Lab 3: HMAC Implementation

Member 1: Member 2: Ahmed Amir

Ruslan X24EC0005

Work in group of 2.

You may try step by step the tutorial **How HMAC Works, Step-by-Step Explanation with Examples** at [https://medium.com/@short\_sparrow/how-hmac-works-step-by-step-explanation-with-examples-](https://medium.com/%40short_sparrow/how-hmac-works-step-by-step-explanation-with-examples-f4aff5efb40e)

[f4aff5efb40e](https://medium.com/%40short_sparrow/how-hmac-works-step-by-step-explanation-with-examples-f4aff5efb40e)

You may also use Cryptool or any other tool to complete the lab. You may mention and put in reference.

# Part A

*Member 1:*

1. Perform HMAC of your full name with UTM matric (message 1) using SHA-512, step-by step. Show your work.
2. Send message 1 and HMAC to Member 2.
3. Alter 1 bit of the message(message 2a), send to Member 2

Изображение выглядит как текст, снимок экрана, Шрифт, число

Контент, сгенерированный ИИ, может содержать ошибки.

*Member 2:*

1. Perform HMAC of your full name with UTM matric (message 2) using MD5, step by step show your work.
2. Send message 2 and HMAC to Member 2.
3. Alter 1 bit of the message (message 2a), send to Member 2.

# Part B

Member 1:

Generate HMAC for message 2 and message 2a, compare with the HMAC send by member 2. Analyse the results.

Show all your work step by step.

Member 2:

Generate HMAC for message 1 and message 1a, compare with the HMAC send by member 2. Analyse the results.

Show all your work step by step.