

Name: \_\_\_\_\_ Student ID: \_\_\_\_\_

## COS30015 IT Security

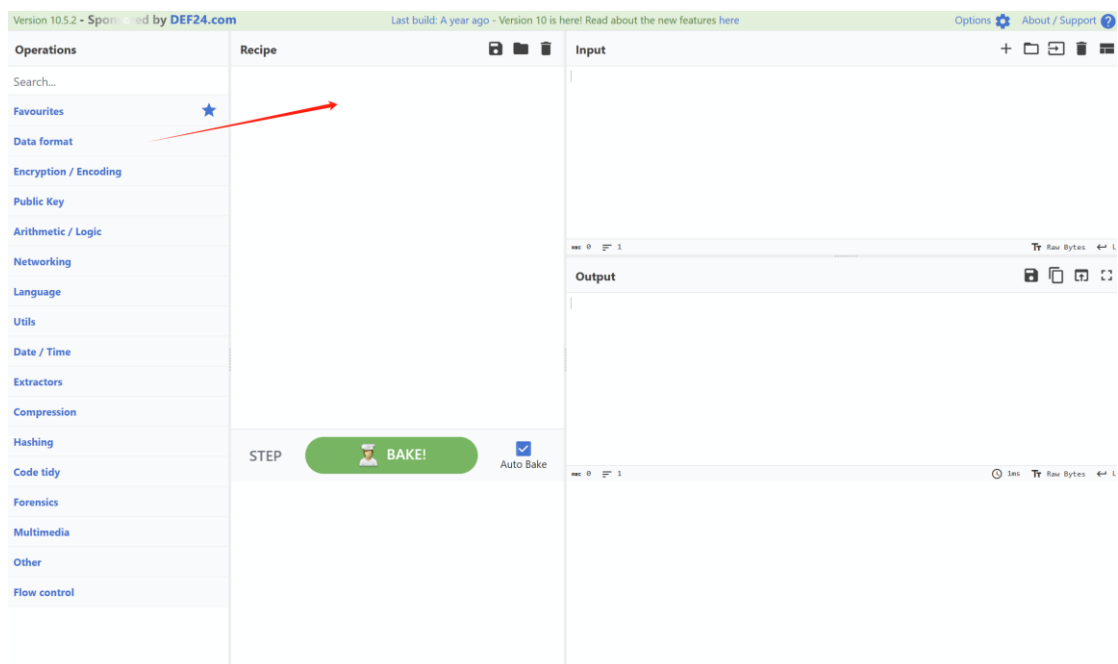
### Lab 8 week 8

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

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

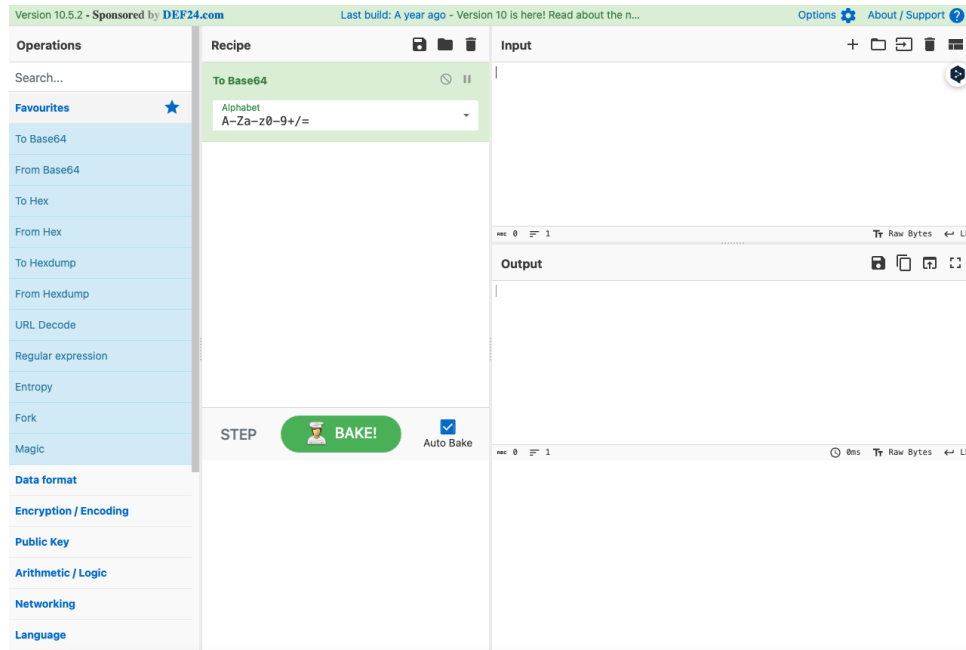
*The following exercises are designed to complete with CyberChef.  
The goal is to change data format with different operations. We have been given the following hint:*



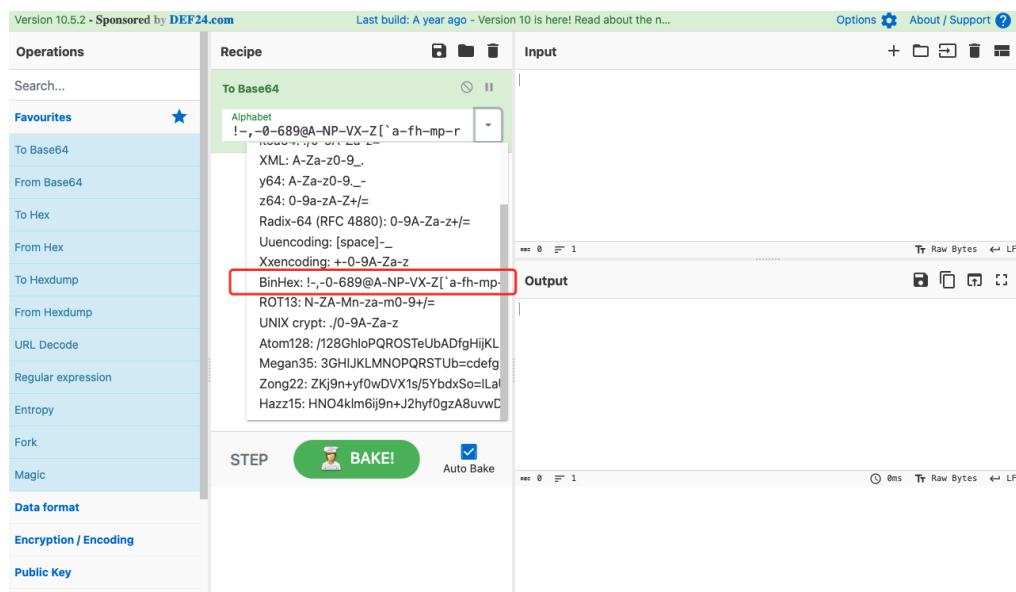
1. What is Base64?

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)



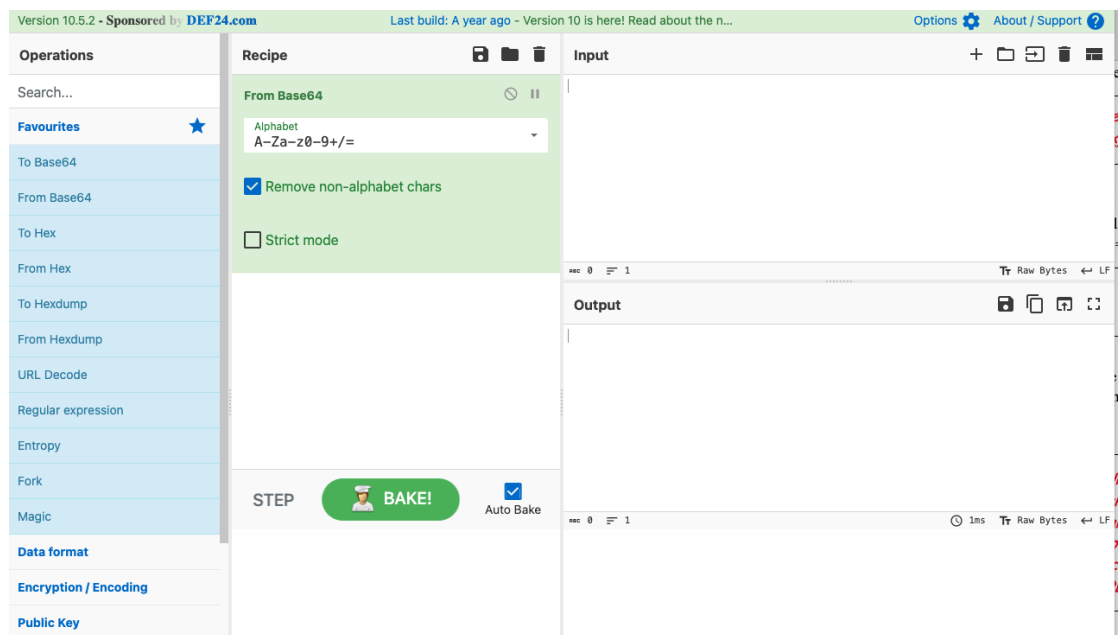
3. With the same input, change the Alphabet standard setting to “BinHex”. What is the output?



Name: \_\_\_\_\_ Student ID: \_\_\_\_\_

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

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



**Name:** \_\_\_\_\_ **Student ID:** \_\_\_\_\_

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



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

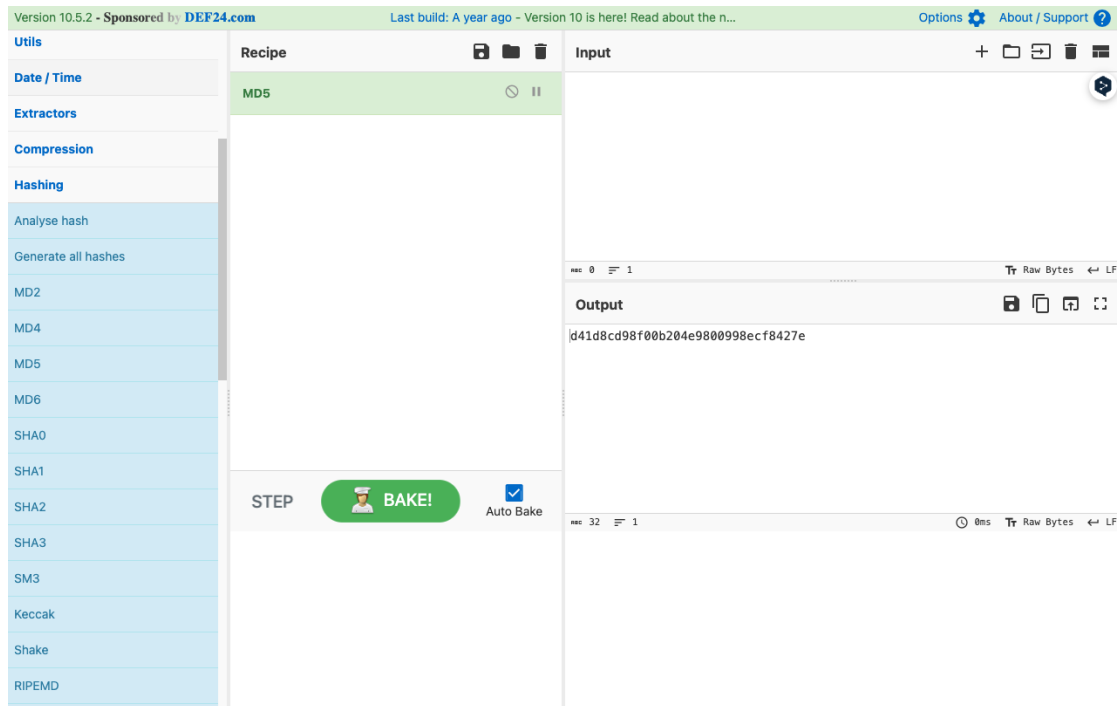


Name: \_\_\_\_\_ Student ID: \_\_\_\_\_

## 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?

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

Name: \_\_\_\_\_ Student ID: \_\_\_\_\_

10. Can we recover the output of MD5 hashing?

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

Version 10.5.2 - Sponsored by DEF24.com

Last build: A year ago - Version 10 is here! Read about the n...

Options About / Support

Operations

Search...

Favourites

Data format

Encryption / Encoding

Public Key

Arithmetic / Logic

Networking

Language

Utils

Date / Time

Extractors

Compression

Hashing

Analyse hash

Generate all hashes

MD2

MD4

MD5

Recipe

SHA0

Rounds  
80

STEP

BAKE!

Auto Bake

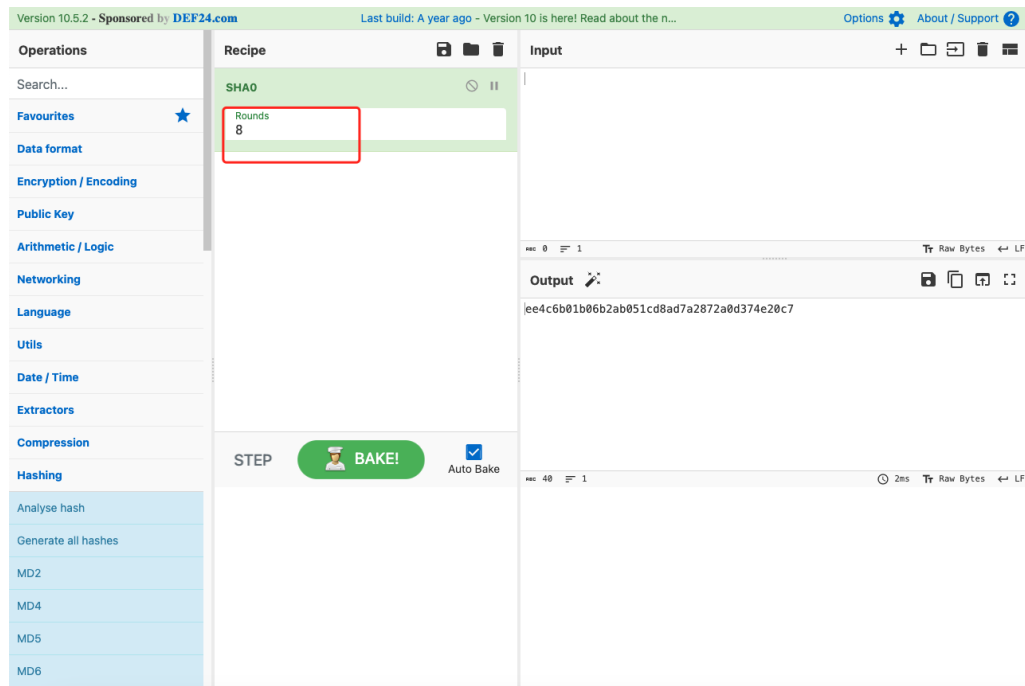
Input

Output

f96cea198ad1dd5617ac084a3d92c6107708c0ef

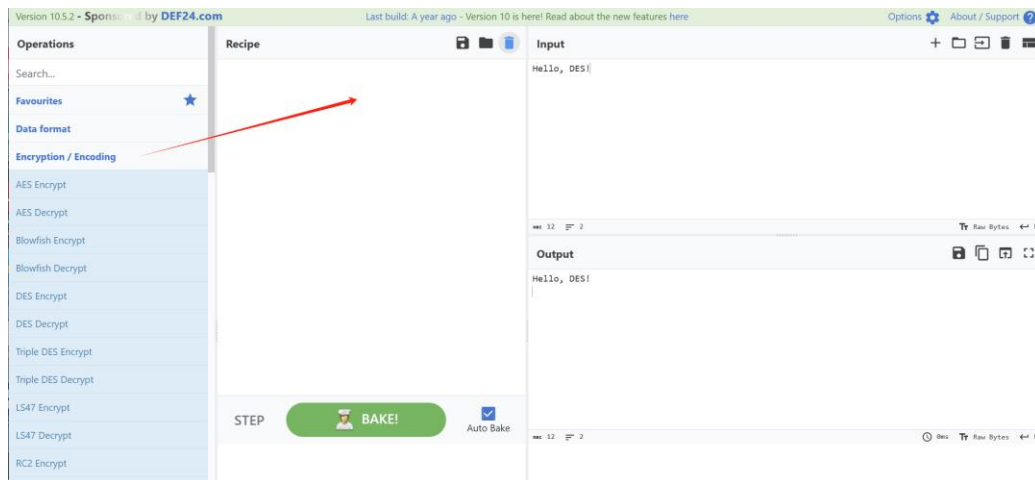
Name: \_\_\_\_\_ Student ID: \_\_\_\_\_

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



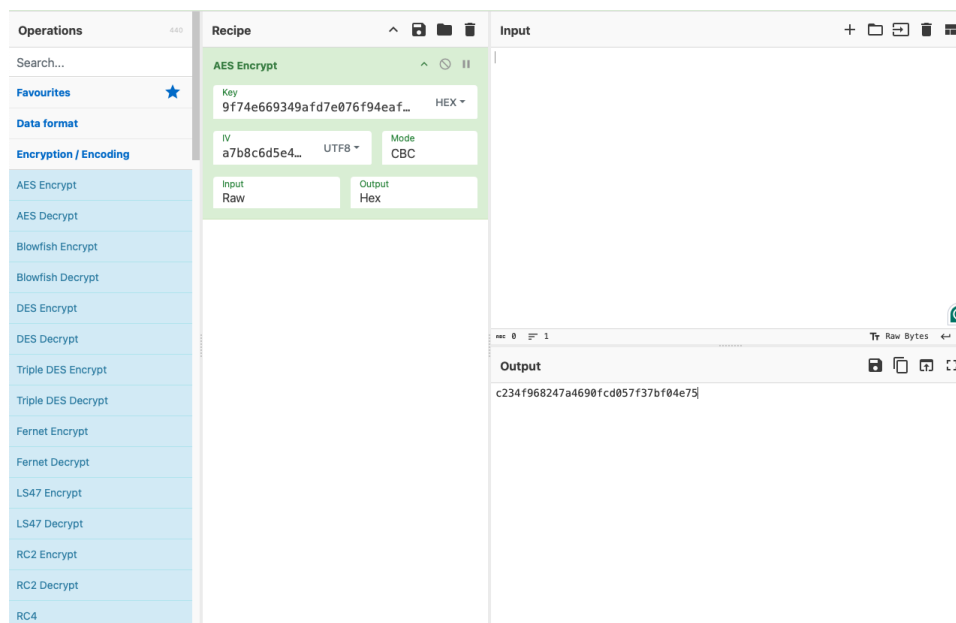
### Part 3: Encryption and Decryption.

Now that we can review the concept of Encryption 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: \_\_\_\_\_

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

15. How can we recover from the output?

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”)

Operations440

Search...

Favourites★

Data format

Encryption / Encoding

AES Encrypt

AES Decrypt

Blowfish Encrypt

Blowfish Decrypt

DES Encrypt

Recipe

DES Encrypt

Key12345678UTF8

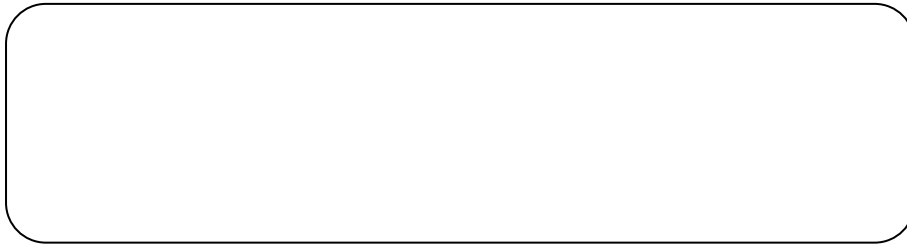
IVabcdefghUTF8ModeCBC

InputRawOutputHex

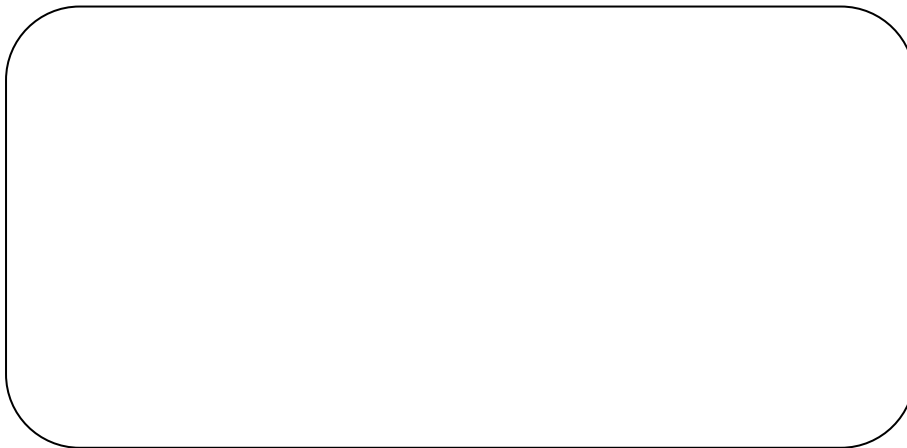
Input

Hello, DES!

**Name:** \_\_\_\_\_ **Student ID:** \_\_\_\_\_



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



**18.** How can we recover from the output?

