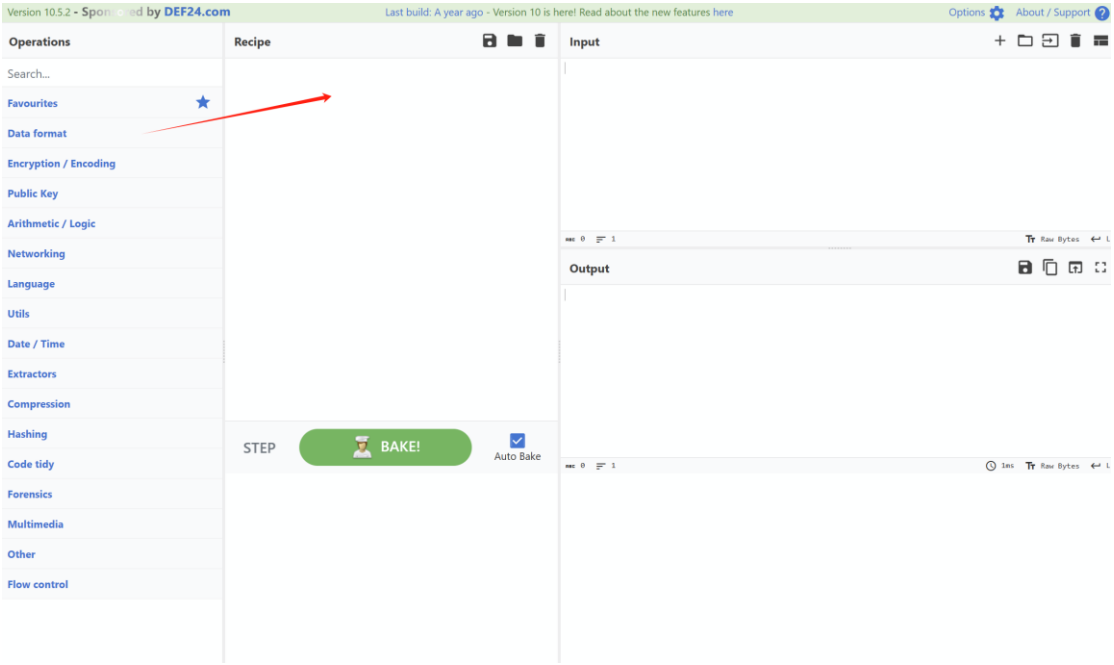
COS30015 IT Security

Lab 8 week 8

In this lab you will do some exercises about encryption algorithms**.** This lab is based on the **CyberChef** (https://gchq.github.io/CyberChef/)

Part 1: Data format

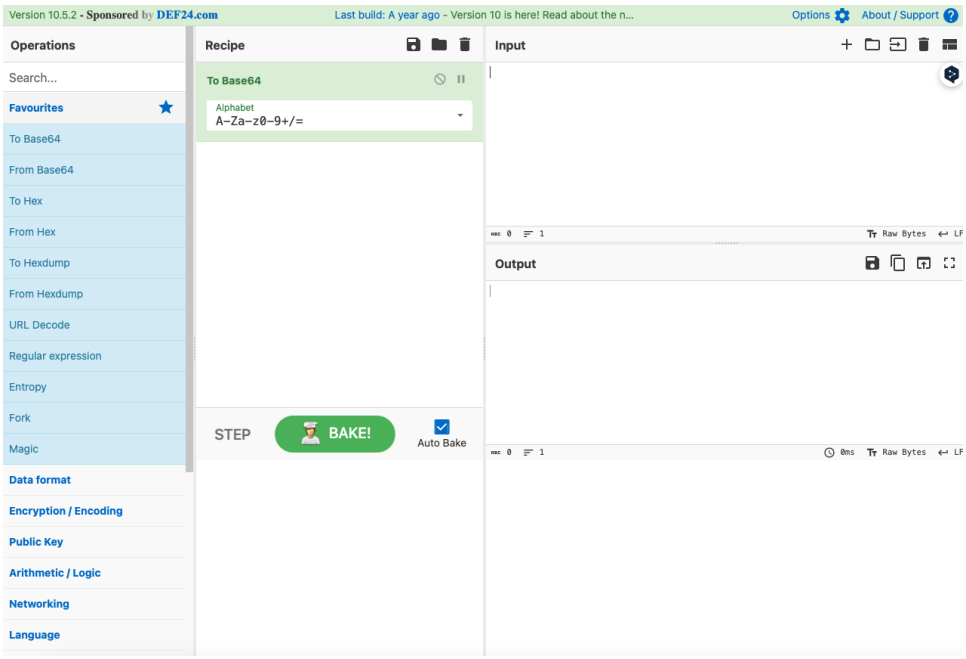
The following exercises are designed to complete with CyberChef.
The goal is to change data format with different operations. We have been given the following hint:



1. What is Base64?

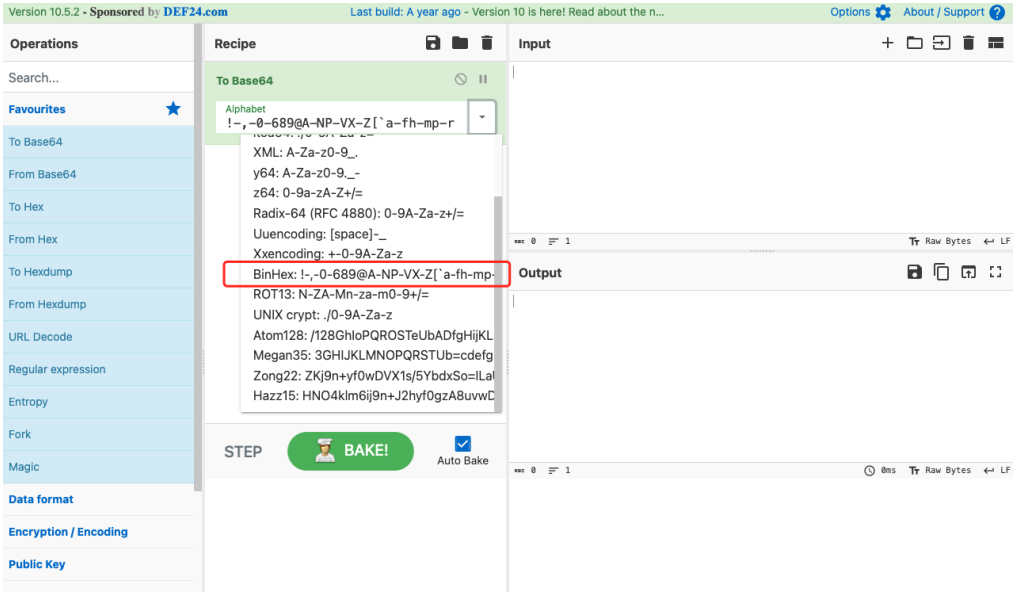
Base64 is a binary-to-text encoding scheme that represents binary data in an ASCII string format by translating it into a radix-64 representation.

2. Choose “To Base64” as the operation method, and type “This is a secret!”. What is the output? （No keep to change the default setting of To Bas64）



VGhpcyBpcyBzZWNyZXQh

3. With the same input, change the Alphabet standard setting to “BinHex”. What is the output?

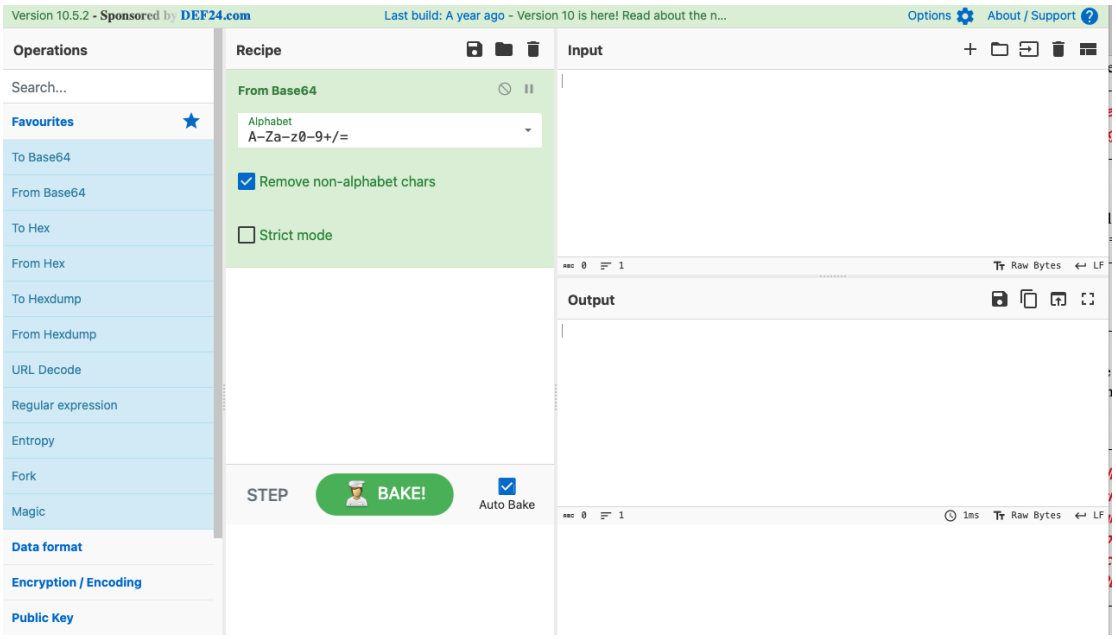


9'KTFb"TFb"cC@0bCA3K

4. Keep the operation and output above, what should we do to recover and output the aforementioned input "This is a secret!" ?

Add the operation "From Base64" and choose "BinHex" as the alphabet parameter.

5. Remove all the operations, choose the "From Base64" operation. Input "aGVsbG8=", what is the output?



hello

6. Change the Alphabet parameter from “Standard” to “URL safe”. Does the output change? Why?

No. "URL safe" is is designed to be safe for use in URLs and other URI (Uniform Resource Identifiers). Standard Base64 encoding includes characters that have special meanings in URLs, such as '+' and '/', which can lead to issues when encoded data is included in a URL. There is no URL in the input.

7. Now you have tried some operations on CyberChef. Can you describe how to use cyberchef?

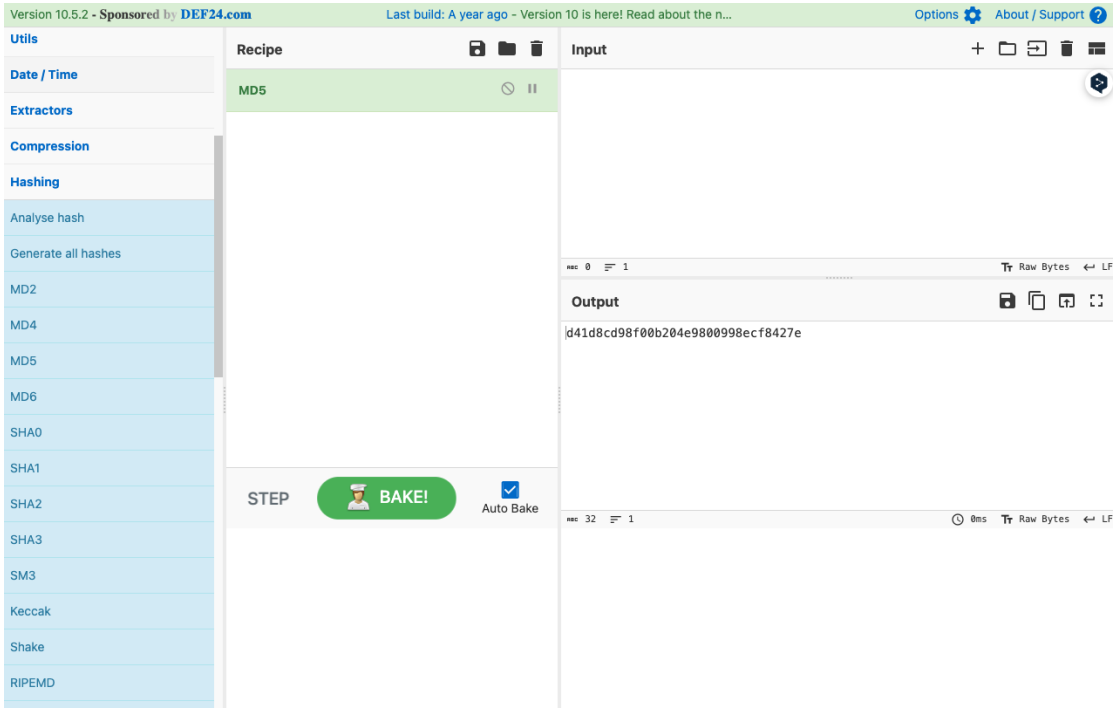
1. Input data by entering it into the "Input" pane on the left side, and use the search bar in the "Operations" pane to find and select the necessary tools by name or category.
2. Drag and drop the chosen operations into the "Recipe" pane to create your sequence of data processing steps, and configure these operations to meet specific requirements such as setting encryption keys.
3. Execute the recipe to automatically process the data and display the output in the right-hand pane, with the option to adjust, add, or remove steps as needed for real-time processing adjustments.

Name: _____ **Student ID:**_____

Part 2: Hashing.

Now that we can review the concept of Hashing, and try some data format operation about hashing on platform CyberChef.

The goal is to have an understanding and some exercises about Hashing using CyberChef.



8. What is Hashing?

Hashing is a process of transforming arbitrary input data (often referred to as a "message") into a fixed-size string of bytes, typically a digest that is unique to each unique input.

9. Choose “MD5” as the Hashing operation, and type “hello world”. What is the output?

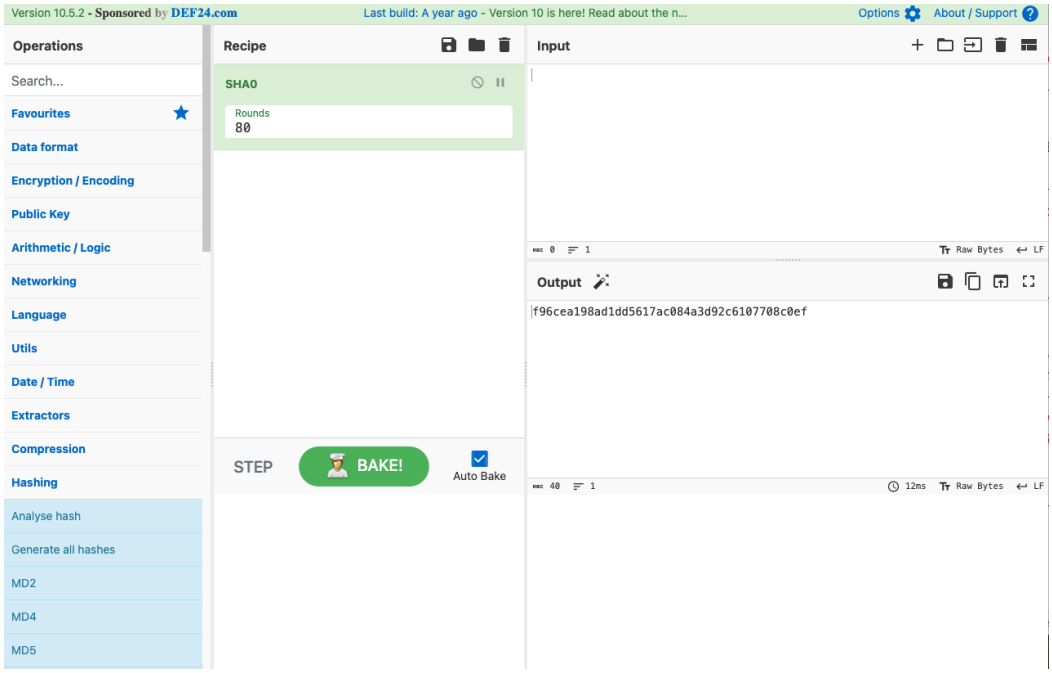
5eb63bbbe01eeed093cb22bb8f5acdc3

Name: _____ **Student ID:**_____

10. Can we recover the output of MD5 hashing?

No. Hash functions are designed to be one-way functions, ensuring that the output does not reveal any information about the input, making it computationally infeasible to reverse-engineer the original data from the hash.

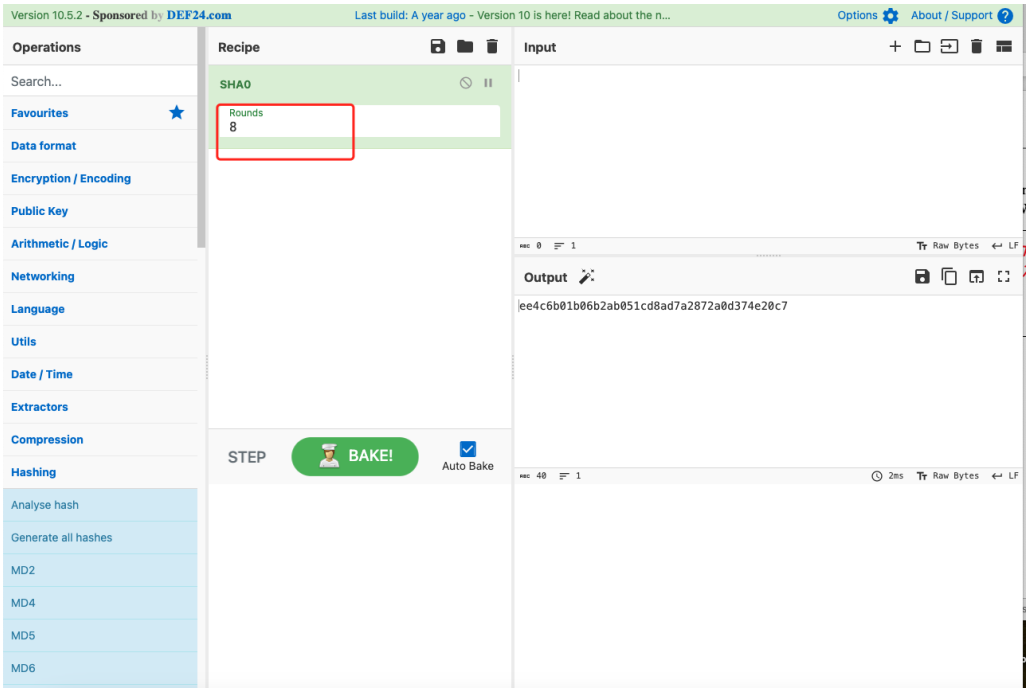
11. Choose "SHA0" as the Hashing operation, and type "hello world". What is the output?



9fce82c34887c1953b40b3a2883e18850c4fa8a6

Name: _____ **Student ID:**_____

12. If we change the “Rounds” parameter from “80” to “8”. Does the output change? What does it output?

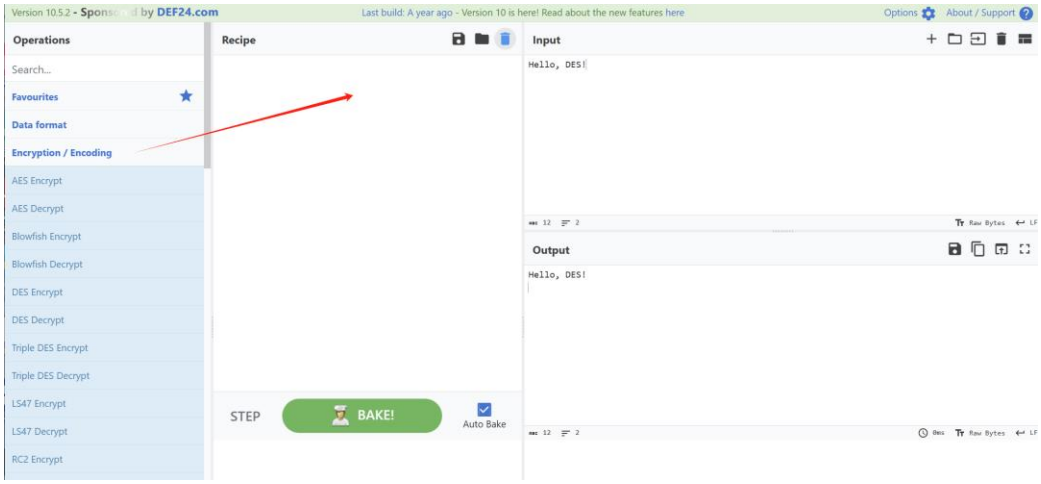


Yes. The output is “e4f674479caaf7ed2a694b51bfbdcd22c86208d0”.

Name: _____ **Student ID:**_____

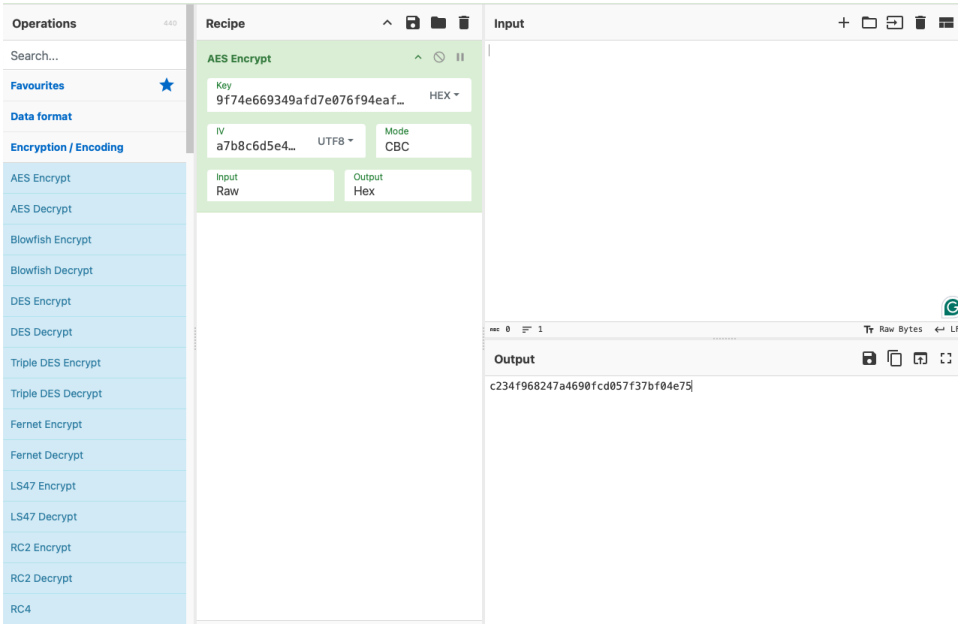
Part 3: Encryption and Decryption.

Now that we can review the concept of Encrption and Decryption, and try some data format operation about hashing on platform CyberChef.



The goal is to have an understanding and some exercises about Encryption and Decryption using CyberChef.

13. Choose "AES Encrypt" as the encryption operation, and type "Hello, welcome to AES encryption!". What is the output? (Hint: the value of Key length and IV length can be set as "9f74e669349afd7e076f94eaf7618d598e3d30c6ee561423dcc5909e44b6ee56" and "a7b8c6d5e4f3021234567890abcdef1")



Name: _____ **Student ID:**_____

8e6ac59e5fe677a7cd2f2b48a20ed1718c6061b44a8f81183212e9cf2a26c09bdab528e26e4ba6c27cbbbfcd6533ce92

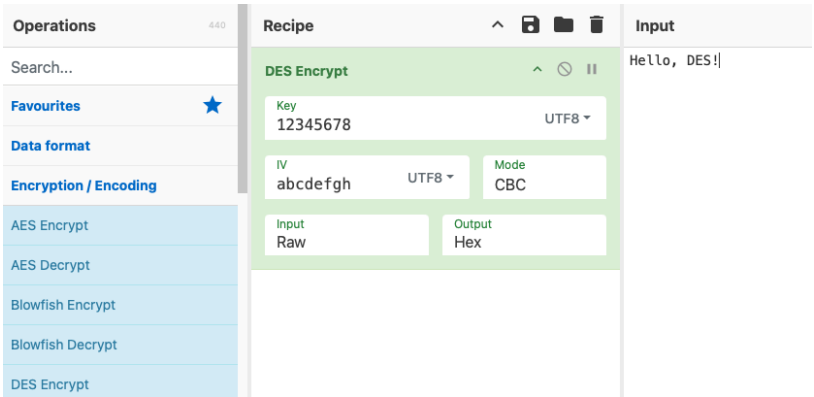
14. Does the output change if we select the type of IV length as "UTF8"?

Yes. The output is "c865e9d5095c1032c6f4a7b29071d082a13c6c8a0f6cc9392a06261bcb83abfe8bd40915866b841ba42f41d13fb924b1"

15. How can we recover from the output?

1.Add the "AES Decrypt" operation.
2.Enter the Key length and the IV length as aforementioned.
3.Change the type of IV length to "UTF8".

16. Choose "DES Encrypt" as the encryption operation, and type "Hello, DES!". What is the output? (Hint: the value of Key length and IV length can be set as "12345678" and "abcdefgh". Both types are set as "UTF8")



00251b5f0276e470721bc679dd546f40

17. Does the output change if we select the type of IV length as "LATIN1"?

NO. Changing the encoding of the IV from UTF8 to LATIN1 will not change the encrypted output, because the byte representation of these ASCII characters is the same in both encodings. This holds true as long as the input characters are within the ASCII range. If non-ASCII characters were involved, then the output could potentially change due to differences in how UTF8 and LATIN1 encode such characters.

18. How can we recover from the output?

1.Add the "DES Decrypt" operation.
2.Enter the Key length and the IV length as aforementioned.