Name: _____ **Student ID:**_____

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

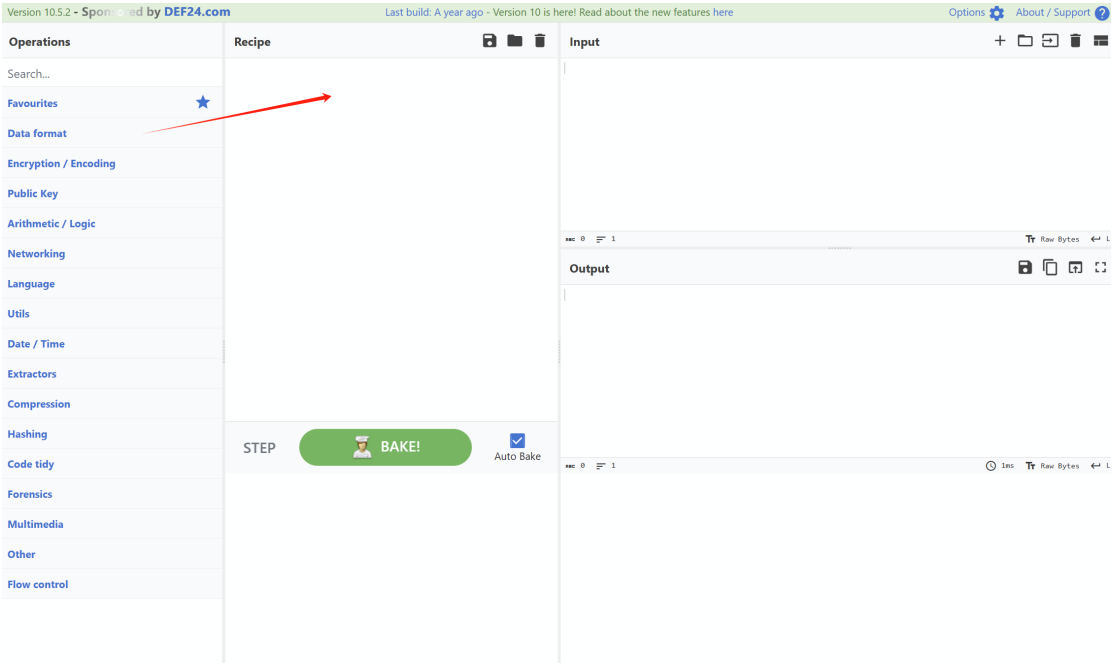
COS30015 IT Security

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:

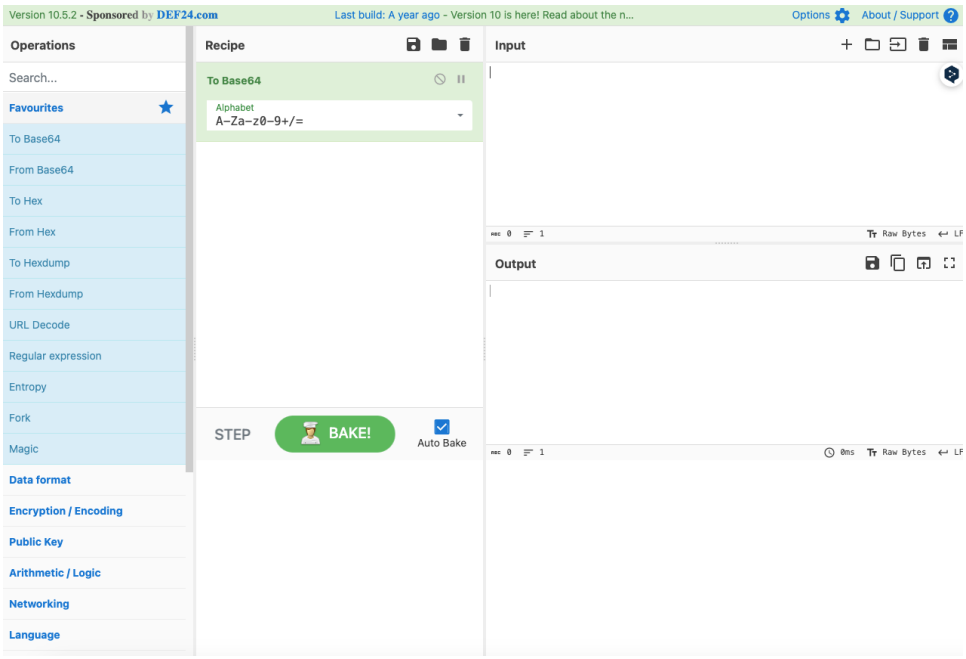


1. What is Base64?

Base64 is a binary-to-text encoding scheme that represents binary data in an ASCII format.

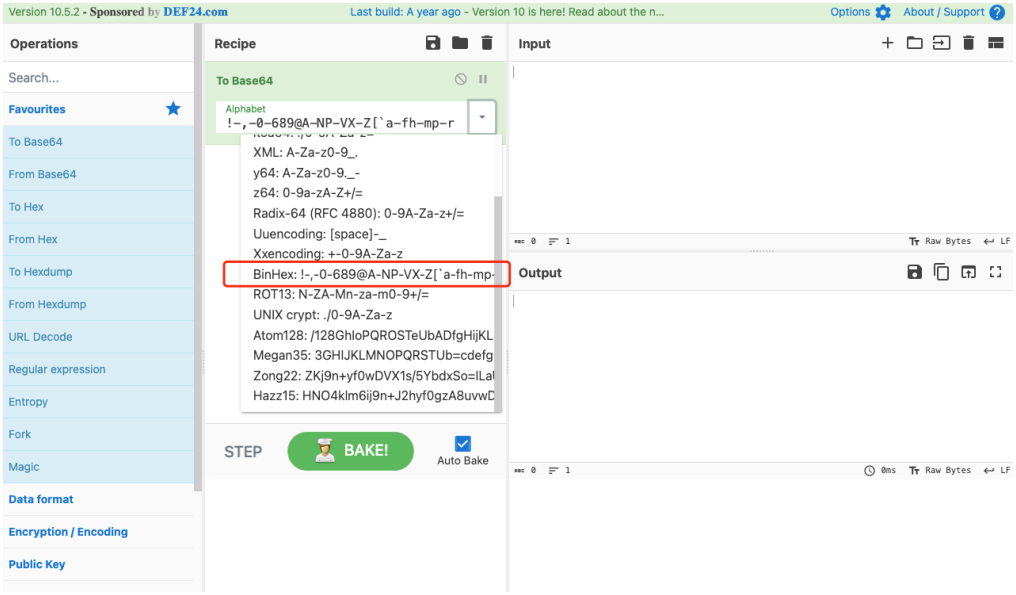
Name: _____ **Student ID:**_____

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）



VGhpcyBpcyBhIHNlY3JldCE=

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

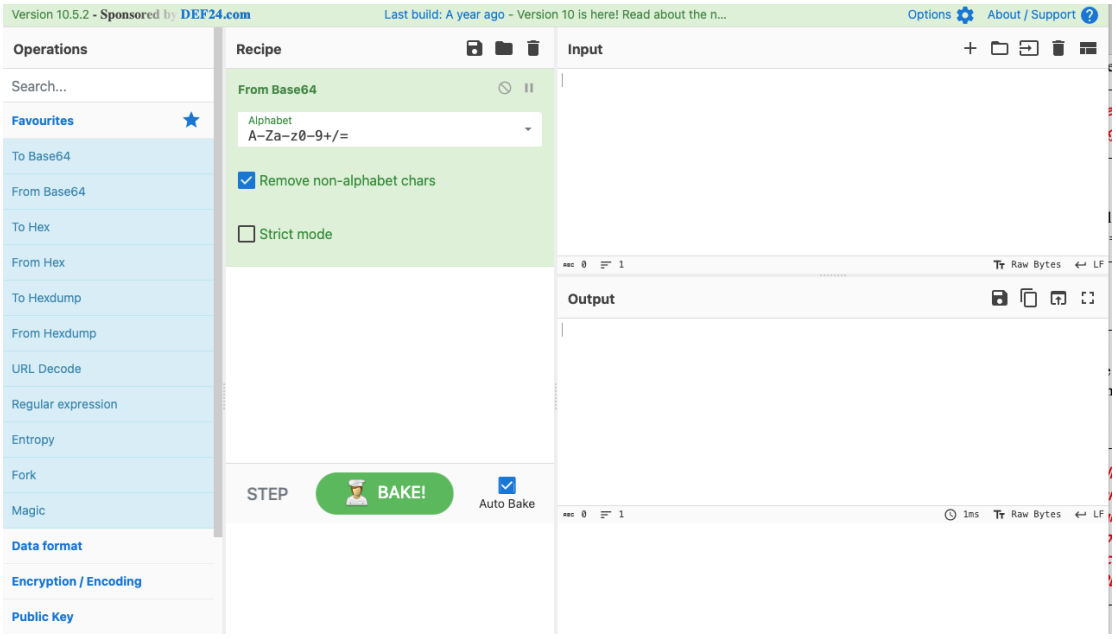


*9'KTFb"TFb"K)(OPBh*PG#%*

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

Change the operation from 'To Base64' to 'From Base64' and then change the alphabet standard setting from standard to BinHex

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, because it's basically the same

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

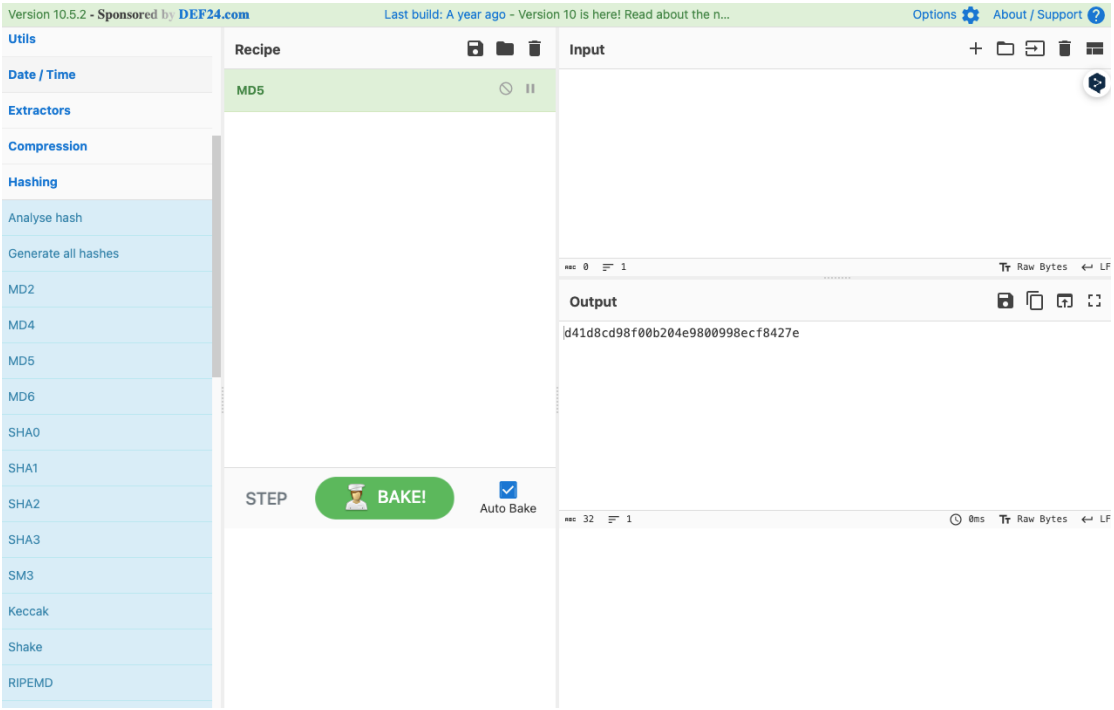
Cyberchef is easy to use, you just pick the operation you want to use and it's pretty much a straightforward approach after that. There's an input field, and an output. You can type in some words or codes based on the operation you chose. It's basically a google translate for machine.

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 input data (such as text, files, or any kind of data) into a fixed-size string of characters, typically a hash code, using a mathematical algorithm.

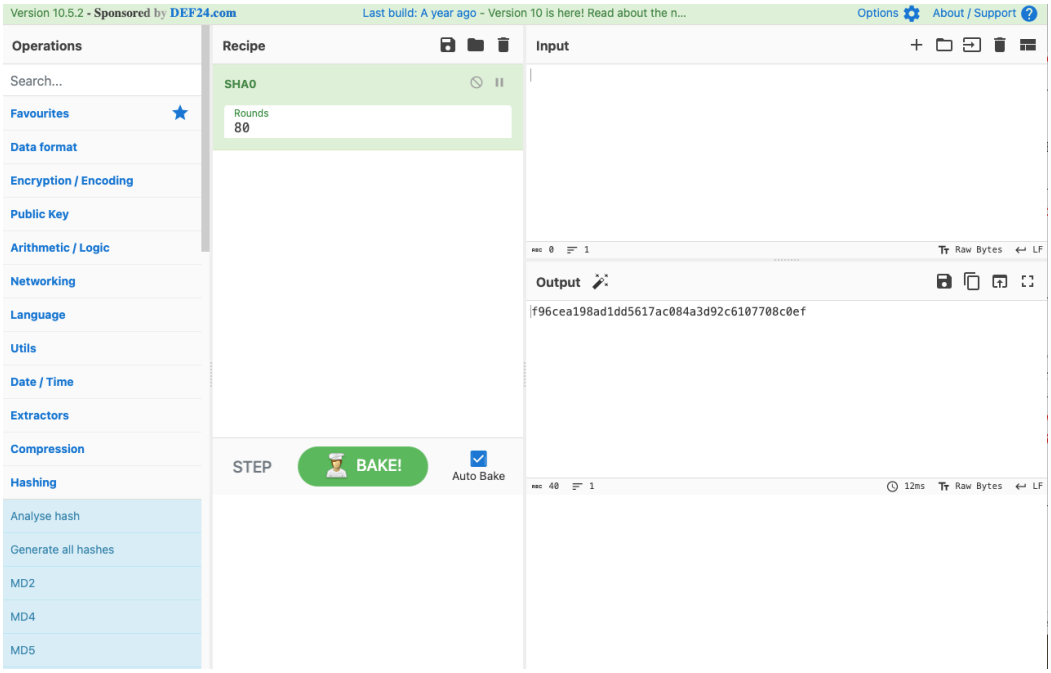
9. Choose "MD5" as the Hashing operation, and type "hello world". What is the output?

5eb63bbbe01eeed093cb22bb8f5acdc3

10. Can we recover the output of MD5 hashing?

MD5 is basically a one-way operation which means it'll be impossible to try and get the original message.

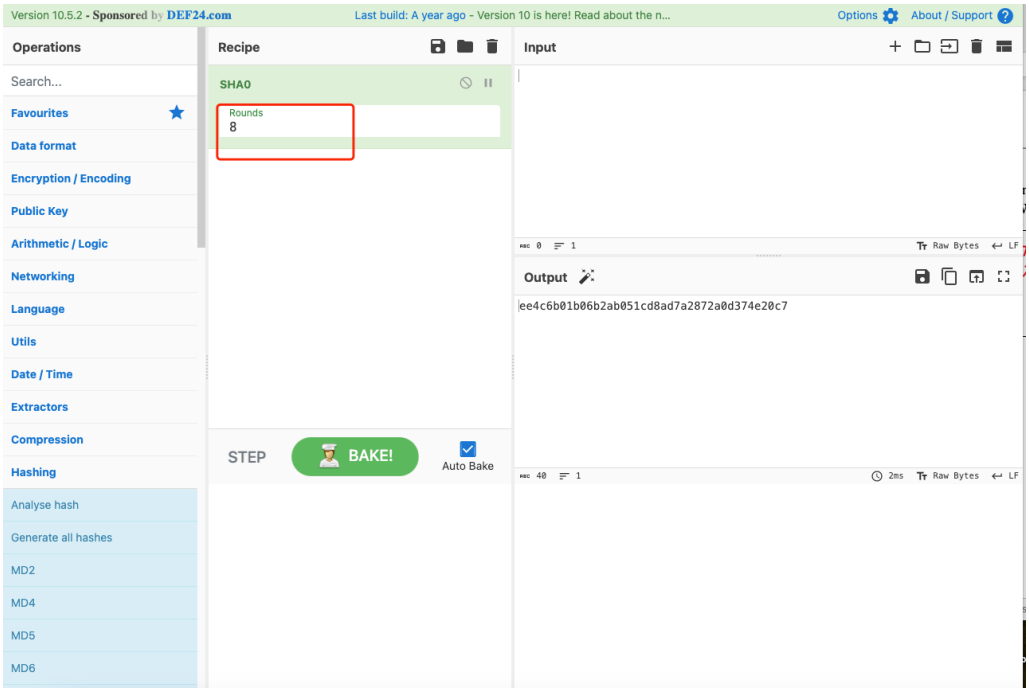
11. Choose "SHA0" as the Hashing operation, and type "hello world". What is the output?



9fce82c34887c1953b40b3a2883e18850c4fa8a6

Name: _____ **Student ID:**_____

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

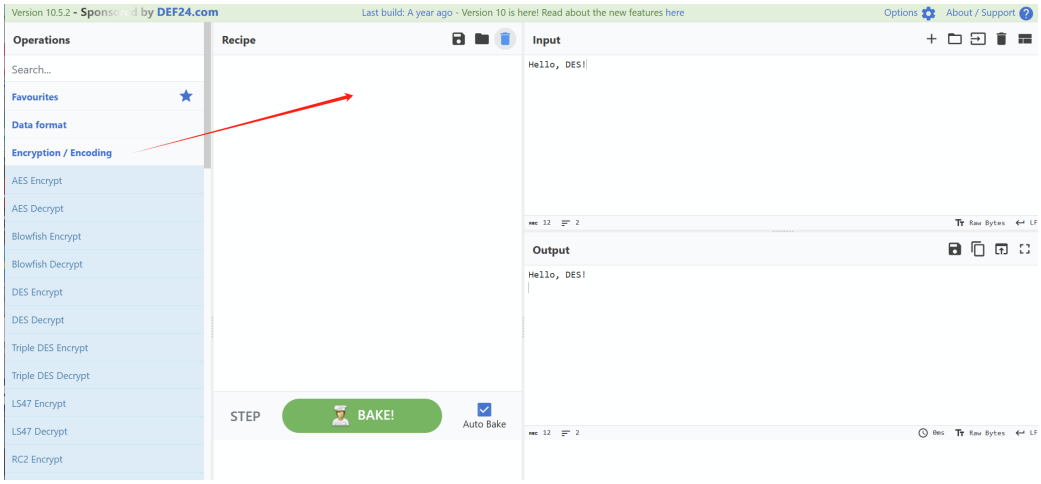


Yes it does,
e4f674479caaf7ed2a694b51bfbdcd22c86208d0

Name: _____ **Student ID:**_____

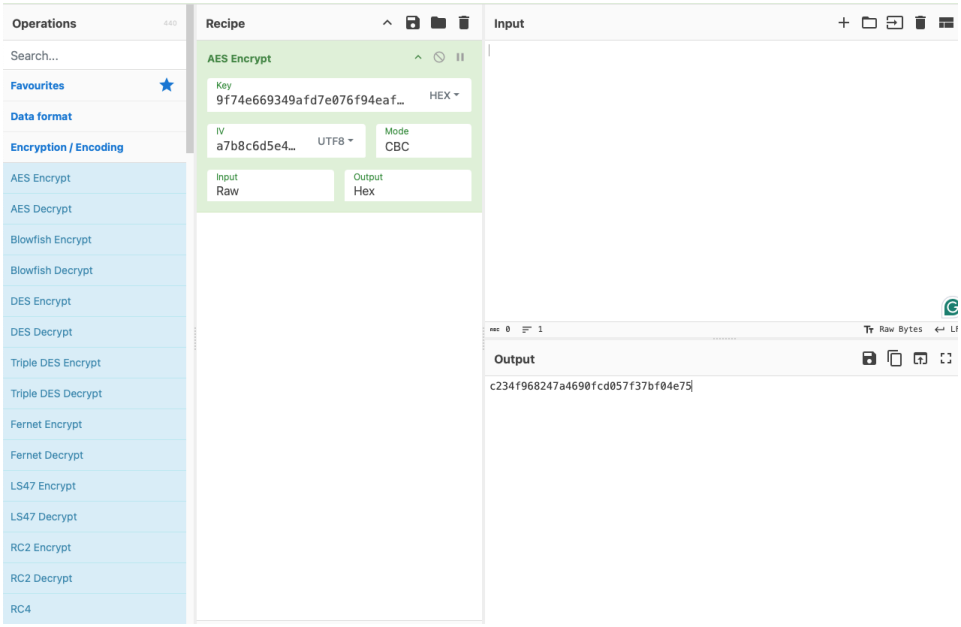
Part 3: Encryption and Decryption.

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")



8e6ac59e5fe677a7cd2f2b48a20ed1718c6061b44a8f81183212e9cf2a26c09bdab528e26e4ba6c27cbbbfcd6533ce92

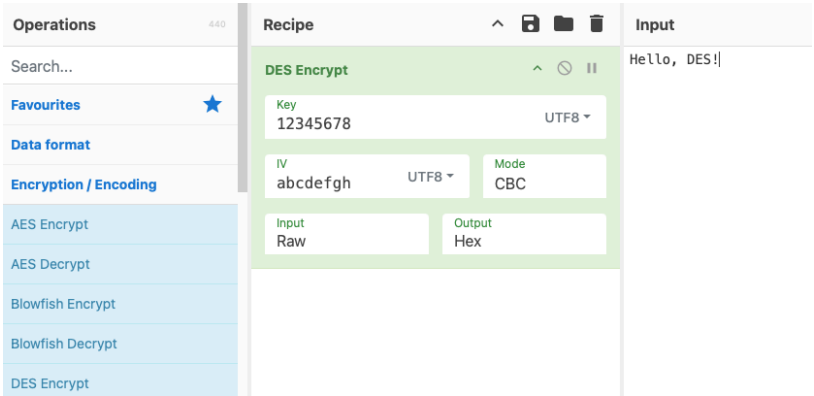
14. Does the output change if we select the type of IV length as "UTF8"?

Yes it does.
c865e9d5095c1032c6f4a7b29071d082a13c6c8a0f6cc9392a06261bcb83abfe8bd40915866b841ba42f41d13fb924b1

15. How can we recover from the output?

Just pick AES Decrypt from the operation

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"?

Nope, because the both present the ASCII character the same way. If there's another character like é, then they would be different.

18. How can we recover from the output?

Same thing like the previous one, just change the operation to decrypt