Part-1 Project

Each group will submit a short proposal (1 page) including title of selected cryptographic algorithm and its short description along with group member information at the end of 8th week. The group can start work on the implementation of selected cryptographic algorithm upon its approval from the instructor. The project code will be submitted by each group for its review and demonstration in 9th week.

Project rubrics:

Following are the project rubrics.

Deliverable	Rubrics	Marks	Obtained Marks	Comments
Proposal	Group formation	1		
	Selection of crypto algo. & its description	2		
	Selection of presentation topic and its selection reason	2		
Code review & demo	Code review	3		
	Demonstration	2		
	Total	**10**		

Part-1 Project

Project Proposal

1. Group formation

#	ID	Name
1	2036023	Abdulaziz Adnan Alsharif
2	2037276	Rakan Adnan Salama
3	2040569	Omar Saeed Alzahrani
4	1743998	Fahad Hamad Alsifri
5	2037675	Nasser Abdulrahman Alharbi
6	1937615	Sultan Fahad Alshammari

2. Selection of crypto algo. & its description

Selection of crypto algo:

Triple DES

Description:

Triple DES performs encryption and decryption symmetrically using two or three keys. It extends the original DES algorithm. Triple DES triples the encryption process by implementing three different keys. This tripartite method greatly supports security, making it hard for attackers to unravel the encrypted data. The procedure entails an initial encryption, followed by a decryption, and ultimately a final encryption. This functions as a protective measure, even if the initial encryption is compromised. There are many reasons makes DES is a good choice for encryption and decryption. DES offers simplicity in its straightforward and easy-to-implement encryption algorithm, which reduces the hardware and software resources needed for encryption and decryption, making it efficient and cost-effective in terms of both processing power and development time. Its use of a 56-bit key can be advantageous for computational efficiency, requiring fewer computational operations. Additionally, DES has seen significant hardware optimizations developed over the years, allowing for faster encryption and decryption in dedicated hardware. This makes it cost-effective for hardware implementations. Furthermore, in some legacy systems or scenarios where backward compatibility is essential, DES remains in use due to its long-standing hardware and software support, which makes it relatively inexpensive to maintain and operate in these specific cases.

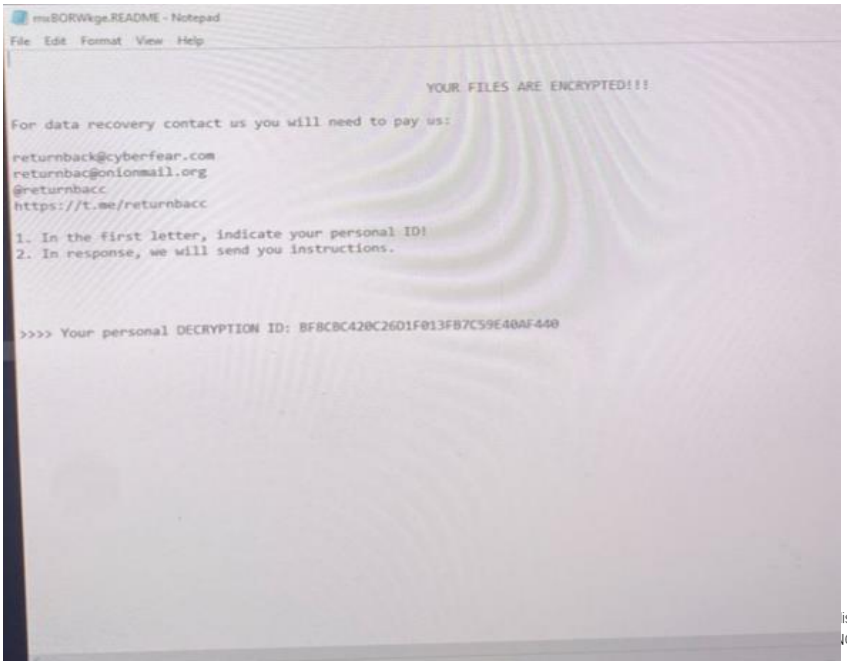
3. Selection of presentation topic and its selection reason

Presentation topic:

Awareness of remote desktop protocol (RDP) hacking and Blackmail

Selection reason:

Our reason for selecting this topic stems from a recent incident within our team (Abdulaziz). Not long ago, Abdulaziz experienced a cyberattack through the Remote Desktop Protocol. In this unfortunate breach, unauthorized individuals accessed Abdulaziz's system and encrypted a significant amount of data, totaling 6 terabytes. The hackers left a message on the desktop, notifying Abulaziz of the breach and the encryption of all files. To regain access to these crucial files, Abdulaziz was instructed to contact the hackers through email. Subsequently, the hackers demanded a ransom of $6,000 in Bitcoin for the decryption key and decryption of the files. The primary cause of this security breach was the exposure of the remote desktop protocol without password protection on PC and the necessary means of protection.



:Hello. To decrypt files, follow these instructions

.Price .1
.for decrypting all your files, or for part of your files, the price is the same (american dollars) $ 6000
We accept only BITCOIN payments. (It is a decentralized digital currency)

.Be careful please .2
.Do not change the encrypted file extension
.Do not try to decrypt your files with programs from the internet, these programs don't work
.If you decide to try any decryption programs, please make a copy of the encrypted files before doing so
.Only our email has the keys to decrypt your files. Do not believe other people

Test decryption as a guarantee .3
.We will decrypt 1 any, not important file, as proof of decryption
,File for test no more than 1 megabyte (not archived). If in our opinion you send an important file
.we have the right to refuse to decrypt it and ask you to send another file

:Decryption process .4
:We are waiting for payment to our Bitcoin wallet. As soon as we receive the money we will send you
.a) Program for decryption
.b) Instructions for decrypting and securing your computer

:Websites where you can buy bitcoins .5
www.bitpapa.com
www.coinmama.com
www.paxful.com
www.localbitcoins.com
www.abra.com

ist of websites https://www.wikijob.co.uk/content/trading/cryptocurrency/places-to-buy-bitcoin#20-local-bitcoins
NOT USE COINBASE! Because through COINBASE you can send them only after two weeks of authorization
/Websites for CHINA: https://www.huobi.io/ https://bitpay.com