### COS30015 IT Security

You will need:

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

### 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:

图形用户界面, 文本, 应用程序

描述已自动生成

1. What is Base64?
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）

**A screenshot of a computer

Description automatically generated**

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

**A screenshot of a computer

Description automatically generated**

1. Keep the operation and output above, what should we do to recover and output the aforementioned input “This is a secret!” ?
2. Remove all the operations, choose the “From Base64” operation. Input “aGVsbG8=”, what is the output?

***A screenshot of a computer

Description automatically generated***

1. Change the Alphabet parameter from “Standard” to “URL safe”. Does the output change? Why?
2. Now you have tried some operations on CyberChef. Can you describe how to use cyberchef?

### 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.**

**A screenshot of a computer

Description automatically generated**

1. What is Hashing?
2. Choose “MD5” as the Hashing operation, and type “hello world”. What is the output?
3. Can we recover the output of MD5 hashing?
4. Choose “SHA0” as the Hashing operation, and type “hello world”. What is the output?

**A screenshot of a computer

Description automatically generated**

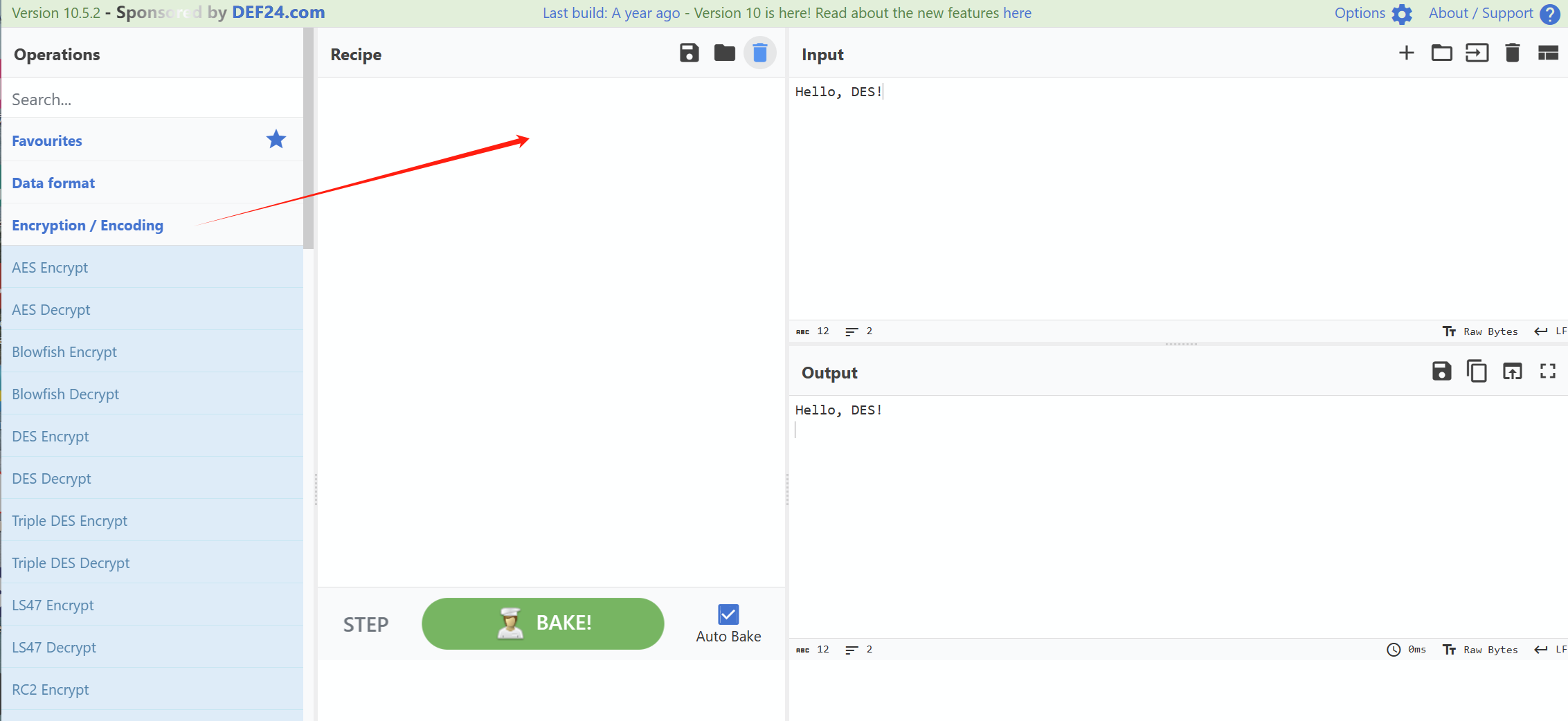
1. If we change the “Rounds” parameter from “80” to “8”. Does the output change? What does it output?

**A screenshot of a computer

Description automatically generated**

### 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.**

1. 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”)

**A screenshot of a computer

Description automatically generated**

1. Does the output change if we select the type of IV length as “UTF8”?
2. How can we recover from the output?
3. 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”)

**A screenshot of a computer

Description automatically generated**

1. Does the output change if we select the type of IV length as “LATIN1”?
2. How can we recover from the output?