TASK:1 **Do you think encryption is a valuable cybersecurity tool? Why or why not?**

Ans. Encryption is a critical cybersecurity technique for safeguarding sensitive data and communications in our digital age. It protects privacy by transforming data into unreadable ciphertext, even if unwanted parties have access. Encryption also protects data by detecting illegal alterations. It restricts access so that only authorized entities can view data. Encryption is required to comply with data protection requirements such as GDPR and HIPAA. While not impenetrable, it is an essential component of a complete cybersecurity plan that adapts to emerging cyber threats. The function of encryption in protecting digital assets and ensuring compliance will continue to increase in prominence.

A screenshot of a computer

Description automatically generated

* Encrypt this file by using the following command in Kali:

openssl enc -aes-256-cbc -in yourFirstName.txt -out encrypted1.bin

Provide any password when required.

Take a screenshot of the command used and its result and include it as part of your submission.

A screenshot of a computer screen

Description automatically generated

* Issue the command cat{yourFirstName}.txt to show the plain-text contents of this file. Take a screenshot of this from Kali and include it in your MS Word document. Also, copy and paste the contents of this file in your MS Word document.

Salted\_\_ Ew V`T \ ү3hi fP T6Jo;+3ͽ Һ FI M ?I '{ ? 5|r

YM VD H S ڇ 0( %B PDnI Pi 5] .` + l Y Rp :z ▒ Y Q ō7 zlς #h Q gami Xo& q K O G V( +^ V 9 ċ }y\9{& 9 "p Lп VՀ P ~tf y 2: ܢ 3 3+<▒ 9 k!t ݟØj

ə ț 'x YmA( u

y E a ; y D Xm E ʲl H kH.C / O\78i gY8 & Z[L 5▒ C ә 'P bzYx] !A a[9% D qþ1 2m# } C 0 = LR8 +^67

orOHlm

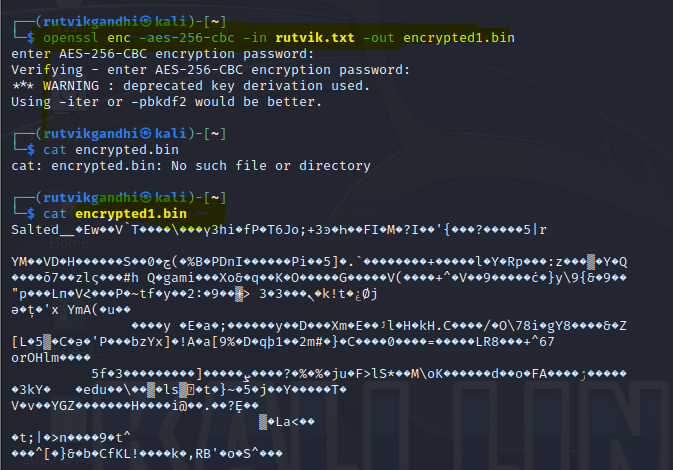
5f ܨ [ 3 ? % % ju F>lS\* M\oK d o FA ڙ 3kY edu \ ▒ ls▒೰ t }~ 5 j Y T

V v YGZ H i@ . ?Ȩ

▒ La<

t;| >n 9 t^

^[ }& b CfKL! k ,RB' o S^



* Repeat the encryption but this time, include the -base64 option as follows:

openssl enc -aes-256-cbc -in yourFirstName.txt -out encrypted2.bin –base64

Take a screenshot of the command used and its result and include it as part of your submission.

A screenshot of a computer screen

Description automatically generated

* Repeat the cat encrypted.bin command after the above command has executed. Take a screenshot of this output and include it in your report. Also, copy and paste the contents of this file into your MS Word document.

U2FsdGVkX1/kbl4HvfjLHf6caBSf8Rkl+q6k5XUr7xeM3pB6jDCf32uWmcSwHyMT

H6JhX6rIqvh2VfrTcxtfVGC051KiIq2+h3SN2uqF6I22Mnv1icocmrgs7XkvK/Om

tWXCH3S2hMnRBL8BhN48xi0Vdx0loZts3F9/4Sm3P+d3dh6sxLr/L09+y/toj0fA

OvIYpk39+18YpOHZ6xPMrJpnEtxXhXpvKWOpTY65hdKPIYWDp4poqQ3h3H5aTVCb

J/DQ1AQ4TxY9rJfvZg68pac0DJ5x/oYt/d5YXBoBkkiHOAuTjD6qwwddOGE3WUEn

wutLmuROGYUcFBQW11rwzQavr5eXvTIDW+Nh4AKbo9wfZgXu40CDrWyg7iXjIzSp

EJyMEiH1saGNPJDJ5VEC/xaHMY0KWYo6CUzF11S1E2+qvGLeNojTE2Dz802Z+Qt5

scYB3RguITEh/o2HtqhAoKIaBV4PCcWo2oBBjKXbqWj/S5CnilDrngkkSWNkGI0U

6gaHhvco9/khruOf9rypn9OxBHfSp+HKXfD4H4UHb/k8yDqFY2nDKGs/hIm3sKEu

Fi4B6vISA1dKq+GKWUCqNgdtCb7Kd39auhV9TDtyIZJ4t0Kkc1xHBu12f9bHjeGt

NyoNXwffMCz19Cjpcg0miJvBWxKusSLCNDlbVQ4AQFuPc2zBsJv6ELcSSnOT6OsG

DHZCHqEqUZ7cFQALw7u1stblFiO01MgMERvtCbJdoGrUzF21uupeN8yIvp7WMwmQ

n9s7Ofd9EFUKLr1uuAHzaFWdlaZjqoYz5K4jZ/sdfrLBDXpB3onNJYKtQytMYr1H

DS+sV6pSWjXqxk/CmVkcXwtrx46dD1hBpA9q6f9DIlrJabgQ7JMw5gDwJUyhaAFs

vePbKawgqmRmwvu7Ta3mmAUJhfLKtEMJhp2D7ANpj/lxFGQIqJy9Z+58QZKSqUKx

2LWaEE2SGWQnW3qDXEv8GHf3l6j/rhydtSJgcJuVfLM7UTebwW4MYK3zfysSkn/h

F2VpN15pWJN6XWuJnXFTfB3++pu6SUPc6yWH+5wIHorKn3GRTZXR7ytiTUby1ECf

Dmp+PtwsnCK0eSAmsmy6lHP3G7qIXeCaL+yF4LAa0zv1WFZURdcr7ILJIKSoVjtp

IMMytfHLp09OfLcJIFnHpA==

A screenshot of a computer

Description automatically generated

* Using the appropriate command option within the openssl tool, perform a decryption of your encrypted.bin file. Take a screenshot that shows the command being used as well as the output and include it in your report. Also, copy and paste the contents of this file into your MS Word document.

1) Do you think encryption is a valuable cybersecurity too? why or why not?

Ans. Encryption is a critical cybersecurity technique for safegurading sensitive data and communications

in our digital age. It protects privacy by transforming data into unreadable ciphertext, even if

unwanted parties have access. Encryption also protects data by detecting illegal alterations. it

restricts access so that only authorised entities can view data. Encryption is required to comply with

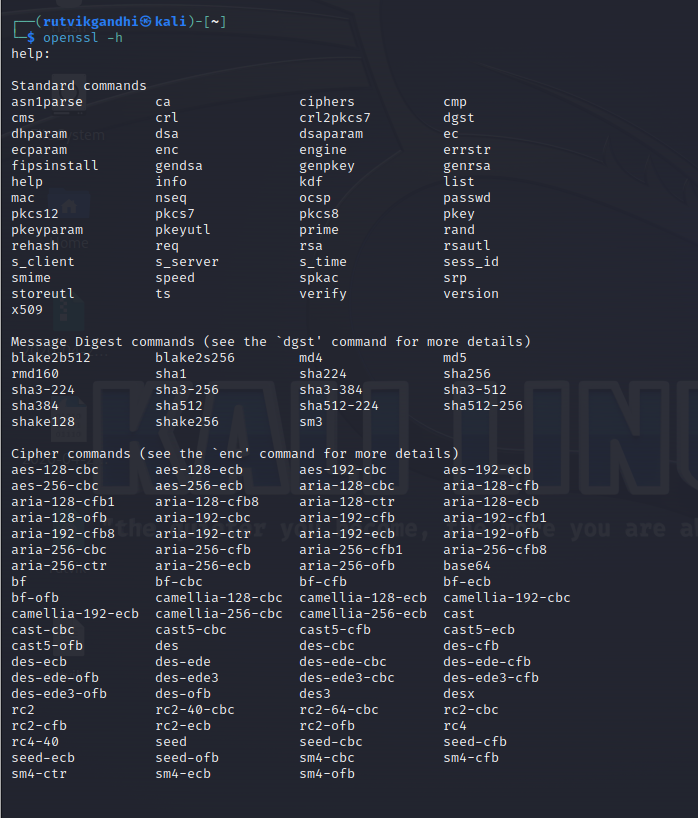
data protection requirements such as GDPR and HIPAA. While not impenetrable, It is an essential

component of a complete cybersecurity plan that adpats to emerging cyber threats. The function of encryption in protecting digital assets and ensuring compliance will continue to increase in prominence EOF

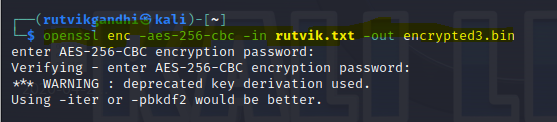
A screenshot of a computer screen

Description automatically generated

TASK2: using two (2) different ciphers, perform an encryption of your original plain-text file (from Task 1) using each of these ciphers.



* Create Encrypted3:



* Create Encrypted4:

A computer screen shot of a computer code

Description automatically generated

* Cat encrypted3:

8[ 9 d6B˯- n M ӡ ? 8 6/ Fr ; l. (> 0 HR" 6} g2: i k XȲG 6 ~w (K z ON .# 7 1 6C}+ I .~NF A ▒ =3h 7]

O) Y ӻԃ ޖ\_ "劳$ $e+( v ժ' Ĝ Q0N 7 L A j M ▒Cm|opA 1 J{ L 1 1c 1 7

&s : s7 { # rY ▒ `ҍPN ڡF ) ` ō dLDV X؉CN }DDZ3 Q 킯&؍CH #kQ r y▒)3 S \ L `$O\_ n▒ nO d = L 6 $9Nɤ ▒7 7 g' MgN u S h%n \_ k Z ߖ ▒ 7o8 M`z "%wD +> x [$ 5 9 U K^ѥs / Y > x x \ > n " ] 'q w !)0,]"

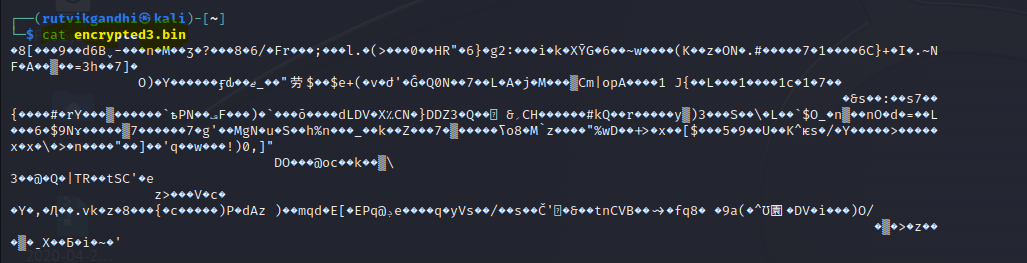
DO @oc k ▒\

3 @ Q |TR tSC' e

z> V c

Y , Ԯ .vk z 8 { ϲ )P dAz ) mqd E[ EPq@ڊe q yVs / s Č'򿚍 & tnCVB ~> fq8 9a( ^Ʊ園 DV i )O/

▒ > z ▒ ˍX Б i ~ '



* Cat encrypted4:

Salted\_\_ N64S/. dG ՠ + )h 蠃z՝ -

탤 / V Xă! ?{{ 4 E=$ K W Sm Ɣ

. E < b- w# 3k ܝg l 9:ۈ f 0 ܙl g 0$ ISt? R) [CD 4k@ \*6 ] X ]P 1 \ Z[? b$ ף }@N: c 砶ι OϠe >At ^ <▒ "[ c +ȿ A ~▒E ; Q4Zϡw▒g}Tg\_ P 2 d > m

v #)6?N - r

ex

x O "y t XKsŒ RP / z; H w nO#` ,{c\* Tm SA▒~~C s M 7▒ H!

p

Q BWid Gڔz i ' p

&u 5 ~Խz5 65 @k A u+ 1

<a .6Ӂ qJ J G Ҋ▒ e > N p6 O Yf Qev Y{ \*D7 \* E% N #\ j cQ Fw 9بi

Dy n U 5 Z\ a Ag

: #Z+s ~ + ڵ 1c\_W C7i jUT &GvH h: r za I 6

Ιb SD fg p |

GJ 둘i ` c N

A computer screen shot of a code

Description automatically generated

* Create descrypted\_aes

A screenshot of a computer screen

Description automatically generated

* Create decrypted\_des

A screen shot of a computer

Description automatically generated

* Cat decrypted\_aes

This report is being created by Rutvik Gandhi. My student id is 8809972

1) Do you think encryption is a valuable cybersecurity too? why or why not?

Ans. Encryption is a critical cybersecurity technique for safegurading sensitive data and communications

in our digital age. It protects privacy by transforming data into unreadable ciphertext, even if

unwanted parties have access. Encryption also protects data by detecting illegal alterations. it

restricts access so that only authorised entities can view data. Encryption is required to comply with

data protection requirements such as GDPR and HIPAA. While not impenetrable, It is an essential

component of a complete cybersecurity plan that adpats to emerging cyber threats. The function of encryption in protecting digital assets and ensuring compliance will continue to increase in prominence EOF

A screen shot of a computer

Description automatically generated

* Cat decrypted\_des

This report is being created by Rutvik Gandhi. My student id is 8809972

1) Do you think encryption is a valuable cybersecurity too? why or why not?

Ans. Encryption is a critical cybersecurity technique for safegurading sensitive data and communications

in our digital age. It protects privacy by transforming data into unreadable ciphertext, even if

unwanted parties have access. Encryption also protects data by detecting illegal alterations. it

restricts access so that only authorised entities can view data. Encryption is required to comply with

data protection requirements such as GDPR and HIPAA. While not impenetrable, It is an essential

component of a complete cybersecurity plan that adpats to emerging cyber threats. The function of encryption in protecting digital assets and ensuring compliance will continue to increase in prominence EOF

A screen shot of a computer

Description automatically generated

TASK3: Using the following grid, perform the tasks listed below in it to symmetrically encrypt and decrypt your name.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **PlainText Name** | R | U | T | V | I |
| **Binary Equivalent** | 01010010 | 01110101 | 01110100 | 01110110 | 01101001 |
| **Key** | 10101010 | 10101010 | 10101010 | 10101010 | 10101010 |
| **Encrypted Output (Binary)** | 11111000 | 11011111 | 11111100 | 11011100 | 11000011 |
| **Encrypted Output (ASCII)** | ÷ | ß | ü | Ü | ƒ |
| **Key** | 10101010 | 10101010 | 10101010 | 10101010 | 10101010 |
| **Decrypted Binary** | 01010010 | 01110101 | 01110100 | 01110110 | 01101001 |
| **PlainText Equivalent** | R | U | T | V | I |

* The name "Rutvi" was encrypted in this example using an eight-bit key "10101010" and a basic XOR technique. As a consequence, the encrypted output is available in both binary and ASCII formats. The same key "10101010" was used to decrypt, demonstrating the symmetric nature of the encryption operation. The textual equivalent of the decrypted binary is "Rutvi," while the original binary representation is "Rutvi."

1. what is one thing that you learned from encrypting and decrypting the first five characters in my name?

Ans. The fundamental principle of symmetric encryption may be learned by encrypting and decrypting the first five characters of my name. Symmetric encryption employs the usage of the same key for both encryption and decryption. It illustrates how, with the right key, i can safely convert plain text to ciphertext (encryption) and then reverse the process to go back to plain text (decryption).

This experiment demonstrates how important key selection is in symmetric encryption. The use of the erroneous key would result in inaccurate decryption, underscoring the need of keeping the key private and safe. It also emphasizes the XOR operation's simplicity in this context, demonstrating how a key may be used to disguise data and subsequently disclose it when appropriate.

1. what importance does the key and the algorithm used in encryption and decryption provide?

Ans. The key and encryption algorithm are critical components in the realm of cryptography, providing critical security for digital data. The key is the linchpin that determines the uniqueness and secrecy of the encrypted data. A strong key, which is usually a long and complicated sequence, protects data against brute-force assaults by assuring that only authorized parties with access to the proper key may decrypt the ciphertext.

The encryption method, on the other hand, specifies how data is converted into ciphertext and then returned to its original form during decoding. A strong encryption technique must be able to withstand mathematical and cryptographic assaults while maintaining the integrity of the encrypted material. Furthermore, it must be scalable and efficient in order to accommodate a wide range of security requirements without sacrificing performance.

The combination of the key and the encryption algorithm creates a multidimensional shield for data, protecting it from illegal access, modification, and interception. Their selection and execution are crucial considerations because they establish the security posture of digital systems, impacting confidentiality, authentication, and overall cyber threat prevention.

Reference:

[1] What is asymmetric encryption? - cloudflare. (n.d.). https://www.cloudflare.com/learning/ssl/what-is-asymmetric-encryption/

[2] Moved. (n.d.). <https://docs.oracle.com/cd/E19047-01/sunscreen151/806-5397/i996724/index.html>

[3] ASCII text to binary converter. (n.d.). https://www.binaryhexconverter.com/ascii-text-to-binary-converter