Raymond Ng

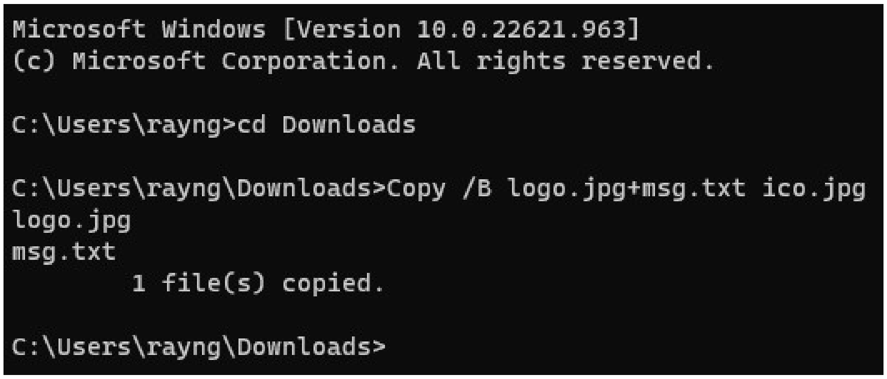
IS 3423 – Network Security

Lab 1: Cryptography

February 8th, 2023

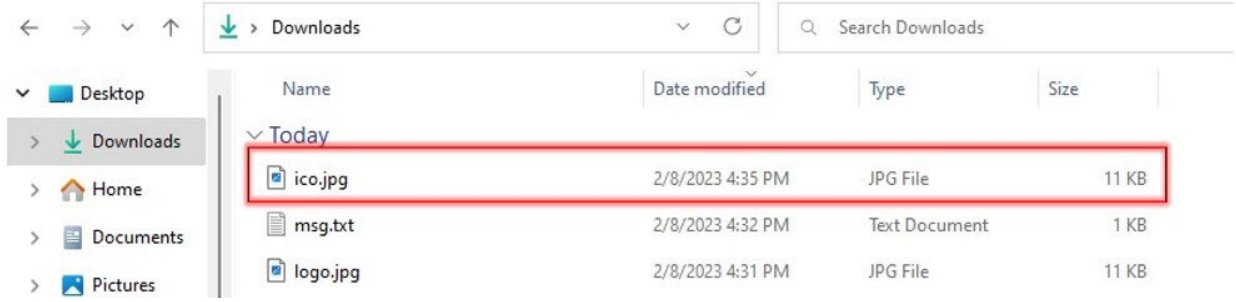
Part A: Steganography

In command prompt, executed `Copy logo.jpg+msg.txt ico.jpg`.



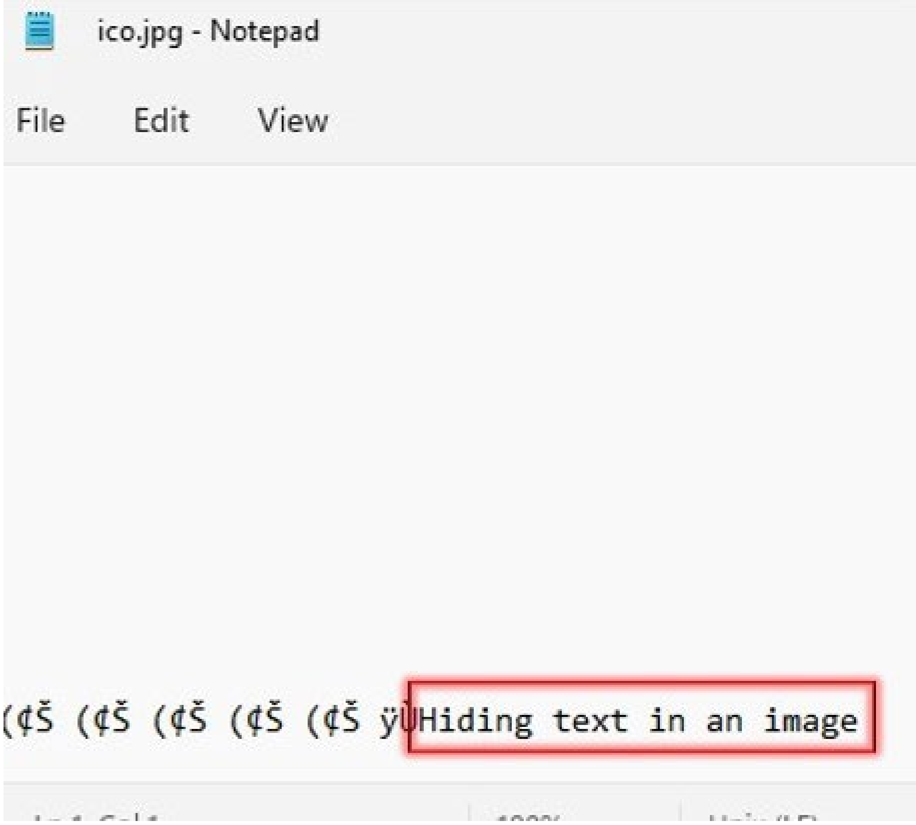
```
Microsoft Windows [Version 10.0.22621.963]
(c) Microsoft Corporation. All rights reserved.

C:\Users\rayng>cd Downloads

C:\Users\rayng\Downloads>Copy /B logo.jpg+msg.txt ico.jpg
logo.jpg
msg.txt
        1 file(s) copied.

C:\Users\rayng\Downloads>
```

`ico.jpg` is created in Downloads folder.



Name	Date modified	Type	Size
ico.jpg	2/8/2023 4:35 PM	JPG File	11 KB
msg.txt	2/8/2023 4:32 PM	Text Document	1 KB
logo.jpg	2/8/2023 4:31 PM	JPG File	11 KB

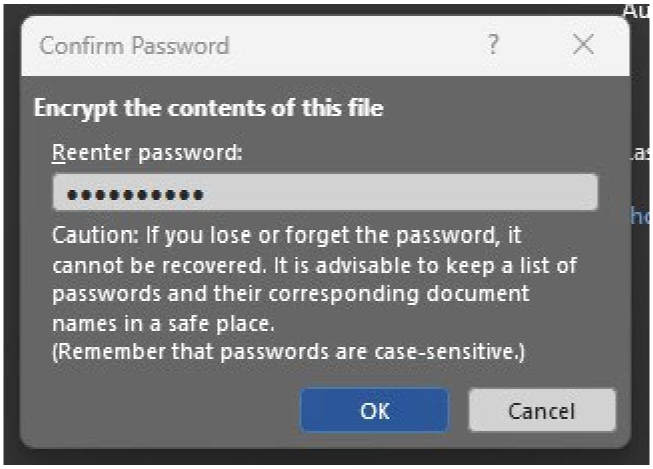
Text hidden in image depicting via Notepad.



```
(¢Š (¢Š (¢Š (¢Š (¢Š ÿÙHiding text in an image
```

Part B: Encryption for data at rest

Opened a new MSWord document. Selected File, then Info and selected Protect Document. Selected Encrypt with Password. Entered a case-sensitive password. Verified it by typing it again (snap shot below).

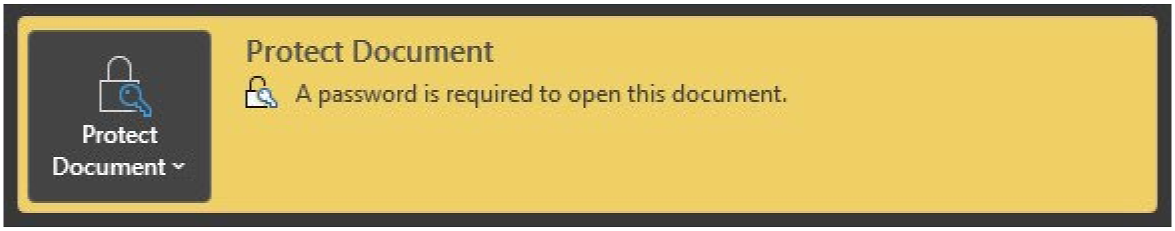


Encrypt the contents of this file

Reenter password: ●●●●●●●●●●●

Caution: If you lose or forget the password, it cannot be recovered. It is advisable to keep a list of passwords and their corresponding document names in a safe place.
(Remember that passwords are case-sensitive.)

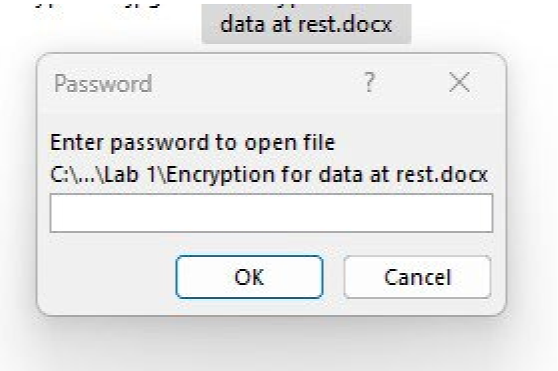
MSWord confirmed document is protected with a password.



Protect Document

A password is required to open this document.

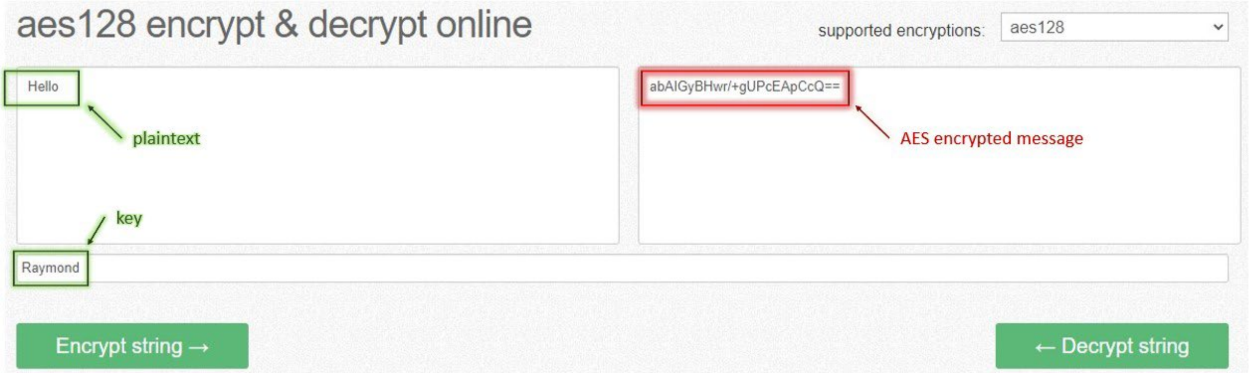
Reopened the file, prompted for the password.



Enter password to open file
C:\...\Lab 1\Encryption for data at rest.docx

Part C: Encryption for data in motion

Encrypted plaintext “`Hello`” with key `Raymond` using AES encryption via `https://encode-decode.com/aes128-encrypt-online/`.

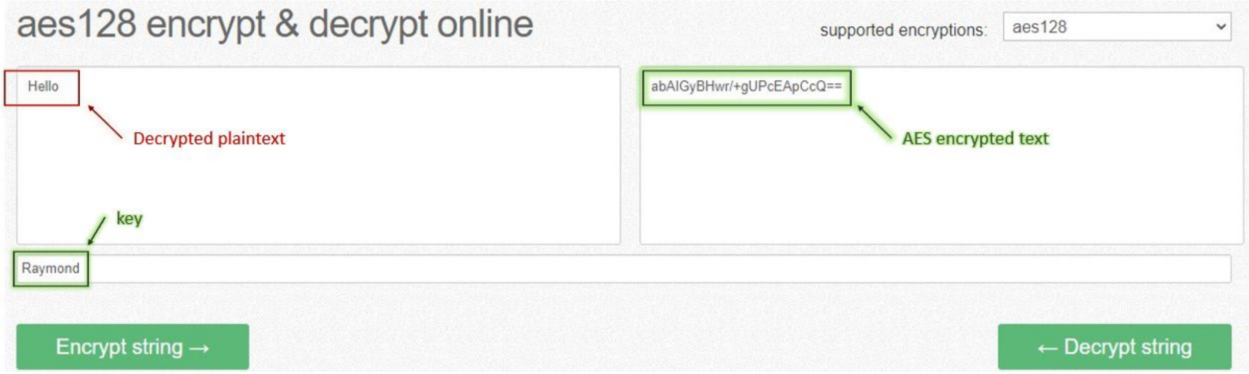


Hello

Raymond

abAIGyBHwr/+gUPcEApCcQ==

Decrypted `abAIGyBHwr/+gUPcEApCcQ==` with key `Raymond` via `https://encode-decode.com/aes128-encrypt-online/`.



aes128 encrypt & decrypt online

supported encryptions: aes128

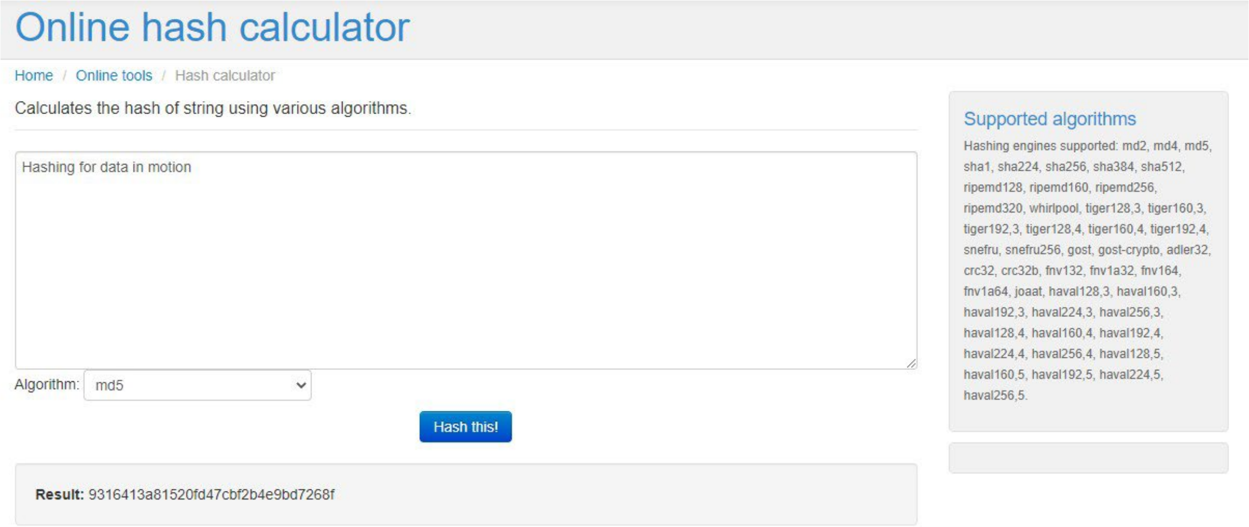
Hello

abAIGyBHwr/+gUPcEApCcQ==

Raymond

Part D: Hashing for data in motion

Using online hash calculator via https://www.toolsnoobs.com/online_tools/hash/ and md5 algorithm, hashed the challenge message, `Hashing for data in motion`. Produced `9316413a81520fd47cbf2b4e9bd7268f`.



Online hash calculator

Home / Online tools / Hash calculator

Calculates the hash of string using various algorithms.

Hashing for data in motion

Algorithm: md5

Result: 9316413a81520fd47cbf2b4e9bd7268f

Supported algorithms

Hashing engines supported: md2, md4, md5, sha1, sha224, sha256, sha384, sha512, ripemd128, ripemd160, ripemd256, ripemd320, whirlpool, tiger128,3, tiger160,3, tiger192,3, tiger128,4, tiger160,4, tiger192,4, snefru, snefru256, gost, gost-crypto, adler32, crc32, crc32b, fnv132, fnv1a32, fnv164, fnv1a64, joaat, haval128,3, haval160,3, haval192,3, haval224,3, haval256,3, haval128,4, haval160,4, haval192,4, haval224,4, haval256,4, haval128,5, haval160,5, haval192,5, haval224,5, haval256,5.