



# CIPHERCRAFT

Research Document

Author

Josh Casey C00261828

(Student C00261828) Josh Casey

## Table of Contents

Abstract .....	2
Introduction .....	3
What is Cryptography? .....	4
Why Teach Cryptography? .....	5
Module Breakdown .....	8
Module 1: The Start of Cryptography .....	8
Module 2: Where it is now .....	11
Module 3: Advanced Encryption Standard (AES) .....	15
Module 4: Hashing Algorithms .....	19
Module 5: Key Management .....	22
Cryptography in Use .....	24
Problems With Teaching Cryptography .....	25
Cryptography in Cyber Security .....	27
Methods Of Learning .....	28
Visual Learning .....	29
Written Learning .....	30
Listening Learning .....	31
Interactive Learning .....	32
Learning Method in CipherCraft .....	33
Assessment Types .....	35
E-Learning .....	37
Technologies .....	39
Web Programming Language .....	39
Framework: Flask, Django .....	40
Tools .....	41
Database: MySQL, Docker .....	41
User Interface Design .....	42
Conclusion .....	50
Bibliography .....	51

## Abstract

Cryptography proves to be a valuable asset in many sectors of the real world, while CipherCraft aims to provide its users with a fundamental understanding of cryptography. This document delves into different aspects of cryptography, understanding its definition, its importance to a more in depth view of different techniques, algorithms, and functions that are used in cryptography world wide.

As CipherCraft is a learning platform, and wanting its users to succeed gathering information on different learning styles was a must, understanding the benefits that come with each and their disadvantages provides valuable insight for the development stage of CipherCraft.

After an eye-opening discovery of the different learning styles and cryptographic algorithms, the only stage left to research was the different technologies available. Which programming languages are best for this development, what tools can I use to test my platform, how can I store all the required information needed to guarantee a successful development of CipherCraft.

## Introduction

CipherCraft is a web based application that aims to provide it's users with a engaging experience, full of knowledge related to the fundamentals of cryptography. This document presents research of different areas and topics that are relevant to the development of CipherCraft. From what cryptography is, the importance of teaching the topic, to different methods of learning, and the technologies available for the successful development of CipherCraft.

Figuring out what cryptography is proves relevance as it is the topic CipherCraft will teach. Without researching what cryptography is CipherCraft will have already failed, knowing the true definition of cryptography will provide a better understanding and the approach taken with the teaching material provided by CipherCraft.

Researching the importance of teaching cryptography and the value it holds in the real world, will supply a deeper a meaning behind the development of CipherCraft and aid in its success. Analysing the different platforms that teach cryptography to figure out the approaches taken and how to further enhance CipherCraft by gaining insights and inspirations.

Exploring the core modules of CipherCraft and learning of the different cryptographic techniques, functions, algorithms, the advantages and disadvantage that come with them, learning of the different vulnerabilities related to this techniques. Allowing for the material provided for the users to be true and accurate.

Gaining a more in depth understanding of various learning styles, assessment types, and e-learning structures to ensure that users of CipherCraft will be presented with a strong teaching platform. Enabling them to further develop skills and knowledge that CipherCraft aims to teach.

The different learning styles will control the development of the material and how it will be presented to the users, the assessment types determining how the users knowledge will be tested, and the structure of e-learning platforms to better understand the development of CipherCraft.

Delving into the technologies available to figure out which of them will prove valuable to the development stage of CipherCraft. Learning about the different tools, programming languages, and databases used throughout for the development of web based platforms.

## What is Cryptography?

Cryptography can be defined in many ways, from ensuring secure communication, to a science used to encode messages so only the intended recipient can understand them. (Coron, 2006) These definitions are not wrong, but they do not capture the true intentions of cryptography which is about more than just secure communications. (Fortinet, N/A) Cryptography allows for confidentiality, integrity, and authenticity as well as secure communications. Cryptography can achieve all this with the use of different protocols, techniques, and schemes. (SaylorAcademy, N/A)

There are many different types of protocols, techniques, and schemes in cryptography, some that are used to encrypt messages such as the Advanced Encryption Standard (AES), some for ensuring end-to-end encryption such as the Diffie-Hellman protocol, some are used for verification such as digital signatures. (Covic, 2016)

Cryptography has an endless range of tasks it can complete, knowing this the areas of focus will be difficult to choose. Individuals exploring the world of computing require a strong base knowledge in cryptography as it will appear in many sectors of computing, from secure network channels, to maintaining confidentiality on sensitive data such as passwords, cryptography is always present. (Buchanan, 2017)

## Why Teach Cryptography?

### **Importance of Cryptography**

As cryptography proves to be an effective method of protecting sensitive and valuable information from criminals, its usage has become more common in the field of information security. The need for cryptography in the modern world is evident through the different platforms such as WhatsApp, that use the different techniques. (Gençoğlu, 2019)

Without cryptography sensitive information such as credit card details, passwords, and more would be visible for criminals to see and steal. When cryptography is used it turns the information into an unreadable format, this doesn't mean that the confidential information is secure. The level of security when cryptography is used, consists of how the information and techniques are handled within the process, for example how the key is created, stored, and used during the cryptographic method. (Gençoğlu, 2019)

The reason why teaching cryptography is very important, is because understanding the process is what allows for handling of the information correctly. There are many places people can go to learn cryptography from books to online resources such as YouTube, CrypTool, CryptoPals, and many more. These places provide the individual with tools, tasks, and knowledge.

### **CrypTool**

CrypTools is an online website that provides downloadable packages where the user can learn about cryptographic techniques and cryptanalysis. CrypTool is broken down into four different sections, an online version that allows to user to view different cryptographic algorithms in their browser. CT1 which is downloadable and allows experimentation with different cryptographic algorithms on windows. CT2 another downloadable which includes visuals, cryptographic procedures, and cryptanalysis, only viable for windows. JCT which is implemented in java and can run on Linux, MacOS, and Window machines, but focus more on advanced cryptography such as post-quantum algorithms. (CrypTool, 2023)

### **CryptoPals**

CryptoPals is online website that provides the users with a set of challenges to complete relating to cryptography, from the basics to abstract algebra, CryptoPals challenges them all. There challenges relate to real world attacks, supplying the user with a problem and asking for a solution. All challenges are related to weakness found in real-world systems, and modern cryptographic techniques. (Devlin, 2023)

## **Contrast Between Platforms**

CrypTools, allows the users to explore and experiment with the many different types of cryptographic algorithms and techniques, focusing more on the experimentation to allow for a comprehensive understanding of the cryptographic concepts, while CryptoPals takes a practical approach, providing users with real-world problems and asking them to discover a solution.

CrypTools covers many different areas, cryptographic procedures, cryptanalysis, visualisation of algorithms, and even post-quantum algorithms. CrypTools provides algorithms from the basics to the advanced. Whereas CryptoPals provides a total of eight different real-world challenges, from the basics to more advanced cryptography attacks, giving the users hands-on learning for real scenarios.

CrypTools provides flexible accessibility offering, online for one of their many different teaching methods, downloadable packages CT1, CT2, and JCT which are all compatible with Windows, the only one compatible with Linux and macOS is the JCT package. While CryptoPals is only accessible online at their website, but do not require any downloading or user information, the challenges are right there to access.

## **CipherCraft**

While CrypTools and CryptoPals provide valuable information for people to learn about cryptography, through experimentation and hands-on activities, CipherCraft aims to teach people the fundamentals of cryptography, starting from the very beginning and bringing its users to a strong fundamental understanding.

CipherCraft will have a structured curriculum, preventing its users from delving into advanced topics when they are unfamiliar with the basics. In order for a user to progress in CipherCraft they must pass a quiz to ensure an understanding of the concepts, this will stop users from becoming overloaded with too much complex information at once, leading them to frustration.

The visual and interactive components of CipherCraft were inspired by CrypTools, as CrypTools focuses more so on experimentation for learning through visualisation of algorithms, CipherCraft aims to provide an area of learning for common learning styles ([Methods of Learning](#)). The hands-on approach that CipherCraft will take is different to CryptoPals as they focus more so on the real-world problems, CipherCraft will focus on the implementation of cryptographic techniques, enabling its users to correctly use cryptographic algorithms.



## Module Breakdown

CipherCraft plans to incorporate many of CrypTools and CryptoPals ideas, such as the visual, interactive, and hands-on learning approach these platforms use. In contrast to the two platforms, CipherCraft will have a structured curriculum, and quizzes allowing its users to progress to the next stage of learning. CipherCrafts curriculum will focus solely on ensuring its users achieve a strong fundamental understanding of cryptography. See below the module break down:

### Module 1: The Start of Cryptography

#### Topics:

- Why it began?
  - o Brief History of why cryptography was invented
- Caesar Cipher
  - o Method of encrypting, decrypting, the use of a key
- Vigenère Cipher
  - o Method of encrypting, decrypting
- Fence Cipher
  - o Method of encrypting, decrypting

#### **Why it Began?**

The first module will provide a brief background on why cryptography was invented, such as keeping information, and messages hidden from adversaries. It will delve into the reasoning behind the need of keeping information hidden, military tactics, formations etc. Providing simple examples of cryptography such as reversing the spelling i.e., gnilleps – spelling.

#### **Caesar Cipher**

In a depth view of a popular historical encryption method, the Caesar cipher, invented by Julius Caesar to keep his communications secure. It follows a substitution approach, where a number between 0-25 is selected to determine the shift. This number is called the key which used for both encryption and decryption of the message. (KhanAcademy , 2012)

The Caesar cipher uses the alphabet to create its ciphertext, which is the name given to the encrypted message. Let's use the message "*Hello friend*" and we will select the key, or shift as the value 4. The Caesar cipher will then move each letter of the message to the fourth position of the alphabet so A would become E. When we use this shift on the message "*Hello friend*" it becomes, "*lipps jvmirh*" which makes no sense.

This encryption method to date is not incredibly strong and can be easily broken with different methods. From the use of frequency analysis, to computational algorithms the Caesar cipher is broken easily. Frequency analysis is the method of calculating the number of times a letter appears within the ciphertext, when doing so we must understand which letters of the alphabet are most commonly used. This data is widely published so being able to determine which of the letters is most used is easily accessible. (FINIO, 2016)

## Vigenère Cipher

The unbreakable cipher, was invented in the year 1553, by an Italian cryptographer Giovan Battista Bellaso, but the name of the cipher comes from a French cryptographer named Blaise de Vigenère, who invented a similar encryption system. The cipher was given the name “the unbreakable cipher” due to the difficulties people had trying to crack this encryption technique. (Simmons, 2023)

Similar to the Caesar cipher, the Vigenere cipher uses a substitution approach, where it will select a code word, also known as the key. The encryption process uses a grid of the alphabet which goes from A-Z to A-Z, on the x and y axis, which performs a one place shift on each row (See Fig 1). The alphabet is wrote consistently 26 times, the first letter of the code word is used to determine that of the plaintext, which is the name given to the message that is readable and has not gone through any encryption process. (Sarkar, 2020)

Lets use the plaintext of “*CipherCraft*”, and we shall have the key be “*Alien*”. When using the Vigenere encryption the first step is matching which letters of the plaintext will accompany the code, so the first letter C of the plaintext will accompany that first letter of the key, A. On the x axis of the grid we will go to the location of the key which is the first column, here we will navigate down to the letter of the plaintext on the y axis which is C, meaning the C will become C. Following this process the ciphertext will become, “*CtxlrrNjest*”. In times where the plaintext is longer than the key, reptation of the key is used.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Figure 1Vigenère Cipher Grid, (Sarkar, 2020)

Although the Vigenère cipher was given the name “the unbreakable cipher”, this was due to how long the cipher went before becoming susceptible to cracking. Once again this cipher is vulnerable to frequency analysis, as well as Kasiski examination. The Kasiski examination is a method that locates repeated letters and sequences within the ciphertext, determining the length of the key making the cipher easier to crack. (Rahmani, Wadhwa, & Malhotra, 2012)

## Fence Cipher

The fence cipher is completely different than the Caesar and Vigenère cipher, as it takes a transposition approach. This is a method that uses the same letters of the plaintext and switches their position, by following a set of instructions. (Datta, 2023) Invented by the ancient Greeks, who used a special tool called scytale to craft their ciphertext, now a days it can be done with a piece of paper. (crypto-it, N/A)

The fence cipher takes it's plaintext and writes it in a zig-zag pattern, the key will determine the number of rows used within the encryption process. For example lets take the plaintext, "*This message is not for you*" we shall use a key of 2, meaning the process will use two rows in the process of encrypting the plaintext. The top row would consist of "*Timsaesofro*" and the bottom row would consist of "*hsesgintoyu*", writing out each of the rows will create the ciphertext. (Datta, 2023)

Plaintext:     This message is not for you  
First row:     T I M S A E S O F R O  
Second row:   H S E S G I N T O Y U  
Ciphertext:   TIMSAESOFROHSESGINTOYU

This encryption technique can be broken with the use of frequency analysis, trail and error. Without knowing the key, this cipher proves time consuming to break when using pen and paper. Lets assume we did not know the key for the ciphertext above. We would draw out a grid on paper the same length of the ciphertext and being filling in every second position on the top row until it is full, moving to the next row. This of course would provide the plaintext, as the key is only a length of 2, if the key was longer this process would have to be repeated until it began displaying the plaintext. (Rodriguez-Clark, 2017)

## Module 2: Where it is now

### Topics:

- Symmetrical & Asymmetrical
  - o What they are, the differences
- Block Ciphers & Stream Ciphers
  - o The differences, how they work
- One-Time Pad
  - o Explaining XOR and demonstrating it
- Methods of Key Exchange
  - o Diffie-Hellman key exchange protocol

The second module aims to provide the users with an understanding of different types of encryption methods, such as symmetrical and asymmetrical techniques for different cryptographic algorithms, different methods of applying these algorithms such as block and stream ciphers. Demonstrating a core piece of some algorithms using the one-time pad, which operates using x-or, and taking a look at how users keep their private messages safe using a key exchange protocol.

### **Symmetrical & Asymmetrical**

Symmetrical and asymmetrical are two different approaches to creating a cryptographic algorithm. Symmetrical refers to algorithms that use the same key for encryption and decryption, this method is the oldest of the two. This encryption method relies on both parties containing the same key which is the biggest setback for this method. (Sasi, Dixon, & Wilson, 2014)

Asymmetrical cryptography refers to the use of a public and private key, this is achieved using a mathematical equation that links both of the keys together. This method of encryption would use the public key to encrypt its data and the private key to decrypt it. The public key is usually sent out into the world so anyone wishing to send a encrypted message to the owner can do so, and only the owner of the public key will be able to decrypt it assuming they have kept their private key secret. The method used to create these key pairs prevent anyone from being able to construct the private key from the public key. (Sasi, Dixon, & Wilson, 2014)

The difference between both of these techniques is that symmetrical cryptography uses a randomly generated key for both encryption and decryption, while the asymmetric cryptography will use a mathematical equation to generate a key pair that are linked together, where one is used to encrypt and the other for decrypting.

## Block Cipher & Stream Cipher

Block ciphers and stream cipher are a sub category of symmetrical encryption, meaning they use a secret key for their operations. Block ciphers is a method of encrypting fixed length information, data that is not moving i.e. text within a file. This technique is commonly used on large blocks of information. (Robshaw, 1995)

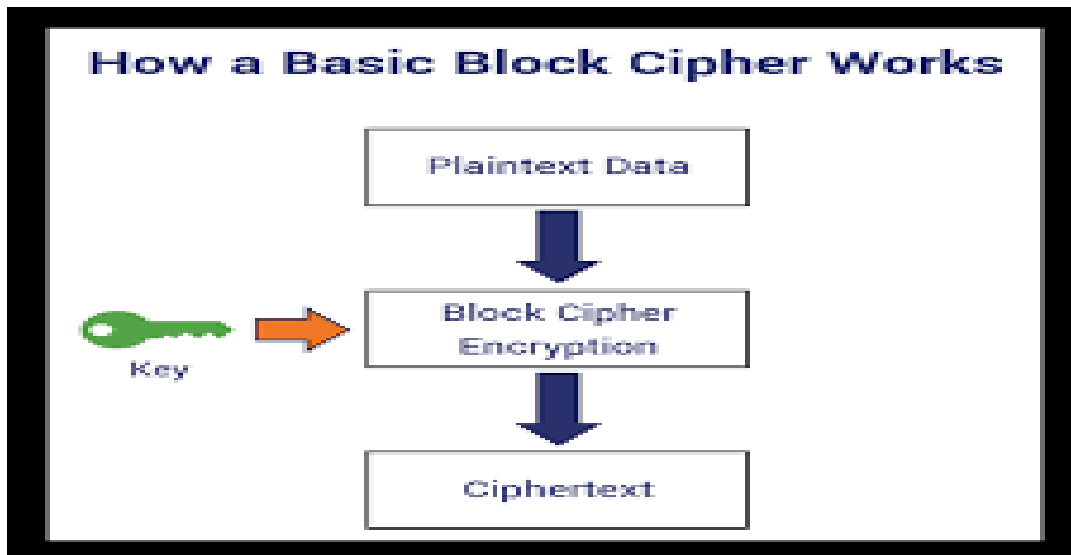


Figure 2Block Cipher, (Crane, 2021)

Block ciphers will perform an operation that converts a block size of plaintext into the same size block of ciphertext. These blocks of data all link together somehow, by either being concatenated or being used as a key itself, either way the blocks must link together for the decryption process. (Houtven, 2017)

Where as stream ciphers operate by encrypting a stream of data, an endless flow. It generates a key stream to encrypt each byte of data, and the same key is used to decrypt that byte. It initially uses a initialization vector or a nonce which is a randomly generate value. This method has its own security flaws such as an oracle attack, and time-memory-data trade off which exploits the birthday paradox. (Moch, 2023)

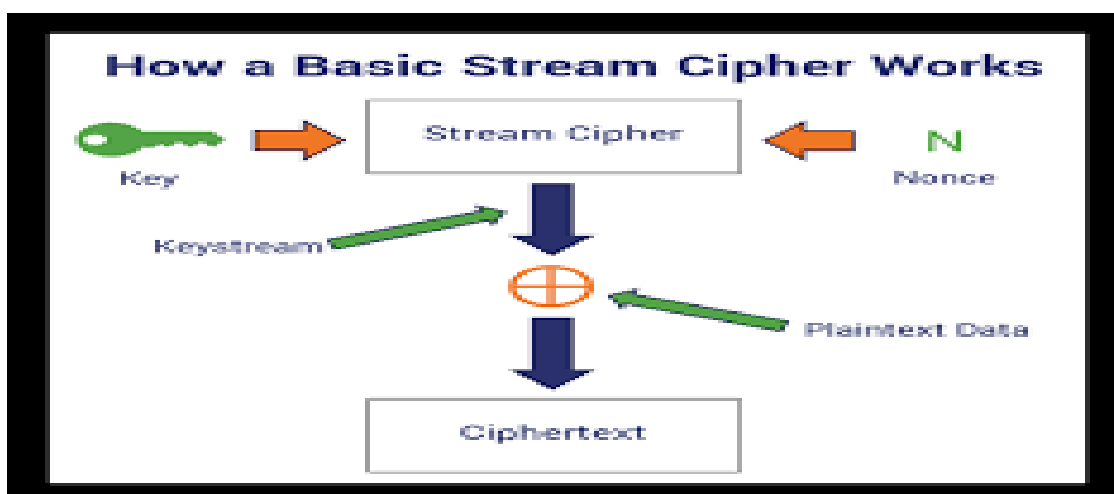


Figure 3Stream Cipher, (Crane, 2021)

## One-Time Pad

The one-time pad is the most secure encryption method that exist, it is the only encryption that is mathematically unbreakable. This encryption is so secure even an unlimited amount of computational power and time are unable to crack this scheme. In order this to be true the procedure for crafting the prefect encryption must be followed correctly. (Rijmenants, 2021)

The procedure of creating the unbreakable encryption is as followed, the key must be the same length of the plaintext or longer. The key must be truly random, not generated, but completely random. That the key is only ever used once, it cannot be used multiple times by the sender or receiver. Lastly the key most only exist for the sender and receiver(s). (Rijmenants, 2021)

The process used to create the one-time pad is the x-or of each bit, let use “10010110” as are plaintext, and “01010011” as the random key. We x-or each bit of the plaintext and key to create the ciphertext. It is a very simple operation and doesn’t require much computational power. When x-or is used if the bits are the same it is represented with 0, and if they are different it is shown with a 1. In this example the ciphertext would be “11000101”. (Houtven, 2017)

<b>Inputs</b>		<b>Output</b>
<b>A</b>	<b>B</b>	<b>X</b>
0	0	0
0	1	1
1	0	1
1	1	0

Figure 4X-OR table, (Themis, 2022)

These strict rules that must be followed are reasons why this encryption method are not ideal, or seen very often in the real world. The need for the key to be the same length of the plaintext is impractical as it can sometimes be an unknown as to the length of a plaintext. The need for the key to be shared before the message was encrypted with the person(s), without knowing the length of the plaintext, not even taking into account if the person(s) is at a distance making sharing of the key impossible or difficult. (Houtven, 2017)

## Diffie-Hellman Key Exchange Protocol

The Diffie-Hellman protocol allows for two users to create the same secret key, they can use to encrypt and decrypt messages with, enabling them to have a secure method of communication. This protocol is susceptible to man-in-the-middle attacks, which is a person that views the exchanging of messages between to people, they may alter the information or just simply view it. (Li, 2010)

Diffie-Hellman protocol is typically used to ensure secure communications so that a symmetrical key can be transmitted securely. The first step taken to generate the shared key is for all parties to create a public-private key pair, they then share the public key with each other. A mathematical equation is then used with the private key of the owner, with the received public key, once this is complete both parties should have the same key. (Kallam, 2015)

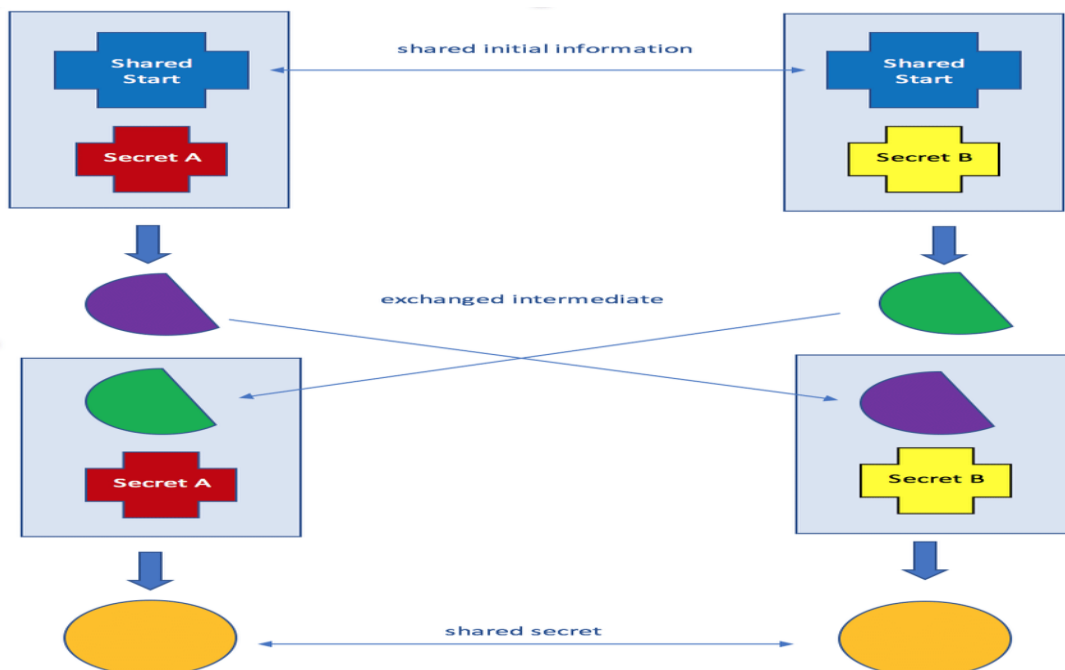


Figure 5 Basic illustration of Diffie-Hellman, (Johnson, 2017)

The image above demonstrates a basic understanding of how the Diffie-Hellman protocol operates. Both started with a shared piece of information (public key), each party member has a secret (private key), they exchange the information (output of the mathematical equation), and repeat with the exchanged information, to obtain the same secret key.

## Module 3: Advanced Encryption Standard (AES)

### Topics:

- AES Process
  - o Showing how AES functions
- Electronic Codebook (ECB) Mode
  - o Example of a bad mode of encryption
- Cipher Block Chaining (CBC) Mode
  - o Strong mode of encryption
- Counter (CTR) Mode
  - o Mode used the most

This module is used to demonstrate how encryption algorithms can use be differently to produce a stronger and more efficient encryption. It will explain the process of AES in depth and some of the different methods available to weaken or strengthen the algorithm.

### AES

The advanced encryption standard is one of the most popular symmetric block cipher algorithms used in the world. This algorithm has found it's way into hardware and software across the world due to its process of encrypting and decrypting sensitive data. AES allows for three different key sizes, 128, 196, and 256 bits, with a block size of 128 bits, this algorithm gives threat actors a hard time deciphering what the data is. (Abdullah, 2017)

The AES algorithm uses a substitution-permutation network, meaning combines both substitution and permutation within its algorithm. Each round consists of AddRoundKey, SubBytes, ShiftRows, MixColumns, and AddRoundKey, the final round does follows the same process minus the MixColumns. (Rawal, 2016)

What do they all mean?

AddRoundKey: is performed on each byte of the block, performing an x-or with each bit using the key. (Rijmen & Daemen, 2001)

SubBytes: performs a substitution with a predefined table known as the S-box, for each byte within the block. (Rijmen & Daemen, 2001)

ShiftRows: this section creates a left shift for each byte in a row. The number of shifts is different for each row. It performs an n-1 shift, where n is the row number (1-4). (Rijmen & Daemen, 2001)

MixedColumns: This step mixed with ShiftRows creates diffusion within the cipher. It multiplies each column with a fixed polynomial. (Rijmen & Daemen, 2001)

These steps are used to perform a single round, which is performed multiple times to create the ciphertext. The number of rounds is based upon the key size, a key of 128 bits performs 10 rounds, 196 bits completes 12 rounds, and a 256 bit key does it 14 times. (Rawal, 2016)



## Electronic Codebook (ECB)

ECB is a mode that can be applied to a block encryption algorithm that will divided each block and preform the encryption on each block individually. This method contains the benefit of parallel processing, which most otherwise modes do not have. (Elashry, Allah, Abbas, & El-Rabaie, 2009)

This can also be considered a disadvantage as it does not rely on any of the other blocks it allows for a threat actor to swap blocks with an intercept block. The use of ECB also has the potential of creating identical blocks of ciphertext, so large blocks of data within images cannot be kept secret with ECB mode. (Elashry, Allah, Abbas, & El-Rabaie, 2009)

The process ECB takes, is encrypting each block individually. ECB will separate each block of the message and preform the encryption on it using the key. The ciphertext will then be a concatenation of the results of each block, this is the easiest mode but is prone to vulnerabilities. (Naouel, Zakarya, & Badr, 2021)

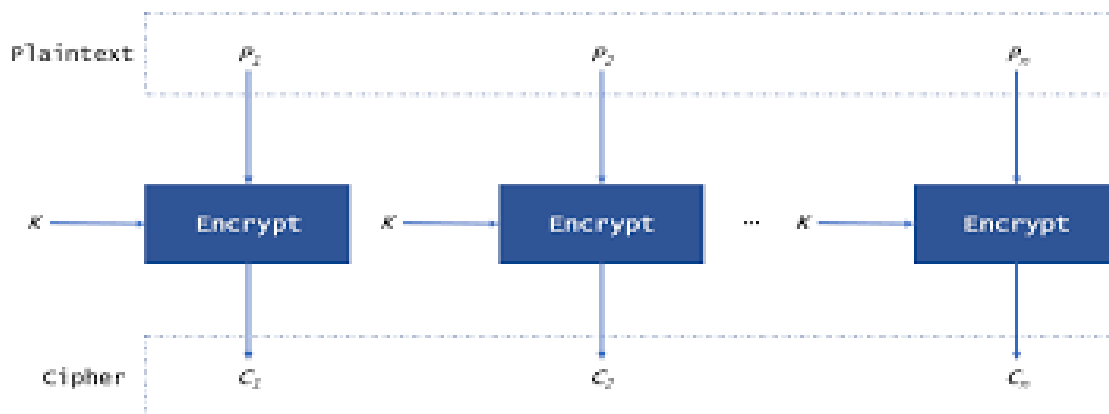


Figure 6 ECB mode process, (Wang, 2019)

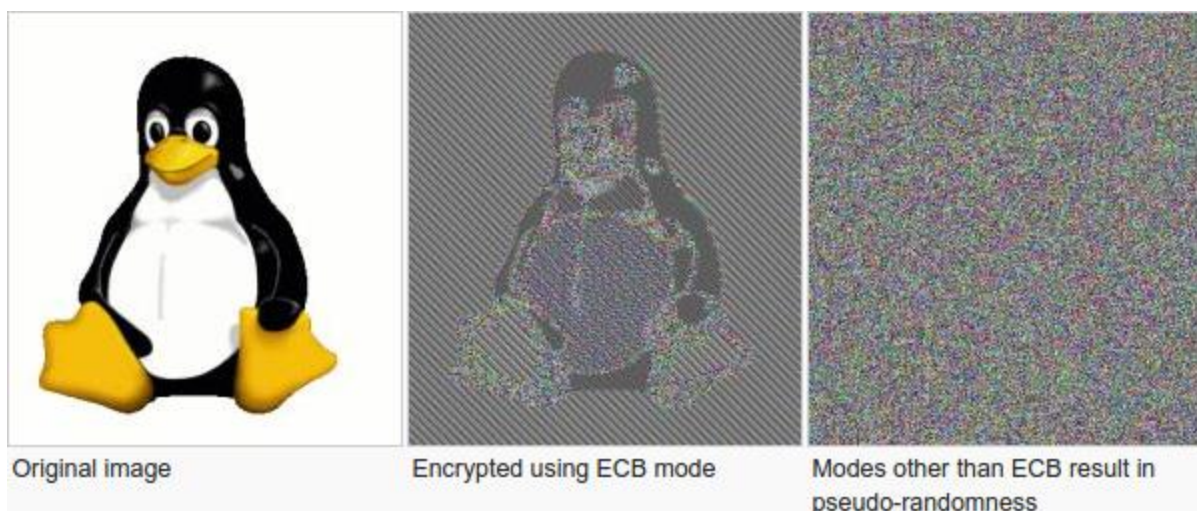


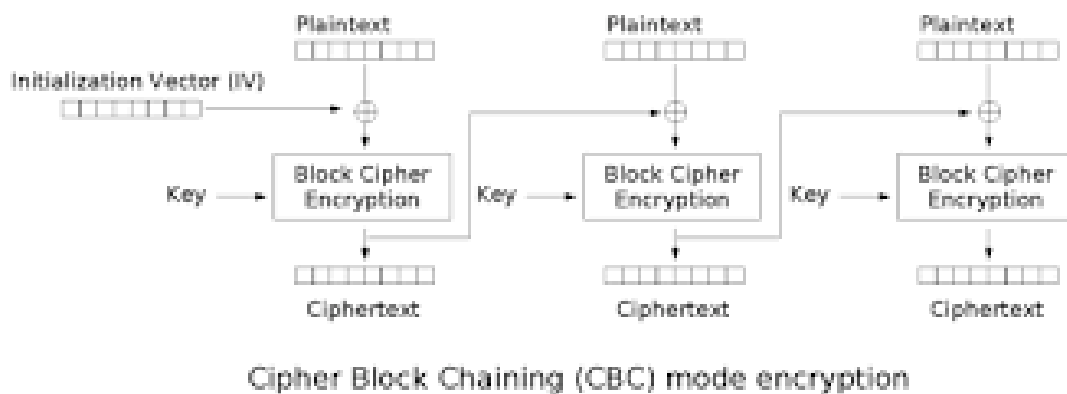
Figure 7 Vulnerabilities of ECB, (Mustafeez, 2023)

## **Cipher Block Chaining (CBC)**

CBC mode of operations provides a higher level of security to the encrypted data compared to the ECB mode. Unlike the ECB mode of operations the CBC mode links each block together, using the n-1 block, where n is the blocks number. The block that becomes encrypted first will be x-or with the plaintext before it goes through the encryption algorithm. (Alslman, Ahmad, & AbuHour, 2023)

Following this process the first block would not be x-or with anything as there is no previous block. This is where the use of an initialization vector (IV) becomes used acting as the first block. The initialization vector is a randomly generated, and must be used only once. The IV does not need to be kept secret, but is required to decrypt the ciphertext. (Bujari & Aribas, 2017)

The disadvantage of the CBC mode of operations is the lack of parallel encrypting. As the mode of operations depends on its previous block to complete the entire encryption, this can slow down the encryption time. (Sinurat & Pasaribu, 2021)



*Figure 8CBC Mode of Operations, (Rogaway, 2013)*

## Counter Mode (CTR)

CTR mode of operations allows for the high-speed encrypting, but has a lack of protection against bit-flipping attacks. The CTR will allow for fast pace encrypting but will still lack the a method of authentication, when it comes to the keeping up with the CTR. (McGrew & Viega, 2005)

The CTR mode makes use of an IV, for each block. The IV must be distinct and different, randomly generating all of these IV could create issues or problems when attempting to decrypting. So CTR uses the same IV, by incrementing its value,  $IV + 1$ , this solves the issue of having the same IV but can easily be calculated when it comes time to decrypt. (Dworkin, 2007)

The CTR mode has over come the issue of ECB where it can allow for preimages by using the IV at the start of its algorithm. Unlike CBC mode it does not require any previous blocks to create its ciphertext. It uses the encrypted IV and x-or with the plaintext to create the ciphertext for each block, which are then concatenated together. (Charot, Yahya, & Wagner, 2003)

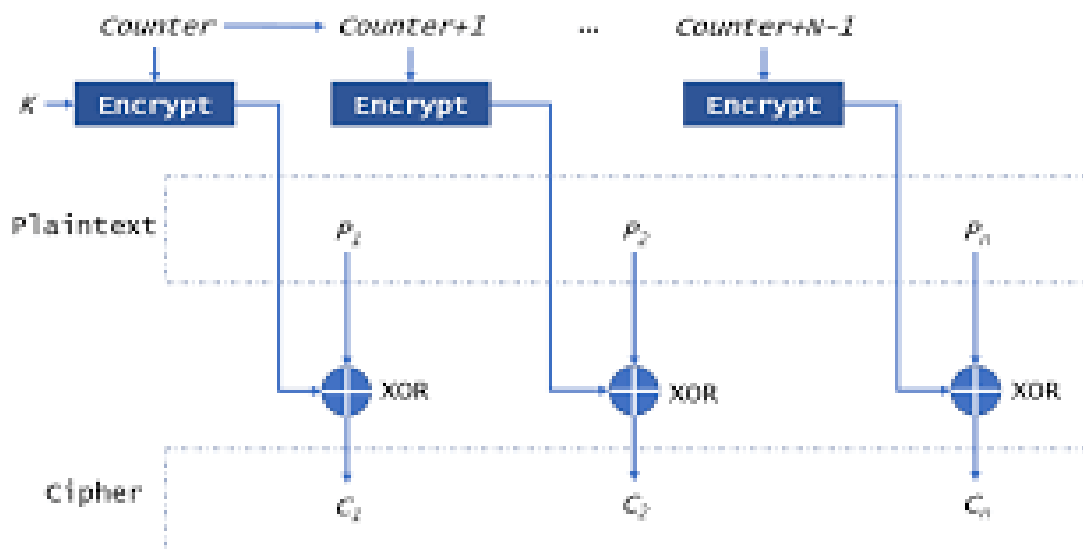


Figure 9 CTR Mode of Operations, (Wang S. , 2019)

## Module 4: Hashing Algorithms

### Topics:

- What is a Hashing Algorithm
  - o Explaining hashing
- Strength of hashing
  - o Collision resistance, Preimage resistance
- Different types
  - o SHA1, MD5, SHA256
- When & where it's used
  - o I.e., Passwords, Files

The fourth module discusses a new cryptographic method, called hashing. It will explore what hashing is, the strengths of a hashing algorithm an overview of different hashing algorithms available. Reasons why this cryptographic technique is used.

### What is Hashing

A hashing algorithm is somewhat similar to an encryption method. The big difference and advantage that hashing algorithm has over a regular encryption is how the hashing algorithm cannot be decrypted, and how the hash value is a fixed value. There is no way of converting the hash value of a plaintext back to a readable format. This is why hashing is also referred to as a one-way function. (Pieprzyk & Sadeghiyan, 1993)



Figure 10 Hashing Algorithm Process, (CodeSigning, N/A)

## Strengths of Hashing

When it comes to hashing algorithms their two main ways of ensuring that the hashing algorithm is secure and unbreakable. These methods are preimage resistance and collision resistance. Ensuring that the algorithm is secure from both will allow for a high level of security. (Houtven, 2017)

Preimage resistance: is when the hashing algorithm makes it next to impossible to invert. Given a range of elements in the hashing function, it should be infeasible to computationally map the elements to an input. (Preneel, 2011)

Collision resistance: refers to how difficult it should be to produce the same hash value with two distinct messages. Message 1 and Message 2 should never have to the same hash value. (Houtven, 2017)

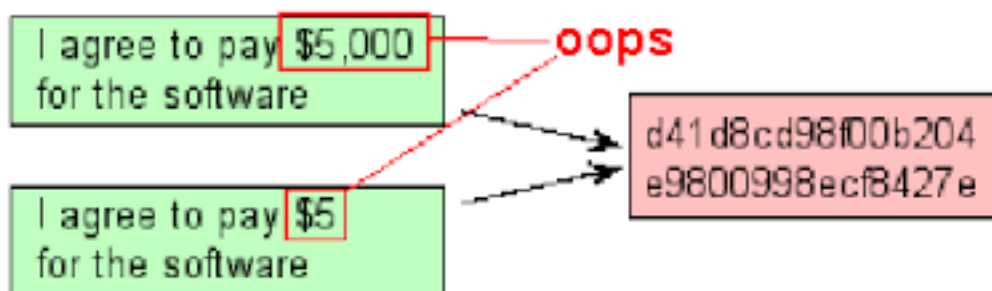


Figure 11 Collision Resistance, (Friedl, 2005)

## Different Hashing Algorithms

SHA1: was created by the National Security Agency 1995, as is the first variant of the revised algorithm. Messages less than 264 bits are supported by this algorithm and will produce a hash value of 160 bits. (Pittalia, 2019)

MD5: which stands for message digest 5, the first mention was in 1989 and has been revisited to last in 1991. The hash value created by MD5 is a length of 128bits. The MD5 hashing function although very popular and widely used, is vulnerable. It is still used as a checksum to ensure the integrity of data, and other non-cryptographic purposes. (Pittalia, 2019)

SHA256: is a variant of the SHA1 algorithm, it produces a hash value of 256 bits, and the function is computed using 32-bits words. This hashing function proves difficult to adopted into systems when compared to SHA1. (Pittalia, 2019)

Algorithm	Word Size	Block Size	Output Size	Rounds	Collision F
MD-2	32	128	128	18	YES
MD-4	32	512	128	48	YES
MD-5	32	512	128	64	YES
SHA-0	32	512	160	80	YES
SHA-1	40	512	160	80	YES
SHA-2	56/64	512/1024	224/256 /384/512	64/80	THEORETI
SHA-3	64	1152/1088 832/576	224/256/384/512	24	NO

Figure 12 Hashing Algorithm Table, (Kamal, 2019)

## Module 5: Key Management

### Topics:

- Importance of Key Management
  - o Explaining why it's important
- Key Generation
  - o Randomness needed
- Key Storage
  - o Different Methods of Storing Keys
- Key Life cycle diagram
  - o The Life of a Key

Module five will delve into the topic of key management, expanding on its importance, how it can be generated entirely random, methods of storing the key in a safe manner, and a diagram detailing the life cycle of a key.

### **Importance of Key Management**

Key Management is important in both symmetric and asymmetric cryptography, both deal with keys, one uses the same key while the other uses key pairs. The importance is being able to keep these keys secret and out of harms way, if a threat actor is able to locate or identify the key, it's encrypted message can be easily decrypted. (Devi, 2013)

Let say I send an encrypted message to a friend, who does not have the key. Someone intercepts the ciphertext, all this person can do it view the unreadable message or change some bits within the ciphertext. If I send this key in the open using an unsecure channel they will be able to decrypt the message and see what I was sending to my friend.

Similar to a large organization who hold plenty of sensitive data they must be able to correctly manage the key, and have a set of instructions on how to deal with the key from creating to storing. (Chojnowska, 2023)

### **Key Storage**

As the key is a critically important aspect of the encryption its storage should be properly done. When storing a key it should be encrypted itself using a different key, this method is called Key Encryption Keys (KEK). This makes sure the key is not stored in plaintext. The keys should be stored within a vault, hardware security module (HSM) or within an isolated area. (OWASP , 2023)

The use of key management libraries should also be used, this refers to the generation, storage, distribution, rotation, revocation, and access control of the key. Ensuring all cryptographic procedures are complete within the vault. Rotation of the key should take place every so often, such as after every use a new key is generated. (OWASP , 2023)

## Life Cycle of a Key

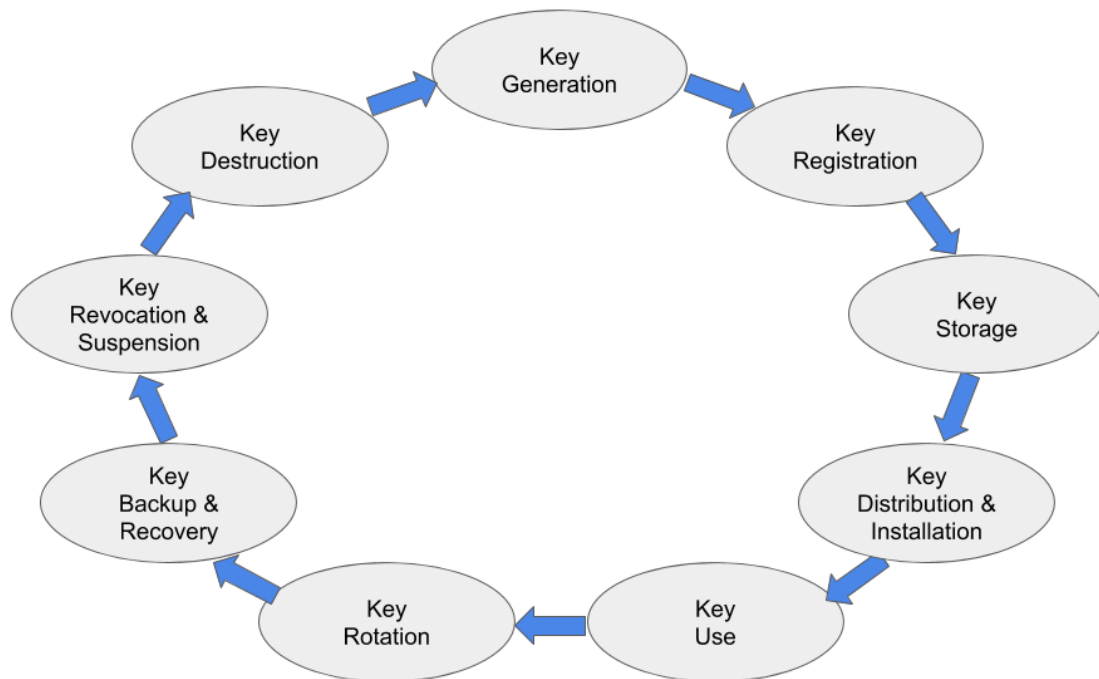


Figure 13 Life of a Key, (Smirnoff, 2018)

The image displays the life cycle of a key, from generation to destruction. It entails 9 different steps:

Key Generation: where the key is created.

Key Registration: refers to key pairing where a person will register their public as their own key.

Key Storage: where the key will be placed for storage until later use.

Key Distribution & Installation: when the key is handed out to a person for use.

Key Use: when it is used within the encryption process.

Key Rotation: changing of the key after a certain length of time, or use.

Key Backup & Recovery: relates to having a backup key available in case the key is lost.

Key Revocation & Suspension: refers to key pairing when an individual's private key is lost/forget/stolen.

Key Destruction: when the key is no longer used and reached the end of its cycle.

(Smirnoff, 2018)



## Cryptography in Use

Cryptographic techniques are used in many different avenues such as, social media platforms, communications systems, financial transactions, healthcare systems, the list goes on. This sections will explore the fundamental algorithms used in each sector.

### **Communication Platforms**

Platforms such as WhatsApp, Telegram, and Signal all use different cryptographic techniques ensuring End-to-End encryption. (Spadafora, 2023) End-to-End encryption is a cryptographic procedure of encryption that allows for messages to be sent encrypted to the intended party, and decrypted on the recipient's end. This can be achieved with the use of the Diffie-Hellman key exchange protocol, which is used to create a key that both parties can use for encrypting and decrypting a message. This allows for confidentiality and integrity, as any information viewed by a third party will all be encrypted and therefore unreadable. (Houtven, 2017)

### **Financial Transactions**

Online banking, e-commerce, and digital currencies are all made possible with cryptography. These different sectors of financial transactions use many different cryptographic techniques to ensure sensitive information is kept secure. Most of these sectors would use the Advanced Encryption Standard (AES) to encrypt the sensitive information. (Ertl, 2023) AES is a symmetrical encryption method that focuses on blocks of data, using the same key for both encryption and decryption. When using the AES encryption method the main focus is storing of the key, as it is required for encrypting and decrypting it must be handled securely. (Houtven, 2017)

### **Healthcare Systems**

Healthcare systems and records contain personal and private information, to ensure that the information is kept anonymous many healthcare facilities use hashing functions. (Physician, 2023) Hashing functions are a one-way algorithmic technique that makes it irreversible, so the data can go through the algorithm but cannot be undone after. These techniques would be used in areas where the information is unlikely to change, such as a person's name, date of birth, and security number. This type of technique is very popular with passwords due to the complexity it takes to reverse engineer these algorithms. (Houtven, 2017)

All these sectors and more use some form of cryptography, demonstrating the value cryptography has in the world. Without it personal, private, and sensitive data would be easily accessible by anyone. (AccessOne, 2023) The descriptions of these sectors using cryptography demonstrate the need for individuals in the computing industry to have a foundational knowledge of cryptography.

### **Complexity of Cryptography**

Cryptography proves to be a complex topic, as it uses mathematical theorems to form the algorithms that they use, these theories can be far to advanced for an average person to understand. Even the most basic cryptography algorithm will use some mathematics to create the algorithm. One of the most popular and widely used mathematical theorems in cryptography is the elliptic curve and how it is paired with many different algorithms, such as AES, and Diffie-Hellman protocol.

The elliptic curve in a basic understanding is the looping of lines intersecting at two axes, which are lines on a graph used to indicate the position of a point. The points are completely symmetric, or mirrored on the x-axis of the graph. (Andrew Froehlich, 2022)

This method is used in cryptography, as it provides a more efficient method with algorithms as the use of elliptic curves require smaller keys, such as Diffie-Hellman Protocol, it creates a finite field which is public knowledge and has both parties generate random keys to add to the points used on the curve. (Vagle, 2000)

Attempting to explain this to individuals who the lack the knowledge of fundamental cryptography, or advanced mathematical background will prove difficult, as the use of mathematical theories can not be avoided in the explanation. Explaining how it operates in terms of cryptography adds an additional layer of complexity.

## **Malicious Cryptography**

As cyber security is all about safeguarding information technology and related areas, discussing the malicious uses of cryptography and how it creates an issue with teaching the topic, is an important area to research. Teaching cryptography the thoughts of malicious uses need to be considered for the approach taken, preventing any users from creating malicious cryptography. Cryptography has many different uses, not only for defending but malicious intent included.

In 1996 at the IEEE Security & Privacy conference was the beginning of malicious Cryptography with Young and Yung who discussed how cryptography could be used within malware to encrypt the local files of the machine and hold them for ransom. This works with the use of generating a key pair, where the public key is implanted within the malwares code and encrypts the files, once the ransom is paid the private key to decrypt is then provided. This method of attack is commonly known as ransomware, but was named cryptoviral extortion by Young and Yung. (Galteland, 2020)

Threat actors can use cryptography to encrypt their malicious code, preventing any form of static analysis. Environmental encryption keys are typically used for this action, it may consists of the victims IP address, paths, information that will be on the victims machine. It will take that information perform rerandomization techniques. When the threat actor performs this, they are not attempting to hide the malware but more so the intentions of the malware. (Galteland, 2020)

The impacts of malicious cryptography when it comes to teaching, is how to ensure that the learners will not use the information for malicious intent. The approach taken when teaching these topics will be crafted in a manner that focuses on the security aspect, rather than the malicious uses, for example when teaching key pairs, it will be discussed in how it can create end-to-end encryption, rather than ransomware.

## Cryptography in Cyber Security

Cyber security is a difficult term to define due to how it has been used consistently within different definitions. Each time the term cyber security is used it mainly surrounds the following, safeguarding cyberspace and the system connected through organizing, managing resources, processes and structures. The main goal of cyber security is to protect cyberspace from incidents that break the legal and actual property rights. (Craig, Diakun-Thibault, & Purse, 2014)

There are three main fundamental principles that are used within cyber security, confidentiality, integrity, and availability. These fundamental principles are typically extended to adding accountability and authenticity. These principles are used to prevent cyber attacks such as data breaches and denial of services. (Kaur, Lashkari, & Lashkari, 2021)

As state above in the section “[What is cryptography](#)” the purpose of cryptography is to provide confidentiality, integrity, and authenticity. The fundamental principles used throughout cyber security are confidentiality, integrity, availability, accounting, and authenticity. As cryptography provides three of the fives principles it is a clear indication that cryptography should be considered a pivotal topic used throughout cyber security.

## Methods Of Learning

Methods of learning otherwise known as learning styles, are a form of learning and understanding. These types of learning styles can be grouped differently, such as words, pictures, speech or written, visual, and listening, either way, these methods of learning are used to determine which method best suits an individual's strongest form of understanding and or greatest level of engagement. (Pashler, McDaniel, Rohrer, & Bjork, 2009)

The most popular hypothesis for learning styles is the “meshing hypothesis,” which refers to providing a format of learning that best reflects the individual learning style, for example, a visual learner, focusing primarily on the visual presentation of information would best benefit as it is the best form of learning for the individual. The hypothesis means to play into the individuals' strengths, by providing information for the user in a form of learning that will best suit them. . (Pashler, McDaniel, Rohrer, & Bjork, 2009)

As I discuss in detail the distinct types of learning styles later in this document, I will also provide the different benefits and disadvantages that may be linked to the method, providing clarity on which methods of learning will best suit CipherCraft.

## Visual Learning

### **Description:**

Visual Learning is a style of processing information from nonverbal manners such as images, graphs, maps, etc., it allows for the learner to view the information in a non-written form for a stronger understanding, for these types of learners the use of diagrams and colour would be best suited. Visual learners would tend to visualize objects or have a photographic memory, allowing them to recall information from a mental image. Visual learner will also have their preference in the way data can be visualized, some may prefer graphs while others may prefer maps. Understanding the diverse types allows educators to tailor the information to the learner. (Clark & Paivio, 1991)

### **Advantages:**

Visual learning has its strengths and weaknesses, more strengths than weaknesses. Some of the benefits are explaining complex topics, such as physics, cryptography, and others, using well-designed diagrams and animations can better explain processes than the use of verbal or written formats. An increase in engagement is another benefit of visual learning, as the world today is very visual with social media and websites such as YouTube, which are used every day. The use of presenting information in a visual format can improve engagement whereas listening or reading may cause learners to lack interest. (Cornell & Drew, 2023)

### **Disadvantages:**

A weakness of the visual learning approach is how it requires less thinking, some aspects of visual learning only require passive experiences such as just looking at and allowing for information to be digested by the learner i.e., watching a video only requires a student to keep their eyes on it, but this means that it may not have the same effect as having to focus on reading information or having to listen to a lecturer speak. (Cornell & Drew, 2023)

### **Benefit for CipherCraft:**

The use of visual learning in CipherCrafts production would be beneficial as it contains complex topics, where coloured diagrams and labels would add value to the user's level of engagement and understanding of the complex theories that are to be covered. Flowcharts, graphs, and diagrams will all be used to enhance the user's ability to learn from CipherCraft.

## Written Learning

### **Description:**

Written Learning or read/write learning is a method of absorbing information through the means of reading notes, handouts, and textbooks. These types of learners tend to retain information best from reading and rereading to writing and rewriting information. To increase the success rate for a learner with this style they should include the following in their studies, using lists, headings, notes verbatim in class, and writing statements for diagrams. Written learners nowadays have the benefit of different online tools to assist with their notetaking, as they have places such as Microsoft Word, which allows for automation of creating lists and highlighting of keywords, these tools help the learners with creating their notes for later usage. (SUCCESSCENTERS, N/A)

### **Advantages:**

Individuals who prefer to learn from reading and writing, have the benefit of becoming more independent, as they can learn and understand from simply taking notes, whereas other types of learners would need visual aids or hands-on activities to better understand or grasp the topic at hand. The advantage of being independent in studying allows the learner to have a self-directed approach, which can be an asset in later stages of education where it becomes independent learning. (SMITH, 2018)

### **Disadvantages:**

Although these types of learner have many different resources to assist them with their studies such as books, articles, and even online platforms, they do have the disadvantage of not being able to completely understand when the option for written material is inaccessible, for example, if instruction are given verbally or in an audible format it may cause difficulties for them to fully participate in the tasks, and may disrupt their understanding. They may also find difficulties with understanding visual instructions and aids as written material would be scarce. They could benefit from adapting listening skills or discussing with peers for a better understanding when these situations appear. (SMITH, 2018)

### **Benefit for CipherCraft:**

The use of written learning would be beneficial for the use of CipherCraft as it would assist those using the platform that best learns from reading and writing. However, the incorporation of this learning style may be difficult as the concepts in cryptography can be considered complex and difficult to explain in a written format, whereas the use of a visual aid would make the process simple. Therefore, using written and visual aids where acceptable would be preferred with practical alternative resources for sections where one method may be inaccessible to provide another approach to the topic.

### **Description:**

Listening Learning, otherwise known as auditory learning, is the method of learning where individuals best retain information through verbal communication. People who prefer this method of learning have a strong memory for remembering what they have heard. The components of speech are particularly important for these learners, i.e., the tone, pitch, and loudness are all key aspects in benefiting these learners in retaining and understanding the information, these learners may also read aloud or quietly to themselves to assist them in absorbing the information. These learners may struggle with written instructions but may gain a stronger understanding if verbally explained. Auditory learning is an asset as the ability to understand from listening can be used in an academic, personal, and professional manner, benefiting the learners through life. (Kayalar & Kayalar, 2017)

### **Advantages:**

Some of the advantages of auditory learning include, being able to multi-task, as the learning style only requires listening this allows for the hands and eyes to be free enabling the learner to complete more in less time, i.e., being able to listen to a recording or audiobook, while driving or cooking. The vast number of online resources is another benefit that auditory learners possess, with the likes of podcasts, audiobooks, and YouTube videos there is an endless supply of locations where the learner can gather information. (Regoli, 2016)

### **Disadvantages:**

On the other hand, auditory learners do have the drawback of becoming distracted. The environment around them will determine the success level of their ability to hear and maintain focus on verbal communication. For example, a classroom that would consist of other students, where whispering may occur, or movements could create a moment of distraction for the learner, causing them to lose focus. An auditory learner does not just get distracted but may also increase the distraction levels for those around them, as they tend to read aloud when reviewing written notes, which may cause those around them to become distracted. (Regoli, 2016)

### **Benefit for CipherCraft:**

The ability to incorporate material that is suited for auditory learners is limited, as CipherCraft is an online application, making the process of verbal communication difficult. To create an optimized learning approach for users that best learn through listening, the usage of video lectures and text-to-speech would be required. The usage of text-to-speech may create issues as the components of speech are important for auditory learning, and the ability to pitch, tone, and loudness may include difficulties.



## Interactive Learning

### **Description:**

Interactive learning, also known as kinaesthetic, tactile, and hands-on learning, is the method of absorbing information through physical aspects such as interacting with an object or participating in a lab activity. Interactive learners prefer movement and interaction with their environment to best learn and understand, i.e., if an individual wishes to learn something new like riding a bike, they have the options of verbally understanding from an explanation, watching a video online demonstrating it, or reading instructions, but kinaesthetic learners would prefer to start peddling the bike straight away. These types of learners prefer areas that use hands-on activities instead of passively listening, watching videos, or viewing graphs/diagrams. During the hands-on activities, the engagement level of these learners will be captured, allowing them to process and understand information. (University, 2022)

### **Advantages:**

Kinaesthetic learning has numerous benefits, Cognitive development, creative thinking, problem solving, and keen observation. Learners who prefer the kinaesthetic style tend to view the activities from different perspectives, enabling them to explore creative approaches to the situation or task they face. Experimenting with different techniques and strategies during the activity helps create critical and analytical thinking skills, and having the learners face the challenges head-on allows them to adapt their problem-solving skills, instead of listening or watching demonstrations. As the learners will try different techniques and strategies, they will be looking for any changes that may occur, this aids them in improving their observation skills. (University, 2022)

### **Disadvantages:**

Kinaesthetic learners face the challenges of not being accommodated in most academic settings, as most individuals who prefer this style of learning may struggle with sitting still in a room for a lengthy time frame, meaning that these individuals will struggle when taking exams as their movements are restricted and limited, or listening to a lecturer which requires concentration and focus on the verbal communication, lacking the physical aspect of learning. The disadvantages that kinaesthetic learners face can be overcome by participating and engaging in activities outside of the academic setting, allowing them to develop hands-on skills at home. (YourTherapySource, 2022)

### **Benefit for CipherCraft:**

Interactive learning would be of great benefit to CipherCraft, as it provides many different opportunities for individuals to increase skills that can benefit them at all stages of life, such as problem-solving, observation, and critical and analytical thinking. It would also provide the users of CipherCraft the ability to learn real-world applications of cryptography.

## Learning Method in CipherCraft

CipherCraft plans to incorporate as many learning styles as possible. As individuals learn best when they can engage with their preferred style of learning, meaning the more styles of learning that CipherCraft tailors for the higher success rate users will have with absorbing the information provided to them. Below you will see detailed areas where the different types of methods will be used:

### **Visual:**

Cryptography is a topic that includes many complex topics, techniques, and algorithms. These topics sometimes consist of areas where written explanations become too in depth and therefore the explanation creates complications in understanding. In these sections, diagrams, and step by step explanations would enhance the users understanding.

Block ciphers and Streams ciphers, explaining these methods of encryptions to individuals unfamiliar with cryptography in words could become quite lengthy, whereas a diagram explaining the encryption processes would both simplify, and provide a deeper understanding for how the different methods work.

Visual aspects of CipherCraft, will always be presented where possible and when necessary. Each module will contain some form of visual representation providing a visual aspect as to how encryption methods operate, ensuring that the visual learners using CipherCraft can engage and gain the fundamental knowledge of cryptography. In sections where visual aids become limited, online resources with in-depth explanations will be provided for the users.

### **Written:**

As visual representations play a major role in providing simple explanations on complex topics, this doesn't mean the written aspect of learning will be ignored. The written material will be presented all over CipherCraft, through definitions, terminology explanations, step by step descriptions, and explanations of topics not too complex.

Terms such as Plaintext, Ciphertext, and Key, would be easier to understand through the means of written material, i.e., Plaintext is readable text, whereas Ciphertext is unreadable text, providing a visual representation for this could be beneficial but not necessary. While the key is a secret code used for encrypting and decrypting. These terms will be constantly used throughout CipherCraft and the understanding of them is necessary, and simply explained in written word.

Written material will be prominently displayed in all the modules provided by CipherCraft. At the start each module will contain new keywords/terms with a brief description of what they mean. A step-by-step process break down for all encryption and decryption functions, with examples and descriptions, the inclusion of these will assist the users in obtaining a stronger understanding of how the functions operate and can be used.

## **Listening:**

Incorporating auditory aspects to CipherCraft will prove difficult, as the only options for an online platform to provide some form of listening, would be to include video lectures or a text-to-speech function. As the platform aims to provide a method for each learning style, listening will prove to be the most difficult. Although there are many APIs and libraries in python that provide a text-to-speech function such as Googles gTTs, my knowledge of them is lacking which will create complications in developing a form of text-to-speech.

The other issue with using text-to-speech is ensuring that the components of listening such as, pitch, tone, and loudness are all developed in a considerate manner to the learners, ensuring a high level of success and engagement with the platform. As this learning will provide difficulties in the development stage, the reliance on video lectures cannot be ignored.

Video lectures will be provided for areas of importance or complexity, such as explaining the different types of algorithms and techniques such as Diffie-Hellman protocol and Advanced Encryption Standard (AES), as these functions are key components in the fundamentals of teaching cryptography. The use of video lectures will ensure that a form of auditory learning is available on CipherCraft.

## **Interactive:**

As interactive learning focuses primarily on hands-on learning, implementing functions for this learning style can be done through labs and activities. The labs would contain step-by-step instructions on how to complete the lab, and what it is the user is doing, as well as code snippets in case the user is unfamiliar or lacks confidence with their programming skills. Areas where users can enter plaintext with a key and view the output of the different functions can also be utilized for an alternate interactive method.

A lab may consist of developing a Caesar Cipher, or AES encryption system to implementing the Diffie-Hellman protocol, and have the users encrypt a certain file or phrase with a certain key, uploading the file or entering the key phrase they used to recreate their input and output to ensure completion of the lab. The labs will assist the users in gaining some real-life experience with implementing different cryptographic methods and supplying them with a hands-on form of learning.

These interactive sections will be consistent at the end of each module, i.e., providing a lab after each section allowing for the users to implement the knowledge they have gained, solidifying their understanding of the topic. Throughout different modules interactive sections may also be present allowing for the users to input different phrases and keys viewing the output.

## Assessment Types

There are many different assessment styles, objective and subjective assessments are the most common found in educational settings. I will discuss below what each assessment is, popular forms of assessing within the styles and the problems CipherCraft could potentially run into. The reasoning behind which of the assessment styles are best suited for the success of CipherCraft will also be discussed.

### **Objective Assessment:**

This is a form of assessment where the answer is either correct or incorrect and does not contain any essays or long descriptive answers. It determines the individual's knowledge based on a quantitative approach. This assessment type is more frequently used in subjects such as Maths, Science and Computer Science, where answers are not up for interpretation and are either correct or incorrect. (Turnitin, 2023)

The styles of assessment that is commonly used when following the objective style are:

- Multiple Choice
- True or false
- Fill in the blank
- Matching
- Assertion and reasoning

The issues with following the objective assessment style are the crafting of questions, as they must be well thought out and written with limited grammatical clues, ensuring that there is only one correct answer and that the other options could be plausible. That the questions are not too complicated and easily understood, that they only focus on one concept or topic at a time and not linking different concepts together. (Turnitin, 2023)

### **Subjective Assessment:**

This style of assessment allows the individual to approach their answers with critical thinking and creativity. In a subjective assessment there is more than one correct answer or approach. It uses a qualitative methodology, meaning it is best suited for areas such as art, philosophy, political science where the answers can be justified with reasoning and are not simply correct or incorrect. (Turnitin, 2023)

The methods of assessments generally used in the subjective assessment style are:

- Short answers
- Essay styles
- Defining terms/concepts
- Critically supported opinions
- Response to theoretical scenario

The problem with implementing a subjective assessment with CipherCraft, is how it involves long text, such as essays to be read and graded, understanding the reasons and justifications for the answer provided. The need to read the essays create difficulties, with CipherCraft being an online learning platform it does not have the manpower to read and grade essay style questions. It could be done using a style of checking for keywords, but this does not measure the users understanding as they may use certain words or have incorrect spellings leading to false marks. (Turnitin, 2023)

### **The Style for CipherCraft**

The only option CipherCraft has is to follow the objective assessment style, as it will provide a true and accurate level of the users understanding in a quantifiable manner. Multiple Choice Quizzes containing the likes of true and false statements, fill in the blanks, and selection of plausible answers, would be best suited for CipherCraft. The construction of the questions may create issues if not thoughtfully created, and well planned out.

The use of subjective assessment is not viable for CipherCraft as it primarily focuses on essay style questions where a person's reasoning and justifications is their answer. CipherCraft will simply not have the ability to accurately assess the individual's answer meaning the users progress could be delayed or hastened, creating frustration and stress for the user which is not the goal of CipherCraft.

Providing the users with feedback on their result, such as the areas they did well in and places they did not should be something considered at the development the stage, as it will allow the users to know which sections, they have a strong and weak understanding. In quizzes where the user fails providing alternative resources may be suited, allowing the users to gain a stronger understanding on the topic.

## E-Learning

### **What is E-Learning**

E-Learning is a method of supplying training or learning, using electronic and digital means. E-Learning platforms can be used on any device connected to the internet from desktop computer to smart phones. They provide a formalized way of teaching people online. This means that people have the potential to become proficient in anything that is provided on a e-learning platform, as they can utilize these e-learning site anytime, anywhere, with minimal restrictions. (Lawless, N/A)

### **Types of E-Learning**

There are many different types of E-Learning platforms, synchronous, asynchronous, fixed, adaptive and many more.

Synchronous: enables groups of students to engage in learning activities together, at the same time, anywhere in the world. This type of online learning allows for real time synchronization as it involves video calls, and online chats. It allows the learners to discuss with their instructor and ask questions. (Tamm, 2023)

Asynchronous: Which is the opposite of synchronous as it, focuses more so on the students independent learning. As students will be studying at different time making online chats and video calls inaccessible. These types of e-learning provide flexibility for the users and focuses more so on a self-paced learning style. (Tamm, 2023)

Fixed: Is where the material used is not changed or altered, that every user of the platform is provided the same content throughout the course. This means the material is often predetermined and is not adapted to the student's preference. (Tamm, 2023)

Adaptive: This type of e-learning is new and innovative, allowing for redesign to the material for each student. This style of e-learning focuses more so on the learner and caters the material towards them, depending on their goals, abilities, skills, and other factors the material provided will be different. (Tamm, 2023)

Understanding the different types of e-learning platforms is crucial in identifying what type of e-learning platform CipherCraft will become. The best options would be asynchronous with Adaptive approach, by following in the steps of these two styles it would allow for flexibility and individualistic approach for the users. Creating a self-paced environment, which will gauge the users' skills and performance, providing them with the material required to achieve their goal.

Although following in the footsteps of these approaches will prove difficult, as ensuring that the material provided is catered per user would create complications in the development stage and most likely become very time-consuming. For these reasons CipherCraft will follow in the footsteps of asynchronous and fixed styles, although the fixed approach proves to have lower success rate, the hopes of ensuring that material provided displays all methods of learning and can fix the issues that the fixed styles come with.

## **Common Technologies**

There are many different types learning management systems (LMS) available, such as cloud-based, open source, commercial, and installation-based. These different types of LMS provide features and support to the development of e-learning platforms. The decision process for selecting the best LMS varies on the requirements of the platform.

Cloud-based: Which are of the most popular due to the swift mechanics of creating a course, and accurate tracking of user progress, and user enrolment. The maintenance of using a cloud based LMS relies on the vendor, this includes hardware, software, and any updates required. The vendor is responsible for ensuring that the system is secure and cannot be harmed. (St-Jean, 2023)

Open Source: These systems are built by multiple people who share code, adding features and fixing any issues. These types of LMS are most cost-effective and can be modified if the skills are available. The problem is the security aspect of using an open source LMS as it could potentially use unsecure code or untested areas, which may create complications in the functionality and trustworthiness of the LMS. (St-Jean, 2023)

Installation-based: Is when the LMS is locally hosted, meaning it is installed on the premises. These types of LMS systems allow for customization of the software and for the database to be stored locally, this method allows for security risks to be removed significantly. The downside of these types of LMS is that need for maintenance, upgrading, and setting up, as all of these must be done by an inhouse team. (Avelino, 2022)

## Technologies

This section of the document will detail and discuss the different technologies available to date, that may be used in order to successfully complete the development stage of CipherCraft. The technologies discussed will be the different programming languages available, tools to enhance the production and testing of CipherCraft, and the design ideas and strategies to ensure a pleasant and user-friendly interface.

### Web Programming Language

#### **PHP**

PHP also known as Hypertext Preprocessor is a open source general-purpose scripting language, widely used in web development as it can be embedded within HTML. PHP unlike JavaScript is executed server side of the web-application. PHP is a simple language that offers more advanced features for strong programmers. (PHP, 2023)

PHP offers more than just server-side scripting, it allows for command line scripting, meaning you can create a programme without the need of a server or browser. PHP allows for object-oriented programming and procedural programming. It can be used on with all major operating systems such as, Linux, Windows, and macOS. (PHP, 2023)

#### **Python**

Python is a high-level programming language, it supports both dynamic typing and binding, as well as code reuse with modules and packages. It primarily focuses on readability with the use of easy-to-learn syntax. The Python library is also massive, free, and open source. (Python, 2023)

Although Python is a general-purpose programming language, it can also be used as a web development programming language with the use of frameworks. Frameworks are predefined packages that stand for the foundation and or structure of the website. Python is widely used to create websites due to the frameworks they provide. (Python, 2023) (Chiluka, 2023)



## **HTML & CSS**

Hyper Text Markup Language otherwise known as HTML, is a standard language when it comes to creating websites. Most if not all websites contain HTML. HTML is used to create the structure of a web page with the use of different tags, these elements are then used to inform the browser how the content should be displayed. (W3Schools, 2023)

Cascading Style Sheets (CSS) is used in conjunction with HTML it provides a method of how and where the elements used in HTML will look and feel. CSS can be utilized within a stylesheet which can describe the layout and design of many different elements. (W3Schools, 2023)

## **JavaScript**

JavaScript is a programming language that is used in many different sectors of programming from web development to gaming JavaScript has seen it all. When it comes to web development JavaScript provides a dynamic approach allowing for the addition of new elements as well as altering existing ones. It is primarily used to enhance a website by including interactive elements to the webpage. (Williams, 2023)

Framework: Flask, Django

## **Flask**

Offers simplicity and minimalism, a micro-framework, meaning it allows for the project developer to be more flexible with how they use the framework. Flask is lightweight and has a smaller codebase and fewer built-in features. The flexibility that Flask offers makes it a very enticing framework, as it allows for the freedom of choosing your own components and libraries, which is great when integrating. (Bahgat, 2023)

## **Django**

High-level framework that contains a wide range of built-in features and tools, these built-in features can help save time during the development stage. Django includes many common web development features, which is advantageous when needing to set up the platform swiftly. Django has a strong emphasis on security, making it good for websites that deal with sensitive data. The scalability of Django makes it suited for large web applications. (Bahgat, 2023)

## Tools

### **Visual Studio Code**

Visual Studio Code is a free lightweight yet powerful Integrated Development Environment (IDE). It has many different extensions available for many different programming languages. It supports languages such as Python, HTML, CSS, and JavaScript. (Visual Studio Code, 2023)

### **XAMPP**

XAMPP stands for Cross-Platform, Apache, MySQL, PHP, Perl. It is a web server solution package that is free and open source. It allows for testing of web servers on a local host using Apache HTTP Server. It uses a control panel to determine which of its functions are currently running, with the use of a start and stop button. (Educba , 2023) (Ravikiran, 2023)

### **GitHub**

GitHub is a website that provides cloud-based storage for code, it is widely used by programmers as a method to manage and maintain their projects. It keeps track of any changes made to the code and allows for collaboration, making it easier to work in a team. ( Kinsta, 2023)

## Database: MySQL, Docker

### **MySQL**

MySQL is an extremely popular open-source database management system. It is used to store data in a structured form. It can store many different forms of data such as numbers, characters, strings, and even dates. MySQL can also link different databases together so the information related to a certain piece of data can be stored separately. (MySQL, 2023) (Oracle, 2023)

### **Docker**

Docker is a platform used for developing and running applications. It allows for the separation of applications and infrastructure so software can be delivered quickly. It uses isolated environments called containers, you may have multiple containers running at the same time. (Docker, 2023)

## User Interface Design

The image below is a flowchart of how the user may interact with the platform. The flowchart was created using Draw.io.

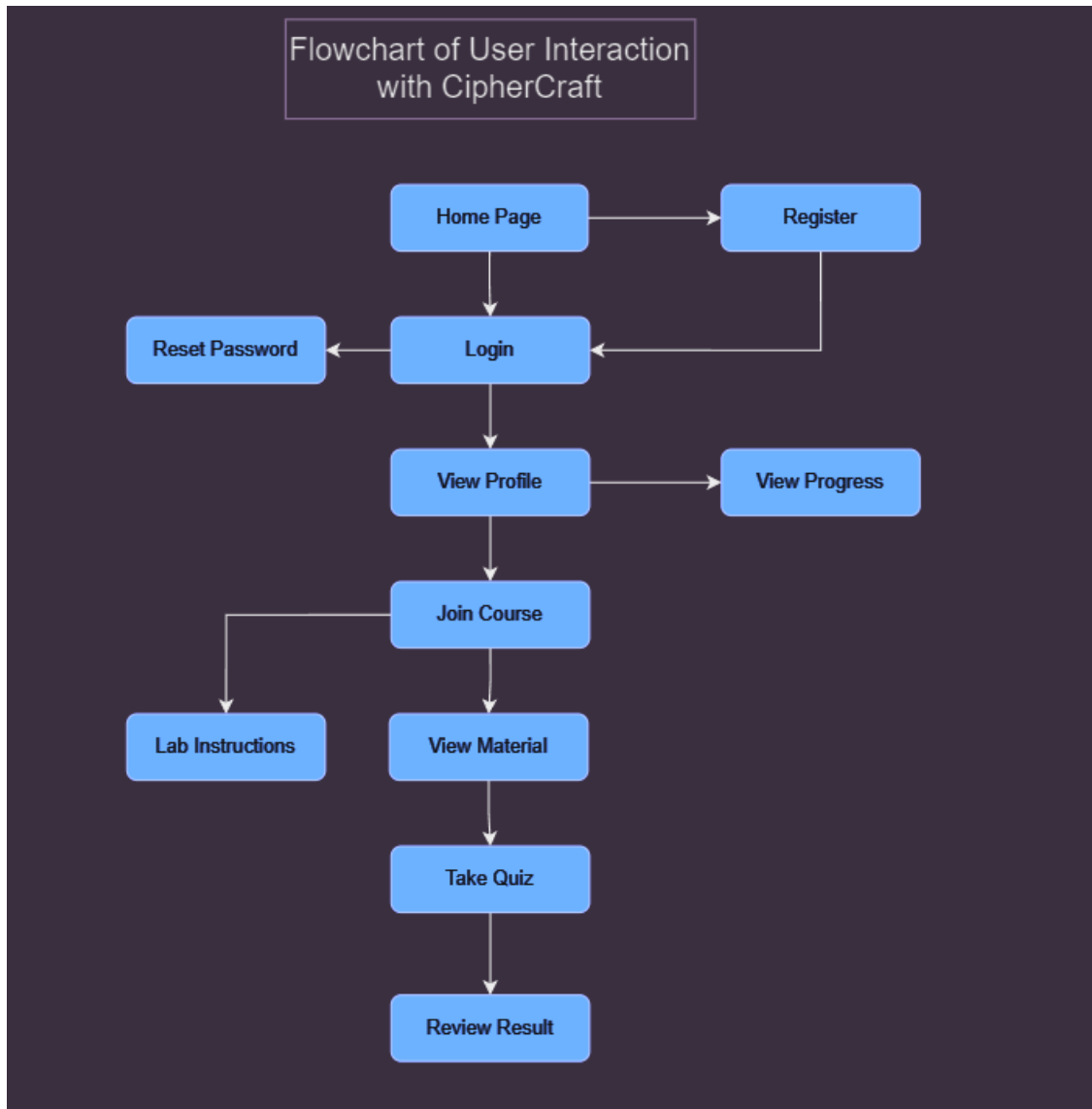


Figure 14:Flowchart Interaction

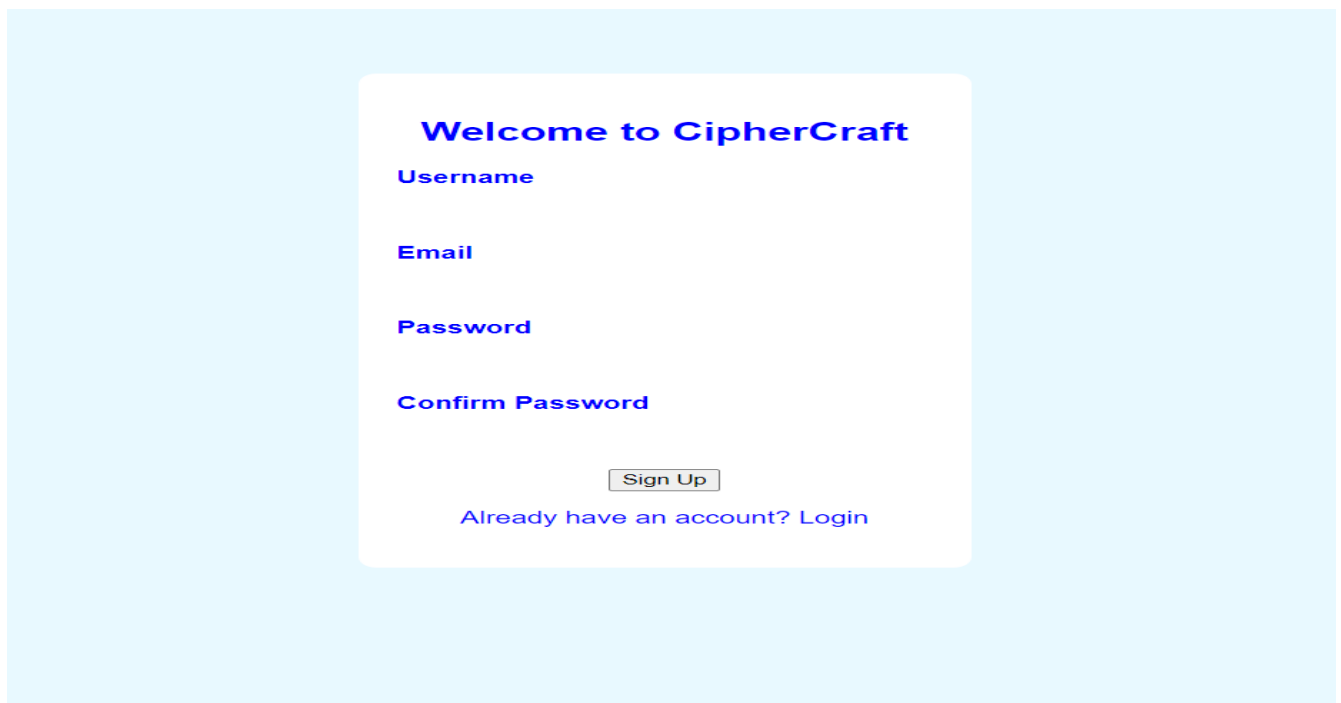
## **Login / Sign up Page**

As CipherCraft is for everyone that is interested in delving into the world of cryptography, there must be a method for signing up and logging into the web page. The design is simple and easy for users to understand.

The sign up page allows for a user to create an account by entering the following information:

- Username : So they have a unique identifier
- Email : To verify that the individual is a person and to allow for emails to be sent directly to them
- Password : As a safe measure for being able to access their information
- Confirm Password : To make sure that they have entered the password correctly

Example Layout:



**Welcome to CipherCraft**

**Username**

**Email**

**Password**

**Confirm Password**

[Already have an account? Login](#)

Figure 15: Sign Up Page

The login page follows the same style of the Sign up page, but requests the users username and password credentials so it can determine that the user is who they say they are and not just another individual. It also contains a method of resetting the password in cases where the user has forgotten it.

Example Layout:

**Welcome to CipherCraft**

**Username**

**Password**

Login

Forgot your password? [Reset](#)

Don't have an account? [Sign Up](#)

Figure 16: Login Page

## **Dashboard / Main Page**

The dashboard of CipherCraft, is the main home page that everyone will be sent to, here they can discover and traverse CipherCraft. It will contain information about the course, be able to start the course, continue the course where they have left off. Learn more about cryptography from additional resources, and discover why cryptography is important.

Example Layout:

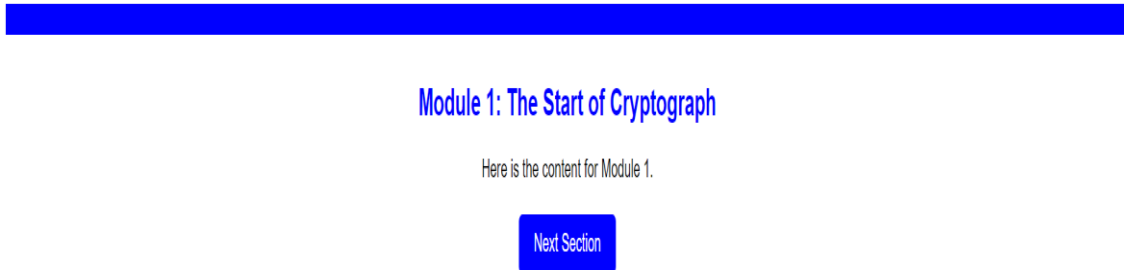


Figure 17:Dashboard

## Course Page

The course page represents the content that will be taught to the users of CipherCraft. It's layout is simple and user friendly, it states the module name, under it shall present all of the content required for that modules topic. With a button to allow the students to move on to the next section.

Example Layout:



*Figure 18:Course Page*

## Quiz Page

The quiz page is where the user will determine if they have learned enough to progress to the next stage. They will be presented with a question, and multiple choice answers where they will select which of the answers they believed to be correct. The page will contain two buttons a 'Previous' and 'Next' these buttons will allow the user to move between questions in case they are unsure of the answer they can traverse them. When a user selects an answer it will be highlighted so they know which one they have selected.

Example Layout:

The image shows a mockup of a quiz page. At the top, there is a blue header bar with the text "Quiz Page" in white. Below the header, the text "Question 1:" is displayed in blue, followed by the question "What is cryptography?" in black. There are four multiple-choice options, each in a blue button: "A: A method of encoding text", "B: A type of encryption", "C: The study of secure communication techniques", and "D: None of the above". Option C is highlighted in yellow. At the bottom, there are two blue buttons labeled "Previous" and "Next".

Figure 19: Quiz Page



## **Lab Page**

The lab page will have a set of instructions detailing how to complete the lab. It will contain a name of the lab, a description of what the user is going to accomplish during the lab, and the benefits of being able to utilize and implement these methods.

Example Layout:

The image shows a template for a lab page. It starts with a solid blue horizontal bar containing the text "Lab Name" in white. Below this is the section "Lab Description" in blue, followed by the text "Name of Lab, What it is for and the benefits of it." in a smaller font. The "Steps" section is also in blue. It contains two steps: "Step 1: Title of Step" with the instruction "Instruction: first step of the lab." and a light gray box containing "Code snippets / examples here". "Step 2: Title of Step" follows with the instruction "Instructions: second step of the lab." and another light gray box containing "Code snippets / examples here".

*Figure 20: Lab Page*

## **Profile Page**

The profile page is where the user can go to learn more about their progress, and achievements. The profile page will display the users information, such as their Username, Email, and Level. The progress they have made on the modules, with their quiz results, and the different achievement that they have gained throughout the course.

Example Layout:

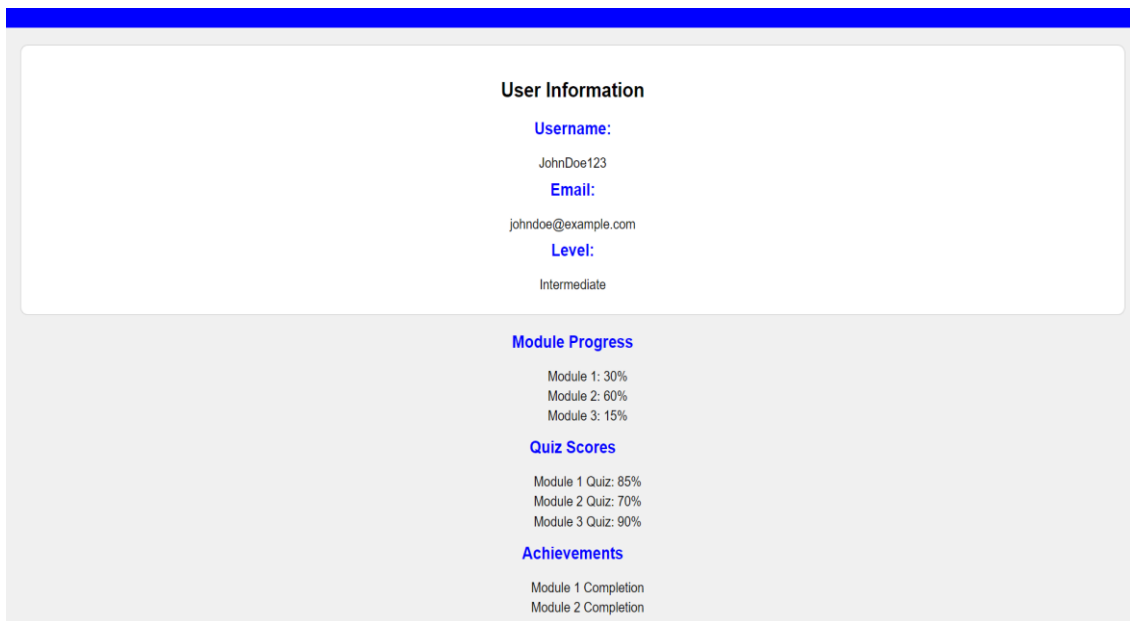


Figure 21: Profile Page

## Conclusion

From gaining a deeper understanding of cryptography such as its definition, providing confidentiality, integrity, and authenticity. To learning its importance in keeping sensitive information secure and the different sectors of the world that use it, hospitals, financial organizations, and much more.

The critical analysis of the different platforms available for teaching cryptography and their methodology and how they differ from one and another, providing valuable insights and inspirations that CipherCraft can follow. Learning how CipherCraft will contrast these platforms, by tracking the users progress, providing a structured curriculum, testing its users knowledge ensuring they are obtaining the information provided to them.

Gaining a more in depth understanding of the topics CipherCraft will teach its users. From the start of cryptography learning about substitution and transposition encryption methods, to the symmetric and asymmetric methods that are used today. The different mode of operations that can be used with block ciphers to increase their security and performance, and the vulnerabilities that come with them.

Methods of learning proved very valuable, understanding how to capture the users engagement by supplying them with their preferred methods of learning. The benefits and disadvantages of each style of learning gave an insight in how to provide the information in an alternative way for users in time where the material may be limited or impossible.

Learning of the different assessment styles, how they are used, and when they are best suited. Lead me down the path of figuring out which style of assessment is best suited for CipherCraft. Gathering information on different E-Learning structures and technologies allowed for a strong understanding on the development it will take to create CipherCraft.

Delving into the technologies that can be utilized to ensure the development of CipherCraft is successful, such as Python and the frameworks available, Php and its advantages, HTML and CSS for the design of the web based application. Tools such XAMPP for hosting and testing CipherCraft, Visual Studio Code as the IDE allowing for a faster development environment. MySQL and Docker for containing and storing the users information.

Creating a mock user interface to have a general idea of how CipherCraft will look, the different pages that will be required, figuring out which colours will best represent CipherCraft and provide an aesthetically pleasing experience for the users. How to create a user friendly interface with ease of navigation and providing information in a simple format.

## Bibliography

- (n.d.). Retrieved from <https://www.educba.com/what-is-xampp/>
- (n.d.). Retrieved from <https://www.simplilearn.com/tutorials/php-tutorial/php-using-xampp#:~:text=on%20your%20PC,-,What%20is%20XAMPP%3F,on%20a%20local%20host%20webserver.>
- Kinsta. (2023). *What Is GitHub? A Beginner's Introduction to GitHub*. Retrieved from Kinsta.com: <https://kinsta.com/knowledgebase/what-is-github/>
- Abdullah, A. M. (2017). *Advanced Encryption Standard (AES)*. Retrieved from researchgate.net: [https://www.researchgate.net/profile/Ako-Abdullah/publication/317615794\\_Advanced\\_Encryption\\_Standard\\_AES\\_Algorithm\\_to\\_Encrypt\\_and\\_Decrypt\\_Data/links/59437cd8a6fdccb93ab28a48/Advanced-Encryption-Standard-AES-Algorithm-to-Encrypt-and-Decrypt-Data.pdf](https://www.researchgate.net/profile/Ako-Abdullah/publication/317615794_Advanced_Encryption_Standard_AES_Algorithm_to_Encrypt_and_Decrypt_Data/links/59437cd8a6fdccb93ab28a48/Advanced-Encryption-Standard-AES-Algorithm-to-Encrypt-and-Decrypt-Data.pdf)
- AccessOne. (2023). *How Encryption Prevents Data Breaches*. Retrieved from accessoneinc: <https://www.accessoneinc.com/blog/how-encryptionprevents-data-breaches/>
- Alslman, Y. S., Ahmad, A., & AbuHour, Y. (2023). *Enhanced and authenticated cipher block chaining mode*. Retrieved from beei.org: <https://www.beei.org/index.php/EEl/article/view/5113/3328>
- Andrew Froehlich. (2022). *elliptical curve cryptography (ECC)*. Retrieved from techtarget: <https://www.techtarget.com/searchsecurity/definition/elliptical-curve-cryptography#:~:text=An%20elliptic%20curve%20is%20not,x%2Daxis%20of%20the%20graph>
- Avelino, J. (2022). *10 Types of LMS*. Retrieved from edapp: <https://www.edapp.com/blog/types-of-lms/>
- Bahgat, A. (2023). *Flask vs Django: Let's Choose Your Next Python Framework*. Retrieved from Kinsta.com: <https://kinsta.com/blog/flask-vs-django/#:~:text=Flask%20tends%20to%20be%20simpler,%2C%20demands%2C%20and%20existing%20requirements.>
- Buchanan, W. J. (2017). *Cryptography across industry sectors*. Retrieved from tandfonline: <https://www.tandfonline.com/doi/full/10.1080/23742917.2017.1327221>
- Bujari, D., & Aribas, E. (2017). *Comparative Analysis of Block Cipher Modes of Operation*. Retrieved from www.researchgate.net: [https://www.researchgate.net/profile/Diedon\\_Bujari/publication/322294203\\_Comparative\\_Analysis\\_of\\_Block\\_Cipher\\_Modes\\_of\\_Operation/links/5a513c97a6fdcc769001fd9a/Comparative-Analysis-of-Block-Cipher-Modes-of-Operation.pdf](https://www.researchgate.net/profile/Diedon_Bujari/publication/322294203_Comparative_Analysis_of_Block_Cipher_Modes_of_Operation/links/5a513c97a6fdcc769001fd9a/Comparative-Analysis-of-Block-Cipher-Modes-of-Operation.pdf)
- Charot, F., Yahya, E., & Wagner, C. (2003). *Efficient Modular-Pipelined AES Implementation in Counter Mode on ALTERA FPGA*. Retrieved from link.springer.com: [https://link.springer.com/chapter/10.1007/978-3-540-45234-8\\_28](https://link.springer.com/chapter/10.1007/978-3-540-45234-8_28)
- Chiluka, V. (2023). *Can we build a website from python?* Retrieved from tutorialspoint.com: <https://www.tutorialspoint.com/can-we-build-a-website-from-python#:~:text=Python%20provides%20a%20lot%20of,one%20of%20its%20primary%20features.>

- Chojnowska, M. (2023). *Data Privacy and Security - Protecting Sensitive Data in a Data-Driven Organization*. Retrieved from sunscrapers.com: <https://sunscrapers.com/blog/data-privacy-and-security-protecting-sensitive-data-in-a-data-driven-organization/>
- Clark, J. M., & Paivio, A. (1991). *Dual Coding Theory and Education*. Retrieved from <https://nschwartz.yourweb.csuchico.edu/>:  
<https://nschwartz.yourweb.csuchico.edu/Clark%20&%20Paivio.pdf>
- CodeSigning. (N/A). *What Is a Hashing Algorithm? A Look at Hash Functions*. Retrieved from codesigningstore.com: <https://codesigningstore.com/what-is-hashing-algorithm-how-it-works>
- Cornell, D., & Drew, C. (2023). *Visual Learning: 10 Examples, Definition, Pros & Cons*. Retrieved from helpfulprofessor: <https://helpfulprofessor.com/visual-learning/>
- Coron, J.-S. (2006). *What is cryptography?* Retrieved from ieeexplore: <https://ieeexplore.ieee.org/abstract/document/1588831/authors#authors>
- Covic, V. (2016). *End-to-end encryption: How does it work?* Retrieved from Mailfence: <https://blog.mailfence.com/end-to-end-encryption-and-digital-signatures/>
- Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). *Defining Cybersecurity*. Retrieved from timreview.ca: <https://www.timreview.ca/article/835>
- Crane, C. (2021). *Block Cipher vs Stream Cipher: What They Are & How They Work*. Retrieved from thesslstore.com: <https://www.thesslstore.com/blog/block-cipher-vs-stream-cipher/>
- crypto-it. (N/A). *Rail Fence Cipher*. Retrieved from crypto-it.net: <https://www.crypto-it.net/eng/simple/rail-fence-cipher.html#:~:text=The%20Rail%20Fence%20Cipher%20was,with%20a%20piece%20of%20p>aper.
- CrypTool. (2023). *CrypTool*. Retrieved from CrypTool: <https://www.cryptool.org/en/>
- Datta, S. (2023). *Cryptography: Rail Fence*. Retrieved from baeldung.com: <https://www.baeldung.com/cs/cryptography-rail-fence-technique#:~:text=The%20rail%20fence%20technique%20is,way%20we%20write%20the%20>message.
- Devi, T. R. (2013). *Importance of Cryptography in Network Security*. Retrieved from ieeexplore.ieee.org: <https://ieeexplore.ieee.org/abstract/document/6524439/authors#authors>
- Devlin, S. (2023). *the cryptopals crypto challenges*. Retrieved from cryptopals: <https://cryptopals.com/>
- Docker. (2023). *Docker overview*. Retrieved from docs.docker.com: <https://docs.docker.com/get-started/overview/>
- Dworkin, M. (2007). *Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM)*. Retrieved from csrc.nist.rip: <https://csrc.nist.rip/external/nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38d.pdf>

- Educba . (2023). *What is XAMPP*. Retrieved from educba.com: <https://www.educba.com/what-is-xampp/>
- Elashry, b. F., Allah, O. S., Abbas, A. M., & El-Rabaie, S. (2009). *A New Diffusion Mechanism for Data Encryption in The ECM Mode*. Retrieved from ieeexplore.ieee.org: <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5383254>
- Ertl, B. (2023). *Ultimate Guide to AES 256 Encryption: Strengthening Data Protection for Unbreakable Security*. Retrieved from Kitework: <https://www.kiteworks.com/secure-file-sharing/ultimate-guide-to-aes-256-encryption/>
- FINIO, B. (2016). *Crack the Code! Make a Caesar Cipher*. Retrieved from scientificamerican.com: <https://www.scientificamerican.com/article/crack-the-code-make-a-caesar-cipher/>
- Fortinet. (N/A). *What Is Cryptography?* Retrieved from Fortinet: <https://www.fortinet.com/resources/cyberglossary/what-is-cryptography#:~:text=Individuals%20and%20organizations%20use%20cryptography,to%20the%20sender%20and%20recipient.>
- Friedl. (2005). *Design of an Enhanced Cryptographic Hash Function-Digest Length 512 Bits*. Retrieved from researchgate.net: [https://www.researchgate.net/figure/Collision-Resistance-depicted-Friedl-2005\\_fig3\\_281319421](https://www.researchgate.net/figure/Collision-Resistance-depicted-Friedl-2005_fig3_281319421)
- Galteland, H. (2020). *Malicious cryptography*. Retrieved from ntnuopen.ntnu.no: [https://ntnuopen.ntnu.no/ntnu-xmlui/bitstream/handle/11250/2649323/Herman%20Galteland\\_PhD.pdf?sequence=1&isAllowed=y](https://ntnuopen.ntnu.no/ntnu-xmlui/bitstream/handle/11250/2649323/Herman%20Galteland_PhD.pdf?sequence=1&isAllowed=y)
- Gençoğlu, M. (2019). *Importance of Cryptography in Information Security*. Retrieved from ResearchGate: [https://www.researchgate.net/publication/331641251\\_Importance\\_of\\_Cryptography\\_in\\_Information\\_Security](https://www.researchgate.net/publication/331641251_Importance_of_Cryptography_in_Information_Security)
- Houtven, L. V. (2017). *Crypto101*. Retrieved from Crypto101.
- Insights, A. (2023). *Objective & Subjective Assessment: What's the Difference?* Retrieved from taotesting: <https://www.taotesting.com/blog/objective-subjective-assessment-whats-the-difference/#:~:text=In%20the%20classroom%2C%20objective%20and,of%20specific%20facts%20and%20concepts.>
- Johnson, J. (2017). *Cyber Security Primer for DER Vendors, Aggregators, and Grid Operators*. Retrieved from researchgate.net: [https://www.researchgate.net/publication/322568288\\_Cyber\\_Security\\_Primer\\_for\\_DER\\_Vendors\\_Aggregators\\_and\\_Grid\\_Operators](https://www.researchgate.net/publication/322568288_Cyber_Security_Primer_for_DER_Vendors_Aggregators_and_Grid_Operators)
- Kallam, S. (2015). *Diffie-Hellman:Key Exchange and Public Key*. Retrieved from cs.indstate.edu: <https://cs.indstate.edu/~skallam/doc.pdf>
- Kamal, P. (2019). *Security of Password Hashing in Cloud*. Retrieved from researchgate.net: [https://www.researchgate.net/figure/Comparison-between-different-hash-algorithms-19\\_fig2\\_331380160](https://www.researchgate.net/figure/Comparison-between-different-hash-algorithms-19_fig2_331380160)
- Kaur, G., Lashkari, Z. H., & Lashkari, A. H. (2021). *Introduction to Cybersecurity*. Retrieved from link.springer: [https://link.springer.com/chapter/10.1007/978-3-030-79915-1\\_2](https://link.springer.com/chapter/10.1007/978-3-030-79915-1_2)

- Kayalar, F., & Kayalar, F. (2017). *The effects of Auditory Learning Strategy on Learning Skills of Language Learners (Students' Views)*. Retrieved from researchgate: [https://www.researchgate.net/publication/320880247\\_The\\_effects\\_of\\_Auditory\\_Learning\\_Strategy\\_on\\_Learning\\_Skills\\_of\\_Language\\_Learners\\_Students'\\_Views](https://www.researchgate.net/publication/320880247_The_effects_of_Auditory_Learning_Strategy_on_Learning_Skills_of_Language_Learners_Students'_Views)
- KhanAcademy . (2012). *The Caesar cipher*. Retrieved from khanacademy: <https://www.khanacademy.org/computing/computer-science/cryptography/encrypt/v/caesar-cipher#:~:text=The%20Caesar%20Cipher%2C%20used%20by,exploits%20patterns%20in%20letter%20frequencies.>
- Lawless, C. (N/A). *What is eLearning?* Retrieved from learnupon: <https://www.learnupon.com/blog/what-is-elearning/#:~:text=eLearning%2C%20or%20electronic%20learning%2C%20is,are%20connected%20to%20the%20internet.>
- Li, N. (2010). *Research on Diffie-Hellman Key Exchange Protocol*. Retrieved from ieeexplore.ieee.org: <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&number=5485276>
- McGrew, D. A., & Viega, J. (2005). *The Galois/Counter Mode of Operation (GCM)*. Retrieved from citeseerx.ist.psu.edu: <https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=dd2166539a6ed65fca90e251f8a9af26e7bf71c2>
- Moch, A. (2023). *Provable security against generic attacks on stream ciphers*. Retrieved from degruyter.com: <https://www.degruyter.com/document/doi/10.1515/jmc-2022-0033/html>
- Mustafeez, A. Z. (2023). *What is ECB?* Retrieved from educative.io: <https://www.educative.io/answers/what-is-ecb>
- MySQL. (2023). *1.2.1 What is MySQL?* Retrieved from dev.mysql.com: <https://dev.mysql.com/doc/refman/8.0/en/what-is-mysql.html>
- Naouel, S., Zakarya, B.-A. M., & Badr, B. (2021). *Optimization of the symmetric encryption mode ECB dedicated to securing medical data*. Retrieved from www.proquest.com: <https://www.proquest.com/docview/2601607624/fulltextPDF/C6A488D9C1DD434CPQ/1?accountid=26695&sourcetype=Scholarly%20Journals>
- Oracle. (2023). *What is MySQL?* Retrieved from oracle.com: <https://www.oracle.com/mysql/what-is-mysql/>
- OWASP . (2023). *Key Management Cheat Sheet*. Retrieved from cheatsheetseries.owasp.org: [https://cheatsheetseries.owasp.org/cheatsheets/Key\\_Management\\_Cheat\\_Sheet.html](https://cheatsheetseries.owasp.org/cheatsheets/Key_Management_Cheat_Sheet.html)
- Pashler, H., McDaniel, M., Rohrer, D., & Bjork, R. (2009). *Learning Styles: Concepts and Evidence*. Retrieved from Sage Journals Home: <https://journals.sagepub.com/doi/full/10.1111/j.1539-6053.2009.01038.x>
- PHP. (2023). *What is PHP?* Retrieved from php.net: <https://www.php.net/manual/en/intro-what-is.php>
- Physician, C. F. (2023). *Utility of hashing and salting algorithms in quality improvement studies*. Retrieved from NHI: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10030136/>

- Pieprzyk, J., & Sadeghiyan, B. (1993). *A construction for one way hash functions and pseudorandom bit generators*. Retrieved from link.springer.com:  
[https://link.springer.com/chapter/10.1007/3-540-57500-6\\_7#citeas](https://link.springer.com/chapter/10.1007/3-540-57500-6_7#citeas)
- Pittalia, P. P. (2019). *A Comparative Study of Hash Algorithms in Cryptography*. Retrieved from d1wqtxts1xzle7.cloudfront.net:  
[https://d1wqtxts1xzle7.cloudfront.net/59869343/V8I6201928-libre.pdf?1561540942=&response-content-disposition=inline%3B+filename%3DA\\_Comparative\\_Study\\_of\\_Hash\\_Algorithms\\_i.pdf&Expires=1702482945&Signature=GxZFPqYx~FkqjTWWVrJxIS--L1v5VfcEDctxHAzHtfCi8iWD3xPA](https://d1wqtxts1xzle7.cloudfront.net/59869343/V8I6201928-libre.pdf?1561540942=&response-content-disposition=inline%3B+filename%3DA_Comparative_Study_of_Hash_Algorithms_i.pdf&Expires=1702482945&Signature=GxZFPqYx~FkqjTWWVrJxIS--L1v5VfcEDctxHAzHtfCi8iWD3xPA)
- Preneel, B. (2011). *Encyclopedia of Cryptography and Security* . Retrieved from link.springer.com:  
[https://link.springer.com/referenceworkentry/10.1007/978-1-4419-5906-5\\_604#citeas](https://link.springer.com/referenceworkentry/10.1007/978-1-4419-5906-5_604#citeas)
- Python. (2023). *What is Python? Executive Summary*. Retrieved from python.org:  
<https://www.python.org/doc/essays/blurb/>
- Rahmani, M. K., Wadhwa, N., & Malhotra, V. (2012). *ALPHA-QWERTY CIPHER: AN EXTENDED VIGENÈRE CIPHER* . Retrieved from researchgate.net:  
[https://www.researchgate.net/profile/Mohammad-Khalid-Imam-Rahmani/publication/276196004\\_Alpha-Qwerty\\_Cipher\\_An\\_Extended\\_Vigenere\\_Cipher/links/5555b0a208ae6fd2d821de69/Alpha-Qwerty-Cipher-An-Extended-Vigenere-Cipher.pdf](https://www.researchgate.net/profile/Mohammad-Khalid-Imam-Rahmani/publication/276196004_Alpha-Qwerty_Cipher_An_Extended_Vigenere_Cipher/links/5555b0a208ae6fd2d821de69/Alpha-Qwerty-Cipher-An-Extended-Vigenere-Cipher.pdf)
- Ravikiran. (2023). *How to Run a PHP File Using XAMPP: A Step By Step Guide*. Retrieved from simplilearn.com: <https://www.simplilearn.com/tutorials/php-tutorial/php-using-xampp#:~:text=on%20your%20PC-,What%20is%20XAMPP%3F,on%20a%20local%20host%20webserver.>
- Rawal, S. (2016). *Advanced Encryption Standard (AES) and It's Working*. Retrieved from www.download-paper.com: <https://www.download-paper.com/wp-content/uploads/2016/04/2016-IRJET-Advanced-Encryption-Standard-AES-and-It%E2%80%99s-Working.pdf>
- Regoli, N. (2016). *6 Advantages and Disadvantages of Auditory Learning*. Retrieved from connectusfund: <https://connectusfund.org/6-advantages-and-disadvantages-of-auditory-learning>
- Rijmen, V., & Daemen, J. (2001). *Advanced encryption standard*. Retrieved from <https://jima.me/wp-content/uploads/2016/05/Advanced-Encryption-Standard.pdf>
- Rijmenants, D. (2021). *One-time Pad*. Retrieved from hawkgirl.net:  
<http://www.hawkgirl.net/documents/communication/One-time-pad.pdf>
- Robshaw, M. (1995). *Stream Ciphers*. Retrieved from people.computing.clemson.edu:  
<https://people.computing.clemson.edu/~jmarty/courses/commonCourseContent/AdvancedModule-SecurityConceptsAndApplicationToLinux/StreamCiphers-RSA-TR-701.pdf>
- Rodriguez-Clark, D. (2017). *Rail Fence Cipher*. Retrieved from crypto.interactive-maths.com:  
<https://crypto.interactive-maths.com/rail-fence-cipher.html>
- Rogaway, P. (2013). *Encryption - CBC Mode IV: Secret or Not?* Retrieved from defuse.ca:  
<https://defuse.ca/cbcmodeiv.htm>



- Sarkar, S. (2020). Retrieved from <https://community.ibm.com/community/user/ibmz-and-linuxone/blogs/subhasish-sarkar1/2020/07/17/how-much-do-you-know-about-the-vigenere-cipher>
- Sasi, S. B., Dixon, D., & Wilson, J. (2014). *A General Comparison of Symmetric and Asymmetric*. Retrieved from [d1wqtxts1xzle7.cloudfront.net: https://d1wqtxts1xzle7.cloudfront.net/33415527/A04330104-libre.pdf?1396920163=&response-content-disposition=inline%3B+filename%3DIOSR\\_Journal\\_of\\_Engineering\\_IOSR\\_JEN\\_Vol.pdf&Expires=1702417274&Signature=Xr4zasKT3eD9cEP~MN-SbWp~CE5TSerRhsEdifA4bTQe-mlF95Hs](https://d1wqtxts1xzle7.cloudfront.net/33415527/A04330104-libre.pdf?1396920163=&response-content-disposition=inline%3B+filename%3DIOSR_Journal_of_Engineering_IOSR_JEN_Vol.pdf&Expires=1702417274&Signature=Xr4zasKT3eD9cEP~MN-SbWp~CE5TSerRhsEdifA4bTQe-mlF95Hs)
- SaylorAcademy. (N/A). *Confidentiality, Integrity, and Authenticity*. Retrieved from Saylor: <https://learn.saylor.org/mod/book/view.php?id=29682&chapterid=5264>
- Simmons, G. J. (2023). *Vigenère cipher*. Retrieved from [britannica.com: https://www.britannica.com/topic/Vigenere-cipher](https://www.britannica.com/topic/Vigenere-cipher)
- Sinurat, S., & Pasaribu, M. (2021). *Text Encoding Using Cipher Block Chaining Algorithm*. Retrieved from [ejournal.seaninstitute.or.id: https://ejournal.seaninstitute.or.id/index.php/InfoSains/article/view/42](https://ejournal.seaninstitute.or.id/index.php/InfoSains/article/view/42)
- Smirnoff, P. (2018). *The private life of private keys*. Retrieved from [cryptomathic.com: https://www.cryptomathic.com/news-events/blog/the-private-life-of-private-keys](https://www.cryptomathic.com/news-events/blog/the-private-life-of-private-keys)
- SMITH, D. (2018). *Advantages & Disadvantages of Different Learning Styles*. Retrieved from Classroom: <https://classroom.synonym.com/advantages-disadvantages-different-learning-styles-2873.html>
- Spadafora, A. (2023). *The best encrypted messaging apps in 2023*. Retrieved from [tomsguide: https://www.tomsguide.com/reference/best-encrypted-messaging-apps#:~:text=End%2Dto%2DEnd%20encryption%2C,handles%20unencrypted%20SMS%20text%20messages.](https://www.tomsguide.com/reference/best-encrypted-messaging-apps#:~:text=End%2Dto%2DEnd%20encryption%2C,handles%20unencrypted%20SMS%20text%20messages.)
- St-Jean, E. (2023). *Learn the 6 types of learning management systems*. Retrieved from [Techtarget: https://www.techtarget.com/searchhrsoftware/tip/Learn-the-6-types-of-learning-management-systems](https://www.techtarget.com/searchhrsoftware/tip/Learn-the-6-types-of-learning-management-systems)
- SUCCESSCENTERS. (N/A). *Helping students PREPARE, ADVANCE and EXCEL*. Retrieved from [https://ccri.edu/: https://ccri.edu/tutoring/pdf/sc\\_LearningStyles-FINAL.pdf](https://ccri.edu/: https://ccri.edu/tutoring/pdf/sc_LearningStyles-FINAL.pdf)
- Tamm, S. (2023). *All 10 Types of E-Learning Explained*. Retrieved from e-student: <https://e-student.org/types-of-e-learning/>
- Themis, S. (2022). *How to find the Signal Probability equation of XOR gate with N inputs*. Retrieved from [electronics.stackexchange.com: https://electronics.stackexchange.com/questions/640020/how-to-find-the-signal-probability-equation-of-xor-gate-with-n-inputs](https://electronics.stackexchange.com/questions/640020/how-to-find-the-signal-probability-equation-of-xor-gate-with-n-inputs)
- Turnitin, E. (2023). *The Difference Between Subjective and Objective Assessments*. Retrieved from [examsoft: https://examsoft.com/resources/subjective-and-objective-assessment-differences/#:~:text=Eduytic%20defines%20objective%20assessment%20as,rely%20heavily%20on%20objective%20exams.](https://examsoft.com/resources/subjective-and-objective-assessment-differences/#:~:text=Eduytic%20defines%20objective%20assessment%20as,rely%20heavily%20on%20objective%20exams.)

- University, B. A. (2022). *Bay Atlantic University*. Retrieved from bau.edu:  
<https://bau.edu/blog/kinesthetic-learner/#:~:text=A%20kinesthetic%20learner%20would%20rather,you%20are%20trying%20to%20learn.>
- Vagle, J. L. (2000). *A Gentle Introduction to Elliptic Curve*. Retrieved from vpb.smallyu.net:  
[https://vpb.smallyu.net/\[Tech\]%20elliptic-curve%20cryptography/A%20Gentle%20Introduction%20to%20Elliptic%20Curve%20Cryptography.pdf](https://vpb.smallyu.net/[Tech]%20elliptic-curve%20cryptography/A%20Gentle%20Introduction%20to%20Elliptic%20Curve%20Cryptography.pdf)
- Visual Studio Code. (2023). *Getting Started*. Retrieved from code.visualstudio.com:  
<https://code.visualstudio.com/docs>
- W3Schools. (2023). *CSS Introduction*. Retrieved from w3schools.com:  
[https://www.w3schools.com/css/css\\_intro.asp](https://www.w3schools.com/css/css_intro.asp)
- W3Schools. (2023). *HTML Introduction*. Retrieved from w3schools.com:  
[https://www.w3schools.com/html/html\\_intro.asp](https://www.w3schools.com/html/html_intro.asp)
- Wang, B. S. (2019). *The difference in five modes in the AES encryption algorithm*. Retrieved from highgo.ca: <https://www.highgo.ca/2019/08/08/the-difference-in-five-modes-in-the-aes-encryption-algorithm/>
- Wang, S. (2019). *The difference in five modes in the AES encryption algorithm*. Retrieved from www.highgo.ca: <https://www.highgo.ca/2019/08/08/the-difference-in-five-modes-in-the-aes-encryption-algorithm/>
- Williams, M. (2023). *What Is JavaScript Used For?* Retrieved from computerscience.org:  
<https://www.computerscience.org/bootcamps/guides/javascript-uses/#popular>
- YourTherapySource. (2022). *KINESTHETIC LEARNERS*. Retrieved from yourtherapysource:  
<https://www.yourtherapysource.com/blog1/2022/09/10/kinesthetic-learners/#:~:text=Kinesthetic%20learners%20may%20struggle%20with,such%20as%20reading%20a%20map.>