Spring 2019

Cyber Security- A New Secured Password Generation Algorithm with Graphical Authentication and Alphanumeric Passwords Along With Encryption

Akash Rao
Old Dominion University, aakashrao86@gmail.com

Recommended Citation

Rao, Akash. "Cyber Security- A New Secured Password Generation Algorithm with Graphical Authentication and Alphanumeric Passwords Along With Encryption" (2019). Master of Science (MS), Thesis, Electrical & Computer Engineering, Old Dominion University, DOI: 10.25777/evz8-6s05
https://digitalcommons.odu.edu/ece_etds/162

CYBER SECURITY- A NEW SECURED PASSWORD GENERATION ALGORITHM WITH GRAPHICAL AUTHENTICATION, AND ALPHANUMERIC PASSWORDS ALONG WITH ENCRYPTION

by

Akash Rao
B.E. July 2011, Gujarat University

A Thesis Submitted to the Faculty Of
Old Dominion University in Partial Fulfillment of the
Requirements for the Degree of

MASTER OF SCIENCE

ELECTRICAL AND COMPUTER ENGINEERING

OLD DOMINION UNIVERSITY
May 2019

Approved by:

Linda Vahala (Director)

Holly Handley (Member)

Weize Yu (Member)

ABSTRACT

CYBER SECURITY- A NEW SECURED PASSWORD GENERATION ALGORITHM WITH GRAPHICAL AUTHENTICATION, AND ALPHANUMERIC PASSWORDS ALONG WITH ENCRYPTION

Akash Rao
Old Dominion University, 2019
Director: Dr.Linda Vahala

Graphical passwords are always considered as an alternative of alphanumeric passwords for their better memorability and usability [1]. Alphanumeric passwords provide an adequate amount of satisfaction, but they do not offer better memorability compared to graphical passwords [1].

On the other hand, graphical passwords are considered less secured and provide better memorability [1]. Therefore many researchers have researched on graphical passwords to overcome the vulnerability. One of the most significant weaknesses of the graphical passwords is "Shoulder Surfing Attack," which means, sneaking into a victim's computer to learn the whole password or part of password or some confidential information. Such kind of attacks is called as Shoulder Surfing Attack.

Many researchers have presented various ideas to curb the shoulder surfing attack. However, graphical passwords are still vulnerable to this attack. Therefore, in the present thesis, the solution for shoulder surfing attack is analyzed and a new algorithm is developed to provide better algorithm with memorability as well as very strong password using the encryption. For alphanumeric passwords, dictionary attack, and brute force attack are critical potential threats to be taken care off. Dictionary attacks mean, attacking every word from the dictionary to crack the password, whereas, brute force attack means, applying all different kind of combinations to crack

the password. Thus, both protection methods have their pros and cons and, therefore in this thesis, the possible solution has been researched to provide more secure technique. Encryption is another essential technique in the field of cybersecurity. The history of encryption dates back to World War 2, where German forces used its encryption technique for the first time, and this encryption has been developed a lot with the consistent contribution of many researchers.

Starting from the German encryption technique, the present encryption field has evolved a lot and compared to its primitive form; the current encryption techniques are more secured. In the encryption, various cryptosystems have been developed, and due to consistently developed computational power, attackers have compromised various cryptosystem. One of the essential cryptosystems is the MD family cryptosystem. In the MD family, a few members have been compromised whereas members such as MD5, had inbuilt algorithm flow and therefore they became vulnerable for different reasons.

In this thesis, the research has been done with Whirlpool encryption, which is never compromised as of now. However, before using the Whirlpool encryption, the string has been processed with multiple steps, such as, perception, shifting of characters, splitting the string into chunks, and then each piece has been encrypted to populate 128 characters long password for each fragment and thus, the algorithm to generate 1280 characters long passwords is proposed which are immune to linear attacks, dictionary attacks, brute force attacks, and shoulder surfing attack.

After the research, the computational time is also calculated for the modern computer (8 core, 2.8 GHz) as well as the present Supercomputers which are 100000 times faster than a modern computer. After all the research, the conclusion and future work are also mentioned for future research.

In the memory of my late maternal grandparents...

ACKNOWLEDGEMENTS

I want to acknowledge the many individuals that assisted me in preparation of this thesis. I want to give special thanks to Dr. Linda Vahala for increasing my knowledge and boosting me ab-initio. I am thankful to Dr.Holly Handley and Dr.Wize Yu for their enormous support and guidance in the manifold.

I am much thankful to my family for their unwavering support. Their persistent and consistent support has contributed to my successful completion of this thesis research. Lastly, I am also thankful to my supervisors at my workplace as well as my colleagues at my second workplace (University library) who have made my experience at Old Dominion University memorable.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

Authentication means the process to determine if a person is a genuine user and the person has been approved to access a specific service or resource. For authentication other than alphanumeric passwords, smart cards and biometrics are also being used [2, 3]. However, despite these alternatives, alphanumeric passwords are dominant and may remain dominant for some time as smart cards require pins and biometrics are related closely with privacy. [4, 5, 6]

The most widely practiced computer authentication method is to use alphanumeric passwords, but it has drawbacks [8]. The drawbacks are used by attackers to compromise the security; therefore, a new algorithm is developed and investigated in this thesis. The new algorithm provides not only memorability, but it also concentrates on the important issue of strength of the password. For this purpose, the algorithm is developed with a good encryption method (Whirlpool encryption) to generate very strong passwords while considering memorability from the user's point of view.

Alphanumeric passwords are more vulnerable compared to graphical passwords because users tend to have a short password to make it more memorable. These short passwords are riskier and can be attacked easily. Further, textual or alphanumeric passwords are at risk of a dictionary attack, key-loggers, password-guessing, shoulder-surfing, and spyware, etc. [8].

Generally, people tend to set short and easily memorable passwords rather than difficult passwords. This is because textual passwords are robust enough to prevent guessing are also tough to remember [8]. For such difficult passwords, the ambiguous question remains as the length of the password. If only textual passwords are accepted as a solution to counter various attacks such as a brute force attack through a computer, then the length of textual passwords comes into consideration, but another question arises about the memory of the users. Therefore, alphanumeric passwords are good, but it is a requirement to develop an algorithm where very strong passwords can be generated that consider the user's memorability.

Therefore, as an alternative to alphanumeric passwords, graphical passwords have been researched by many researchers over time. It has been found that many images may help memorability in graphical passwords [1]. Graphical passwords are secure to remember compared to complex alphanumeric passwords [1, 7, 9]. However, graphical passwords have their drawbacks, and one of them is called a shoulder surfing attack. Graphical passwords are more vulnerable to shoulder surfing attacks compared to alphanumeric passwords. [8]

On the other hand, as discussed earlier, textual or alphanumeric passwords have their drawbacks including dictionary attack and a user's inability to remember lengthy passwords. Considering pros and cons of graphical passwords and textual passwords, a new idea is proposed in this thesis to generate a very long alphanumeric password through Whirlpool encryption which would not be vulnerable to dictionary attack or any such attack from the user's perception on graphics. Also, users are not required to remember long strings of passwords.

"The Graphical authentication have been criticized for susceptible to over-the-shoulder attacks (OSA). To solve this shortcoming, schemes have specifically been designed to be resistant to OSA. Common strategies used to decrease the ease of OSA are grouping targets among distractors, translating them to another location, disguising the appearance of targets, and using gaze-based input."-- Usability Comparison of Over-the-Shoulder Attack-Resistant Authentication Schemes by Ashley A Cain et al.

"For graphical password schemes, security and usability represent opposite ends of a spectrum: increasing security implies decreasing usability and vice versa. Therefore, a

tradeoff is required based on user requirements. To meet user requirements, we should contacts the two aspects with the special target environment when a new scheme is proposed or for selecting the appropriate scheme." "Survey on the Use of Graphical Passwords in Security- Haichang Gao et al. [11].

Many researchers opine that graphical passwords require further research to overcome over the shoulder attack and its security and usability represent opposite ends of a spectrum [11, 10]. Therefore, in this thesis a new method to generate a powerful password which would be extremely difficult for modern computers and even a super-computer to destroy.

On the other hand, encryption is one of the protective methods in the domain of cybersecurity to help protect information and to enhance security.

There are many different cryptosystems that have been developed over time and compromised from time to time by many attackers. The essential cryptosystem is the MD family encryption method. This cryptosystem has MD1, MD2 up to MD5 members and all of them are compromised over time. Therefore, in this thesis, a new algorithm has been designed with its steps and with the help of Whirlpool encryption.

Whirlpool encryption generates a string of 128 characters for each chunk and a 1280 character long password for full input from the user based on the answers given by the user's perception and factual details. The user's perception makes the algorithm strong and memorable and prevents shoulder surfing which is the weakness of graphical passwords. In this algorithm, the idea of the user's perception provides the solution to a shoulder surfing attack. Also, the algorithm includes necessary steps to overcome a dictionary attack and a brute force attack for modern computers as well as supercomputers. We found it successful and secure after analyzing the computational speed of modern computers (8 core, 2.8 GHz) and a current supercomputer [15].

1.1 PRIMARY PURPOSE OF THESIS WORK.

According to Arash and his co-researchers the current graphical password methods require improvement through more research to achieve a high level of maturity and usefulness [8]. Similarly, the textual or alphanumeric passwords are also not fully safe, and textual passwords have many drawbacks including memorability issues as discussed in the introduction. Therefore, an idea has been developed to use graphics to generate textual input from the user based on the user's perception. Here the user's viewpoint is more important as this would randomize the overall password. As the user would not click or choose any graphics on the computer screen, the shoulder surfing attack would be almost negligible.

For a shoulder surfing attack, it is much easier to peer at someone's computer screen and observe the selected picture compared to noticing keystrokes. As graphical passwords provide better memorability compared to alphanumeric/textual passwords [1], a new idea of generating a textual password from graphics is proposed in this thesis. Further, as textual passwords have their drawbacks, to rectify those problems, a new idea is also developed to encrypt the generated textual password through the Whirlpool encryption technique.

At last, to make it more difficult, the encryption includes a new idea, to encrypt the whole textual password/string into chunks. Each chunk would be encrypted separately to generate a large number of characters as textual or alphanumeric passwords. The user is only required to remember his answer based on his perception. The primary objective in this study is to develop a new algorithm to generate a powerful password with better memorability using an advanced encryption method considering consistently increasing computational power as well as overcoming shoulder surfing attacks.

As graphical passwords provide better memorability compared to alphanumeric (textual) passwords, graphical passwords are chosen in this method for the sake of memorability [21, 16 and 17]. This objective is accomplished by understanding and analyzing various graphical password methods over time. Besides, various encryption methods have been learned with their vulnerabilities, and finally, the most advanced cryptography method, the Whirlpool encryption method, has been used in the new algorithm.

The new algorithm has been developed very carefully, and it has four steps in total. Each step of this new algorithm has been introduced to protect the method from various cyber-attacks. The first step of the new algorithm was introduced to generate the string based on the user perception of the images. This step is very to import as it randomizes the input and everyone has their own unique opinion, so the attacker would fall into the trap of his or her perception not matching in the shoulder surfing attack approach.

Further, this step not only includes graphical passwords but also provides questions to include alphanumeric answers from the users. As the alphanumeric passwords are harder to crack, this secured feature of the alphanumeric password has been used in this new algorithm in the first step to enhance the security of the new algorithm. In the second step, the letters are shifted based on the user's answers on accurate details based on questions in the first step. To do so, questions such as the user's birthdate and the user's father's birthdate have been asked in the first step. The responses of the user's answers to these questions are merged, and a large number is obtained. This number is divided by 26 to get the remainder. 26 is chosen as the divider because the English language has a total of 26 different characters. The remainder would be the number of shifts which would be applied on each letter in the same manner as the Shift Cipher cryptosystem. This step was introduced to protect the string from a dictionary attack.

In the third step, the string is divided into ten chunks because of the attackers' attacks on the whole chain rather than on individual fragments. As we have separated the chain into ten pieces, each chunk would need to be cracked by the attacker individually, and this becomes extremely difficult for the attacker. Therefore, in another way for the attacker, it is not the task to break one password but it is the task to break a series of ten different passwords secured through Whirlpool encryption as well as shift ciphers.

In step four, which is the last step of our algorithm, each chunk is encrypted separately through Whirlpool encryption, and then all encrypted output of length 128 characters are merged into one long password of 1280 characters. Thus, in this thesis, we proposed a new algorithm to generate the password for 1280 characters long, which is flexible because the total number of characters of the final password is adjustable in the algorithm.

As the graphical passwords provide better memorability [1], the graphical passwords are included in this algorithm for better memorability. On the other hand, alphanumeric answers are also taken into consideration from the user based on factual details from the user. These details are used to determine the number of shifts required to shift the characters. This shift number is obtained by dividing a total number of numerals by the total number of characters in English, i.e. 26. After the 26 characters the last character is pulled back to the first character of English. Therefore, it makes it more randomized as there would be 25 different remainders and the number of rotation shifts is not known to the attacker.

After shifting, the string is secured against the dictionary attack [42]. Further, the string is split into chunks, which makes it secured against a linearity attack as well. After this, the chunks are individually encrypted with Whirlpool encryption, which is exceptionally advanced, and no vulnerabilities are found till now in its encryption. After encryption, all the separate encryptions are merged to generate a long string, which can never be made by encryption of the original line. Therefore, the original string is encrypted into different parts, and then encrypted portions are merged in the end.

1.2 Scope

In this thesis, graphical authentication techniques have been investigated which are developed over time. Graphical authentication has been chosen in this thesis for better memorability over textual passwords [1]. This thesis focuses on the shoulder surfing attack for Graphical Authentication. To overcome a shoulder surfing attack, a new idea of user perception as textual input has been introduced and this thesis concentrates on the user's data based on the opinion as well as factual and confidential details of the user.

This thesis also concentrates on potential threats such as a dictionary attack and those have been taken into consideration while developing this new algorithm. In addition to graphical authentication, user perception, and user's textual inputs, in this thesis, various encryption methods have been studied along with their weaknesses and based on all these studies, a new algorithm has been developed. At the end, the computational time is calculated for a brute force attack by modern computer as well as a supercomputer. This thesis focuses on various aspects such as previous studies of graphical authentication, encryption techniques and their vulnerabilities and the new algorithm which focuses on both graphical authentication as well as encryption methods.

1.3 Previous Work

Graphical password related analysis and various encryption techniques have been researched in this thesis. The existing research related to graphical passwords and encryption techniques is presented below.

Susan Wiedenbeck et al. [1] developed one system (named as Pass Points) as an alternative to alphanumeric passwords to authenticate users through graphical passwords. In this research memorability, tolerance and margin of error are also analyzed.

G. Agarwal et al. study graphical passwords and textual passwords and mention that graphical passwords provide better memorability compared to textual or alphanumeric passwords [9].

Coventry et al. published that textual passwords are vulnerable to shoulder surfing, brute force attack, key-logging, and many other threats. Textual passwords are less memorable, and graphical passwords can be an alternative for textual passwords as humans tend to remember graphics better than text [3].

In her paper "Authentication Using Graphical Passwords: Effects of Tolerance and Image Choice," Susan provided many details about authentication related with graphical passwords and its tolerance as well as image choice [16].

Sonia Chisson et al. noted that some security vulnerabilities are common to most recall-based systems, and its reason is sharing similar kinds of features by these systems [26].

Dunky et al. found the success rate of the Draw A Shape (DAS) method, and it was 57 to 80%. They also introduced the Background-Draw-A-Shape method (BDAS) for graphical authentication [34].

William Stallings produced his research paper "The Whirlpool Secure Hash Function."

Sadaqat Ur Rehman et al. published a research paper named "Comparison Based Analysis of Different Cryptographic and Encryption Techniques Using Message Authentication Code (MAC) in Wireless Sensor Networks (WSN)" which is very important as it is providing the comparison and analysis of various cryptographic and encryption techniques [35].

Lars Knudsen et al. presented a paper on MD2 encryption and more specifically about collision and preimage attacks on it [36].

In 2003, Bart Preneel presented a paper about Analysis and Design of Cryptographic Hash Functions [37].

In 2003, GIAC Certifications published a paper “A Guide to Hash Algorithms” to analyze and study the Hash algorithm in detail [38].

B. Brumen and co-researchers published a paper on the dictionary attack entitled “Brute-force and dictionary attack on Hashed real-world passwords” in May 2018.

F. Craik et al. published an article in The Journal of Learning Psychology about memory and cognition [29].

The Design and Analysis of Graphical Passwords based papers were published by Ian Jermyn et al. [22].

Karen Renaud, Rob Jenkins, and Jane McLachlan published the paper for familiarity-based graphical authentication [24].

1.4 Thesis Contribution and organization

1.4.1 Contribution

In this thesis, the mission was to provide a better password which would be extremely difficult to compromise by attackers, modern computers and a supercomputer; however, at the same time, we also wanted to provide better memorability. As the graphical passwords provide better memorability [1], the graphical authentication has been taken into consideration to generate secure passwords to reduce the burden on the user of remembering a long password. Therefore, various graphical authentication papers were investigated and analyzed carefully, and we developed the concept of human perception to make the input extremely random as well as to negate a shoulder surfing attack.

After choosing the graphical images as part of the inputs for the factors of the string, a few questions are also added to generate alphanumeric responses from the user based on the confidential details of the user. The idea was to create a number string to get the remainder when divided by the total number of characters in English, i.e., 26. After this, the string characters are shifted by the places of the remainder to protect the password from a dictionary attack.

Every step in the new algorithm was developed very carefully and for a purposeful reason to negate a potential attack on the algorithm. In this thesis, every step is included in the new algorithm very carefully and for a specific reason to overcome potential vulnerabilities existing in previous authentication methods. At the end we developed our password which was always the same for the same input and based on the current computational speed of modern computers (8 core, 2.8 GHz) and a supercomputer; our generated password is secured for millions and billions of years.

1.4.2 Organization

Chapter 1 is the introduction of this thesis. It covers details related to the primary purpose of this thesis, scope, previous related work, and thesis contribution with the organization. This chapter gives a good overview of the thesis.

Chapter 2 includes details of Graphical Authentication techniques, which focus on Grouping, Moving locations, Disguising, Cued Recall System, etc. in particular. This chapter concentrates on previous studies of graphical authentication, which are suggested by various researchers. However, despite the work of these various researchers, a shoulder surfing attack is difficult to prevent.

Chapter 3 focuses on encryption methods such as shift ciphers, affine ciphers, the Vigenere Cipher, and the Substitution Cipher. This chapter focuses on one of the important phases of the encryption period where many encryption techniques were developed and compromised by attackers with various tactics. This is more important to understand since attackers have successfully compromised all encryption methods except Whirlpool encryption.

Chapter 4 describes DES and AES cryptosystems and their weaknesses. DES (Data Encryption Standard and AES (Advanced Encryption Standards) are public encryption techniques, and they were developed as suggested by NIST. However, despite their strong encryption methods, they have been compromised successfully, and this chapter focuses on attack methods as well.

Chapter 5 includes details about Hash Functions -- their overview, efficiency, and weakness. After the DES and AES encryption, the researchers developed a Hash Function, which is also known as a one-way function. This chapter focuses on Hash Function structure and its efficiency, etc.

Chapter 6 is about Whirlpool Encryption and focuses on all details of Whirlpool Encryptions such as its structure, algorithm tasks, Block Cipher W, its layers, and performance of Whirlpool Encryption. This chapter contains details of Whirlpool encryption in extreme detail. This is one of the very important chapters of the present thesis.

Chapter 7 describes the proposed new algorithm and focuses on all its four steps. The chapter focuses on four steps: (1) generating the string through user input based on perception as well as factual and confidential details; (2) shifting of the characters with the remainder generated in the algorithm based on the user's answers; (3) dividing the string into ten parts and encrypting the each part through Whirlpool encryption; and (4) merging all encrypted outputs into one unique big password with extreme strength.

Chapter 8 provides details on why only Whirlpool encryption has been chosen in this thesis. This chapter focuses on the strengths of the Whirlpool encryption and why only the Whirlpool encryption was selected for this new algorithm. This chapter describes the strengths of Whirlpool encryption which the other encryption techniques are unable to offer.

Chapter 9 discusses computational speed of modern computers and supercomputer to break the password. This chapter provides details about the computational speed and the enhancement of the microprocessor's efficiency. This chapter focuses on the time period from a few decades and provides information about how computational power has increased exponentially since its inception and is still continuing to increase.

Chapter 10 focuses on the attack through modern computers and supercomputer on this thesis outcome. Further, the chapter also concentrates on the time period required for the current password patterns to be compromised by the modern computer and the super computer. This chapter demonstrates that the present research is sound and provides an enhanced solution which is extremely safe and secure compared to the present password techniques.

Chapter 11 concludes the entire thesis and provides details about the scope of future work. This chapter outlines for researchers to upscale the new algorithm to a more advanced level and, therefore, makes recommendations for future research to enhance the performance of the algorithm

In the end, all the research articles, websites, journal papers etc. are mentioned in the chapter named references. These details are provided for future researchers to understand the cohesion of the current thesis and to learn and understand the current thesis in a better way as the references have played a great role in developing this thesis.

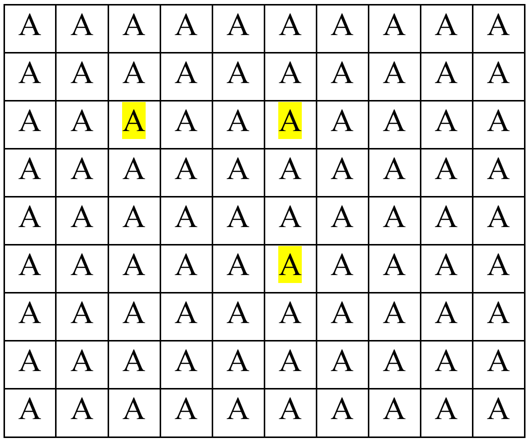
CHAPTER 2

GRAPHICAL AUTHENTICATION TECHNIQUES

Graphical passwords are secure to remember compared to complex alphanumeric passwords [21, 16, and 17]. Therefore, picture passwords were offered by many researchers [16, 17, 18, and 10], but they are vulnerable to over the shoulder surfing attacks [2, 10]. Picture passwords are susceptible to this attack. On the other hand, alphanumeric passwords provide higher security compared to picture passwords, but they are challenging to remember when they have a more significant number of characters (Picture Passwords Superiority and Picture Passwords Dictionary Attacks). For the solution of shoulder surfing attack for picture passwords, the following alternatives have been suggested, but they are still not efficient [19, 10].

2.1 Grouping

Grouping actual password-pictures among other non-password pictures. The method proposed for finding target images mentally assumes the image and then selects the distractor in the image, but it is still vulnerable. All in all, the idea is to distract the attacker with other images.

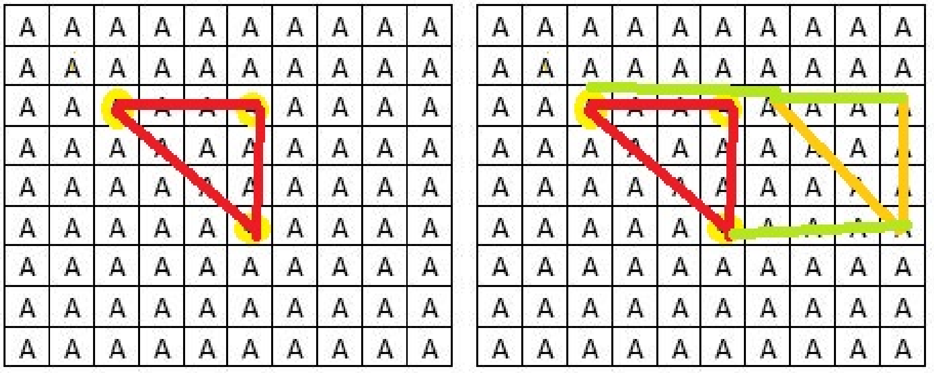


A	A	A	A	A	A	A	A	A	A
A	A	A	A	A	A	A	A	A	A
A	A	A	A	A	A	A	A	A	A
A	A	A	A	A	A	A	A	A	A
A	A	A	A	A	A	A	A	A	A
A	A	A	A	A	A	A	A	A	A
A	A	A	A	A	A	A	A	A	A
A	A	A	A	A	A	A	A	A	A
A	A	A	A	A	A	A	A	A	A

Figure 1: Grouping scheme (Finding the targets).

2.2 Moving to other locations

Rohit Khot and his co-researchers presented an idea to move the password point from one point to another position, but this alternative also didn't work to protect from a shoulder surfing attack. This scheme was introduced by Bianchi et al. to move the targets to a different location instead of just clicking on the targets [10].



[23]

Figure 2: Grouping Scheme (Moving the targets).

2.3 Disguising

Find and select the first picture password, and then choose the second target and the third one. So, follow the chronological order of the pictures. Which also didn't provide better security. In this method, it is expected from the user to find the targets, and mentally discard the part of the picture which does not contain the target and click the result on the new locations.

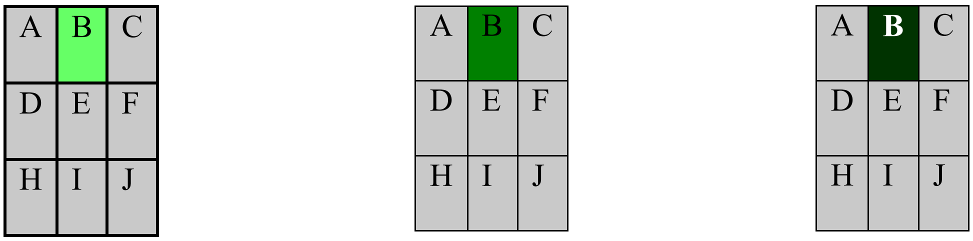


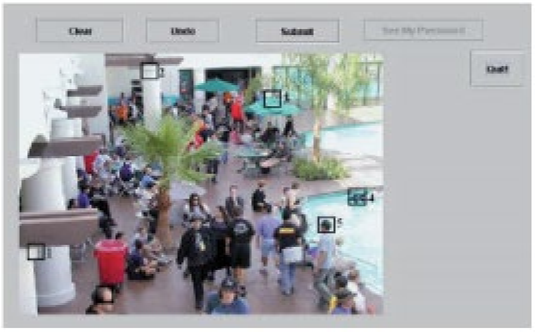
Figure 3: Disguising the target[24].

This method was proposed by Karen Renaud, Rob Jenkins and Jane McLachlan and the idea was to disguise the color of the object placed among other distractors. It relied on the user's ability to identify the correct target among the distractors [24].

2.4 Cued Recall System

This method needs the users to remember specific locations and target them. This method was introduced to decrease the memory load on people. This system is given the name "Loci metric" [25]. According to Hollingsworth and Henderson [27], if the users initially concentrate on an image, they may remember specific parts of that picture in the form of their password.

“The schemes discussed next share a vulnerability to shoulder surfing and malware and are vulnerable to MITM phishing attacks similar to recognition-based schemes. To capture a click-based graphical password using malware, a mouse logger may suffice if the attacker can also determine the position of the image on the screen. Alternatively, a screen scraper may identify the image location and be sufficient if the attacker can identify when the user clicked the mouse button (some users very familiar with their password may not necessarily stop moving the cursor while clicking). Shoulder surfing may also reveal a user’s password in a single login, as the entire password may be observable on the screen as the user enters it” [26]



[26]

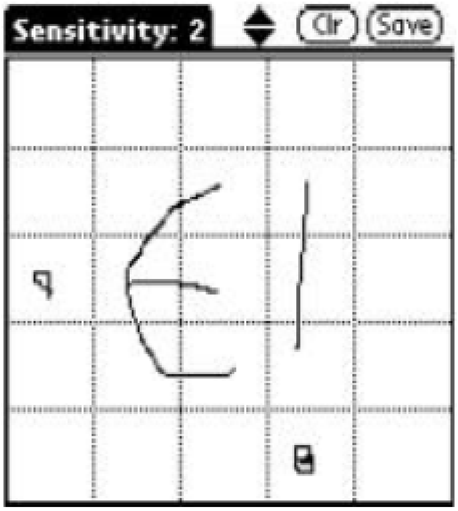
Figure 4: Pass-points password example.

2.5 Recall-Based Systems:

These systems are also known as draw-metric systems [28]. This kind of system requires the user to reproduce a deep drawing by recalling it. This recalling is done without any help such as memory prompts or cues, and therefore recalling is difficult [29]. The recall based system is described in detail in this chapter.

2.5.1 DAS (Draw A Secret):

DAS was the first recall based picture authentication system proposed in 1958[30]. In this method, the users were supposed to draw their design-password on a two-dimensional grid as shown in figure 5[26]. In this method, the user can draw a continuous pen stroke or multiple pen strokes which restart the next stroke in a different cell of the grid. For complexity, the user can choose the unusual shape of the doodle; however, this method was limited to a small network, and it was still vulnerable to over the shoulder attacks.



[26]

Figure-5: DAS (Drawing a Secret).

2.5.2 BDAS (Background Draw A Secret):

The BDAS technique was proposed by Dunphy et al. [31]. In this method, a background image was introduced to generate more difficult passwords. This method is developed from the DAS which is Draw a Secret method. The DAS method is applied on a background picture. BDAS has been described in figure 6. Background Draw A Secret method is one of the methods of a recall based system. Background Draw a Secret method is an enhancement of the Draw A Secret method which is also one of the recall methods.

[12]

Figure-6: Sample BDAS Grid.

The idea was to provide cued recall through a drawing grid as well as a background image. In this method, the chosen image needed to be chosen carefully depending on the number of potential hot spots available [32]. The difference between BDAS and DAS is only the background image; the rest is similar to graphical passwords. The most significant difference is providing cues not only from the grid but also from the background, which was not possible in DAS due to the plain background.

2.6 Inkblot Authentication Method:

This method is not an ardently graphical authentication method. This method relies on the cue provided by blurred images. In this method, users are shown inkblots to remember, and the users are asked the first and last character of the word which represents the inkblot. The location of the inkblots would also change among each other, and users generally remember the correct inkblot cue. Inkblot authentication has been described in figure 7.

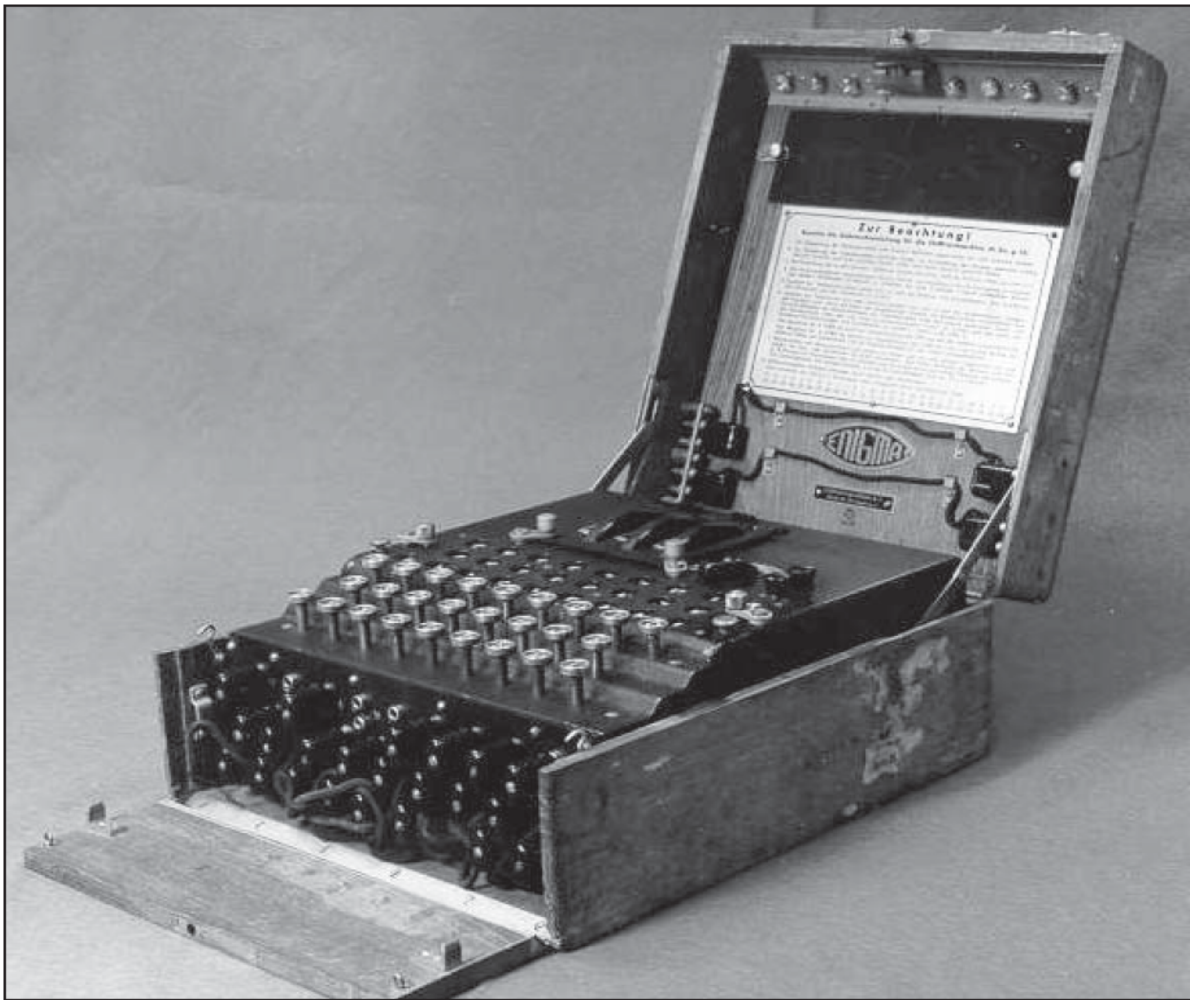
[26, 33]

Figure-7: Sample inkblot authentication image.

CHAPTER 3

ENCRYPTION METHODS

Encryption methods have been developed over decades and were used at the end of World War 1. In 1925, the German Army bought many cipher machines, and they were named Enigma. The German scientist Arthur Scherbius had invented the German Enigma Machine at the end of World War I. The later Enigma machines were developed by many other researchers.

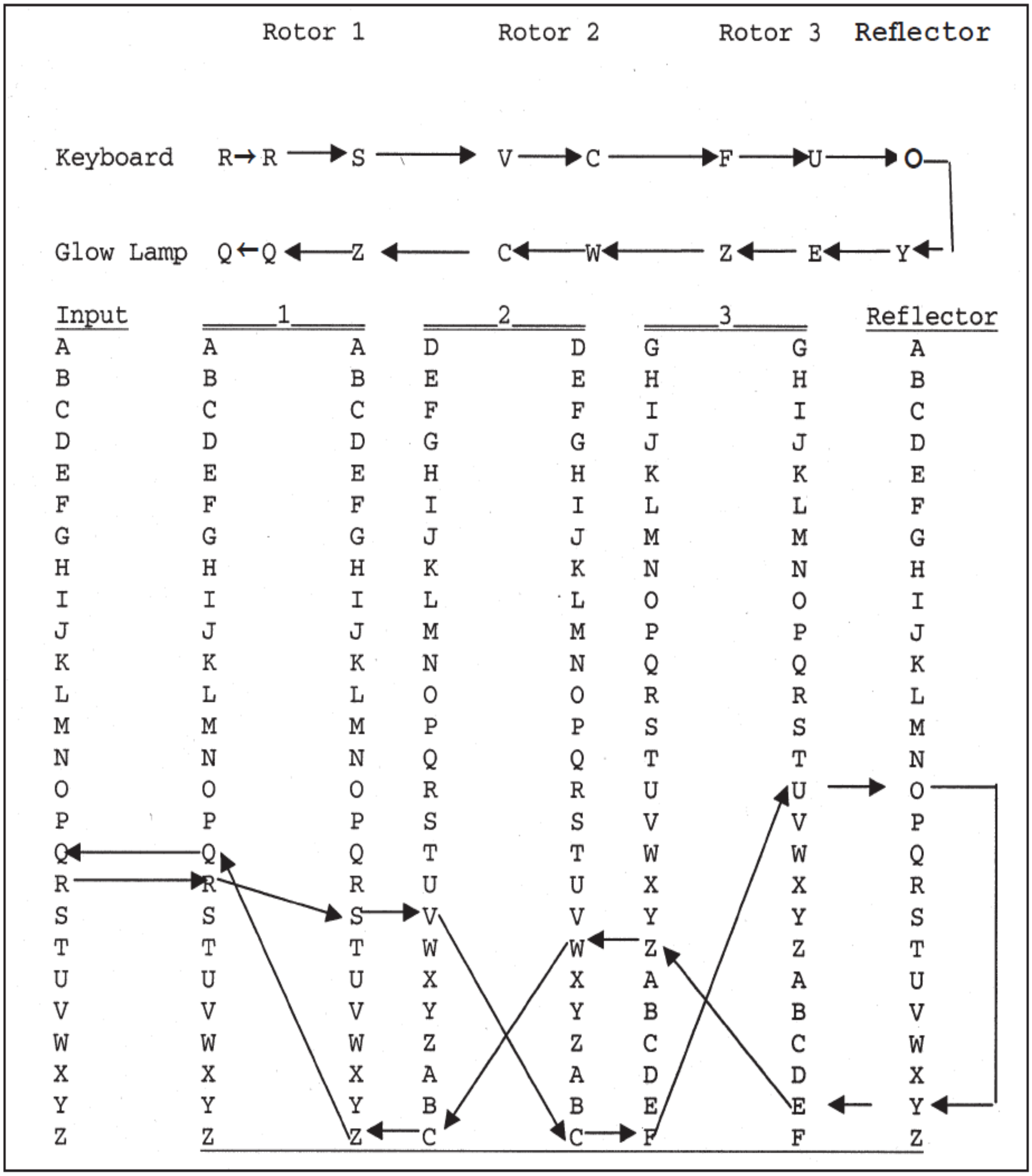


[43]

Figure 8: German Enigma Machine.

There were a few rotors based on the type of cipher machine (figure 9). These rotors were installed in such a way that they can represent a different character for each given input character.

Input characters are called plain text, and encrypted characters are named Cipher text. This machine is arranged to encrypt the plain text "R" as "Q." This kind of encryption method has been developed over time. Many encryption techniques have been developed over time, and their brief details are included here.



Input	1		2		3		Reflector
A	A	A	D	D	G	G	A
B	B	B	E	E	H	H	B
C	C	C	F	F	I	I	C
D	D	D	G	G	J	J	D
E	E	E	H	H	K	K	E
F	F	F	I	I	L	L	F
G	G	G	J	J	M	M	G
H	H	H	K	K	N	N	H
I	I	I	L	L	O	O	I
J	J	J	M	M	P	P	J
K	K	K	N	N	Q	Q	K
L	L	L	O	O	R	R	L
M	M	M	P	P	S	S	M
N	N	N	Q	Q	T	T	N
O	O	O	R	R	U	U	O
P	P	P	S	S	V	V	P
Q	Q	Q	T	T	W	W	Q
R	R	R	U	U	X	X	R
S	S	S	V	V	Y	Y	S
T	T	T	W	W	Z	Z	T
U	U	U	X	X	A	A	U
V	V	V	Y	Y	B	B	V
W	W	W	Z	Z	C	C	W
X	X	X	A	A	D	D	X
Y	Y	Y	B	B	E	E	Y
Z	Z	Z	C	C	F	F	Z

[43]

Figure 9: Sample Enigma Type Encryption Machine.

3.1 Shift Cipher:

This crypto technique is also known as Julius Caesar. In this technique, all the letters are shifted by a fixed number (shift). In this method, all the characters are shifted based on the shift and the last character would be shifted to the beginning. The shift can be any number, but any number higher than 26 is just repetition as the shift would again start from the beginning from 26 as there are a total of 26 characters only in the English alphabet.

For example, for the word AKASH and shift 1, "A "would be replaced by "B', "K" by "L," "A" by "B," "S" by "T," "H" by "I."

For the same word AKASH, the shift of 27, 53 would populate the same result.

This encryption can be exercised by $X \rightarrow X + K \pmod{26}$.

Weakness: This is a weak encryption method. It just requires permutation and combination of the 26 characters, and the cipher text would be immediately decoded without knowing the shift number.

3.2 Affine Ciphers:

In this Affine ciphers, two characters α and β were introduced in the above formula. It is required that the greatest common divisor of α and β has to be one only.

The formula for affine ciphers can be written as $X \rightarrow \alpha X + \beta \pmod{26}$.

Similar to the Shift cipher, the last character is linked with the beginning which means, as described for Shift ciphers, this encryption is also mod 26.

For example, the word "FINE," "F" would be encrypted as "V," "I" as "W," "N" as "P," and "E" as "W." Thus, "FINE" would be encrypted as "VWPM" after being encrypted from the Affine cipher text.

Weakness: This cryptosystem is vulnerable. This cryptosystem is based on the pair of (α, β). As we have only 26 characters (which is β), there are only 12 possible alternatives for α where the greatest common divisor with 26 characters would be 1. Therefore, total choices would be 26*12 = 312 for the key.

Attack through Cipher Text only: If an attack would be launched by the computer with all 312 keys, it would take no longer for the computer to decode cipher text. This attack is called known as a cipher text attack. For launching this attack the attacker has to access the encryption machine and derive the key in order to compromise security. This kind of attack is very simple to launch if an attacker gets access to an encryption machine.

Attack through Known Plain Text: This approach requires only a few attempts to know the two letters of plain text, and the key can be retrieved through this. For example, if a sentence starts or ends with FINE and the corresponding Cipher text is VWPM, analyzing any two characters would give us the value of α and β as follows,

F → α (F) + β ➔ which turns to be, $6 = 6\alpha + \beta$

I → α (I) + β ➔ which turns to be, $8 = 8\alpha + \beta$

Here it is important to note that, solving these two equations would give the value of α and β.

Attack through Chosen Plain Text: For the "ab" as input, the cipher text would be $\alpha(0) + \beta$, which would reveal the value of β, and once the value of β is known, by applying the above equations, the value of α can be found. Here, the attacker has access to input the fake plaintext into the machine. Here, as previously mentioned, the values of α and β play a very important role and can be obtained by choosing specific plain text. Chosen plain text requires access to the encryption machine. This attack cannot be launched without access to the encryption machine

Attack through Chosen Cipher text: In this type of attack it is assumed that the attacker has access to the encryption machine to choose the cipher text. Therefore, to launch this attack, specific cipher texts are chosen, such as, if input would be fed as "AB," it would yield αX + β, and the decryption key would be exposed.

3.3 The Vigenere Cipher:

The Vigenere Cipher was invented in the 16th century. In this method, the security is based on the randomness of the keyword and key length. In this cryptosystem, a keyword is chosen, and its characters are given a number from 1 to 26, and then these numbers are applied as the shift on each character of the plain text. Often such a keyword is known as a vector.

For example, the keyword "vector" itself would be a key as (21,4,2,19, 14,17), and each character would be shifted with a corresponding shift to the vector.

The plain text, “ I am good ” can be encrypted as :

Plain Text: "I a m g o o d."

Shift (Key): 21 4 2 19 14 17 21

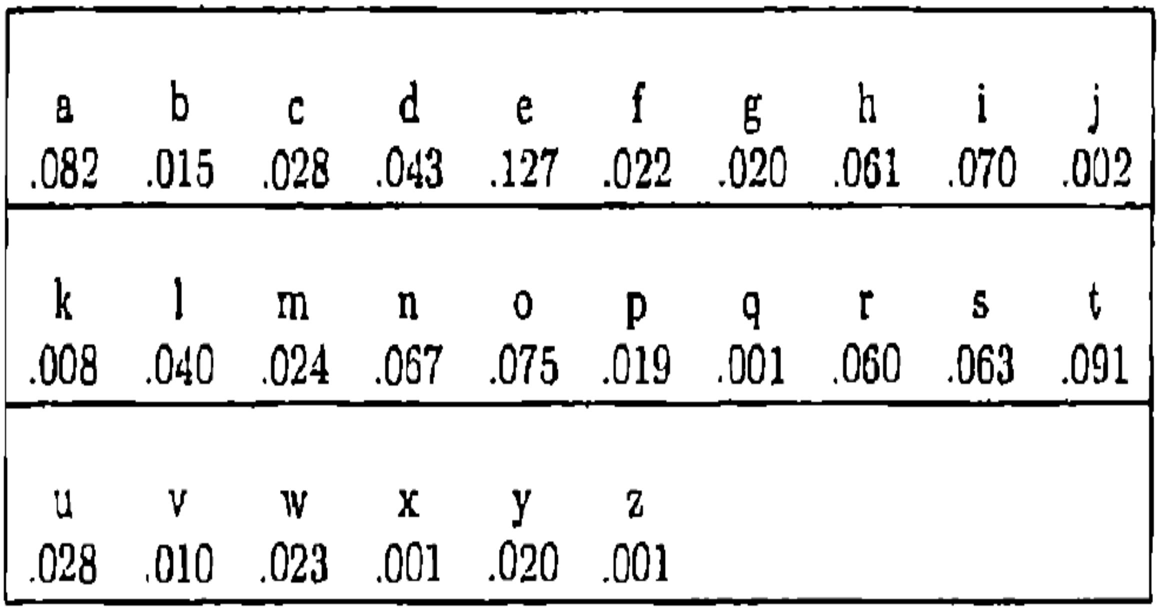
Cipher text: "d e o z c f y"

Weakness: Similar to the previously discussed vulnerable encryption methods, this cryptosystem is also not safe and vulnerable to various attack methods. The weaknesses are mentioned below. Weaknesses include attack through known plain text, attack through chosen cipher text, & cryptanalysis attack.

Attack through known plain text attack: A known plain text can be launched on this encryption method to decode the cipher text. For example, feeding all characters as "aaaaa….", immediately reveals the key. No additional efforts are required to crack the cipher text.

Attack through chosen cipher text: For example, a cipher attack that selected "AAA…." would expose the negative of the key. For the attacker to launch this attack, some selected cipher texts are chosen. For example, if input is "AB," the output would yield αX + β, and the decryption key would be exposed. Therefore, this is called a chosen cipher text attack.

Cryptanalysis Attack: In this attack, the attacker only requires cryptanalysis. As we know, in English almost all characters have different frequencies. In 1982, Beker Piper mentioned this method in the book *Cipher Systems about Cryptanalysis*.

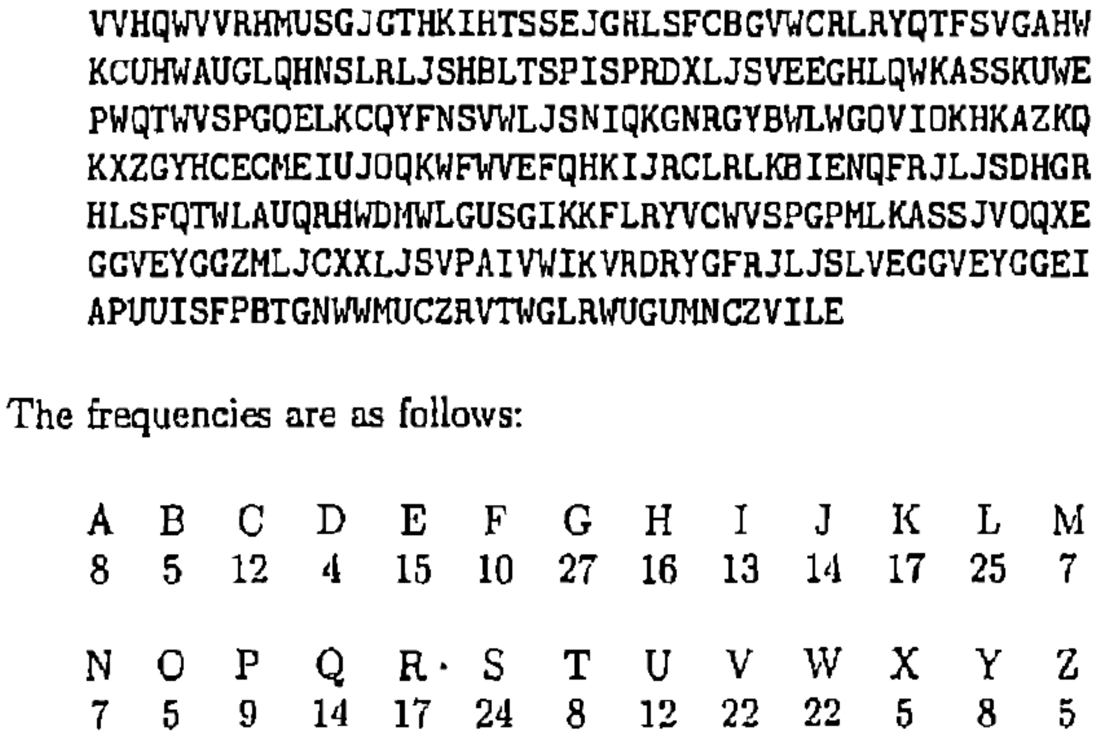


a	b	c	d	e	f	g	h	i	j
.082	.015	.028	.043	.127	.022	.020	.061	.070	.002
k	l	m	n	o	p	q	r	s	t
.008	.040	.024	.067	.075	.019	.001	.060	.063	.091
u	v	w	x	y	z				
.028	.010	.023	.001	.020	.001				

[44]

Figure 10: Frequencies of letters in English.

The frequencies of all the letters in English can provide analysis to help break this cryptosystem. The frequencies are more important as they provide a rough estimation of all characters possibly encrypted in the coded message. The important character in this figure is the letter "e" which has the highest frequency among all the characters. The frequency of "e" is demonstrated in figure 11.



```
VVHQWVVRHMUSGJGTHKIHTSSEJGHLSFCBGVWCRLRYQTFSVGAHW
KCUHWAUGLQHNSLRLJSHBLTSPISPRDXLJSVEEGHLQWKASSKUWE
PWQTWVSPGOELKCQYFNSVWLJSNIQKGNRGYBWLWGOVIOKHKAZKQ
KXZGYHCECMEIUJOQKWFWVEFQHKIJRCLRLKBIENQFRJLJSDHGR
HLSFQTWLAUQRHWDMWLGUSGIKKFLRYVCWVSPGPMLKASSJVOQXE
GGVEYGGZMLJCXXLJSVPAIVWIKVRDRYGFRJLJSLVEGGVEYGGEI
APUUISFPBTGNWWMUCZRVTWGLRWUGUMNCZVILE
```

The frequencies are as follows:

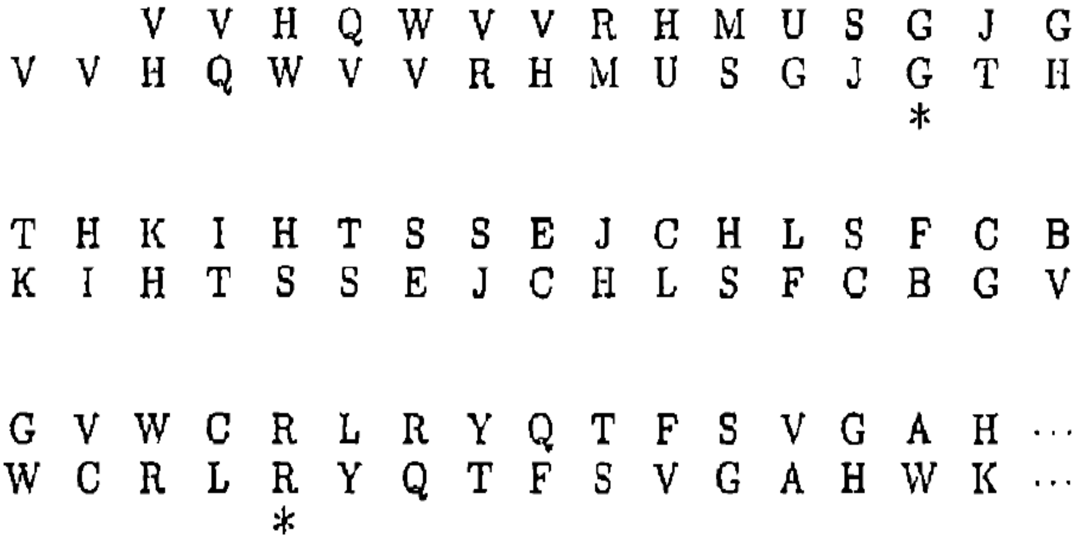
A	B	C	D	E	F	G	H	I	J	K	L	M
8	5	12	4	15	10	27	16	13	14	17	25	7
N	O	P	Q	R·	S	T	U	V	W	X	Y	Z
7	5	9	14	17	24	8	12	22	22	5	8	5

[44]

Figure 11: Cryptanalysis.

Now, it is necessary to find the key length; for this, the string must be compared with its own each time by shifting one place, and the coincidences (each time a letter is the same while comparing a string), are depicted with * in figure 12.

For doing so, the strings are being written on a couple of pieces of paper, and then one of the papers is moved onto the other paper to move and compare the strings with each other. This step is repeated again and again until all coincidences are determined. Moving papers like this is also known as displacing papers, and the shift is known is as displacement. Table 1 is very important as it provides details related to displacement and coincident.



```
    V V H Q W V V R H M U S G J G
V V H Q W V V R H M U S G J G T H
                            *

T H K I H T S S E J C H L S F C B
K I H T S S E J C H L S F C B G V

G V W C R L R Y Q T F S V G A H ...
W C R L R Y Q T F S V G A H W K ...
        *
```

[44]

Figure 12: Breaking Vigenere Cipher

Here, after continuing displacements of strings 14 times, the observations are as follows,

Displacement	1	2	3	4	5	6
Coincidence	14	14	16	14	24	12

Table 1: Displacement and Coincidence.

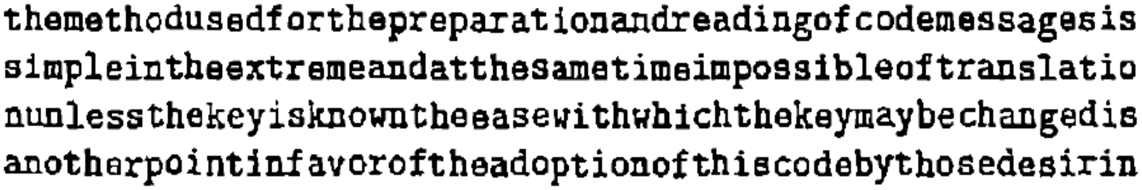
Now, for finding the key, we would assume the key length to be five as there is a maximum number of coincidences at key length 5.

Here, in the Cipher text, the significantly high frequencies characters are as below. As in the English language, the frequency of “E” would be generally high; therefore, it is important to investigate E. However, other than “E” it is also advisable to look for other English vowels. It is important to analyze and study table 2 to understand the frequencies of characters. Table 2 below explains the frequencies of L, H, R and V.

Character	L	H	R	V
Frequency	10	5	5	8

Table 2: Characters with higher frequencies.

It is necessary to consider each character as "E" and link the other letters in their alphabetical order one after another for each combination of this table until a meaningful plaintext is decoded. After doing this, as mentioned earlier, the vector (key) is {2, 14, 3, 4, 18}, and by applying this key to the cipher text, the plain text can be decrypted as shown in figure 13.



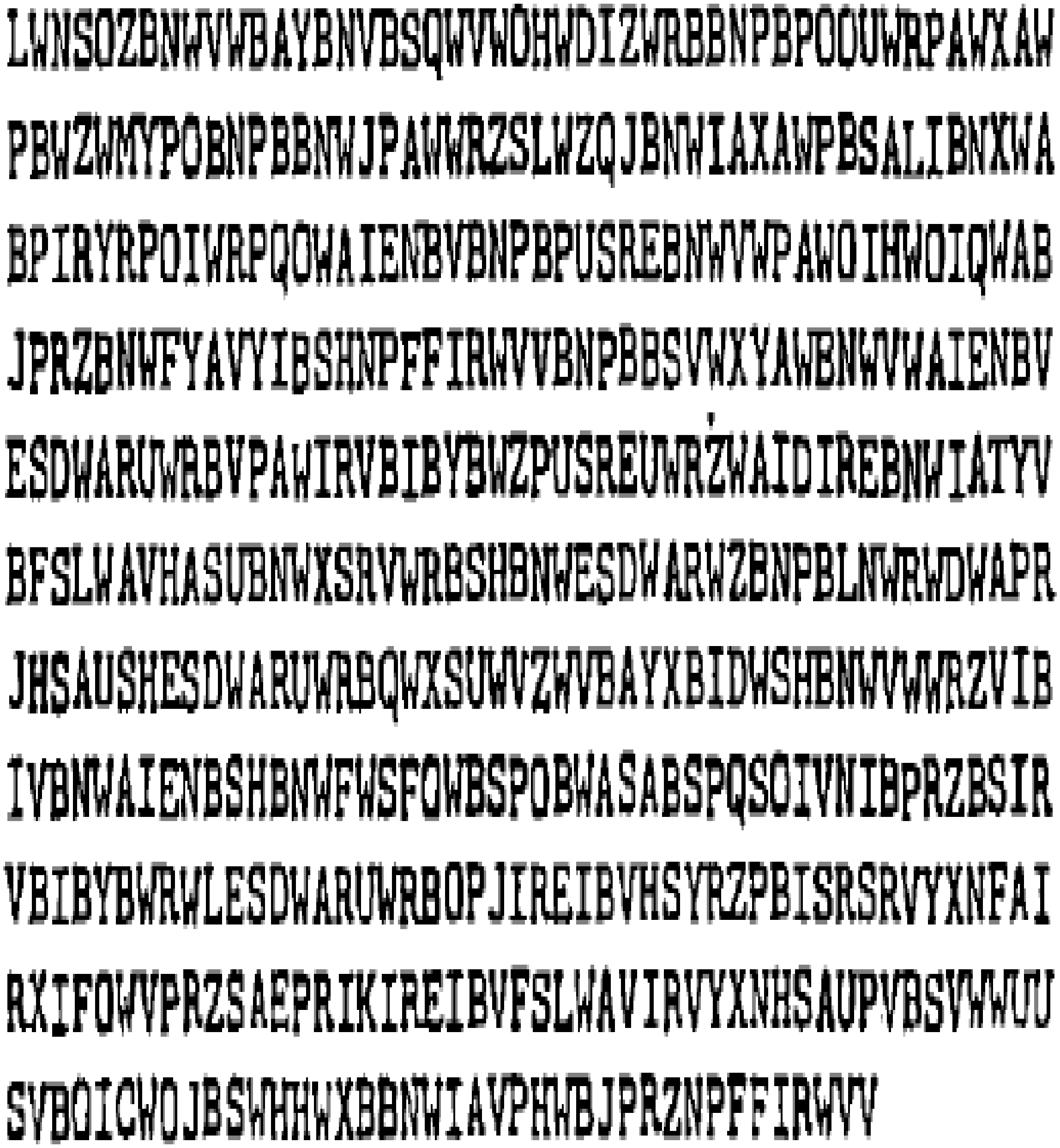
themethodusedforthepreparationandreadingofcodemessagesis
simpleintheextremeandatthesametimeimpossibleoftranslatio
nunlessthekeyisknowntheeasewithwhichthekeymaybechangedis
anotherpointinfavoroftheadoptionofthiscodebythosedesirin

[44]

Figure 13: Decoded plain text.

3.4 Substitution Ciphers

In this cryptosystem, all letters are replaced with different letters, and sometimes some of the letters are not replaced to make it more complicated. In this method, frequency analysis can be vulnerable to exposing the cipher text and decoding the plain text. For example, for the passage in figure 14, frequency analysis can be a threat to the plaintext. In this cipher text method all the characters in English are substituted with any randomly picked characters from the English alphabet. To understand this fully, it is important to study and analyze figure 44, which provides a sample image of an encrypted message decoded later in this chapter.



```
LWNSOZBNWVWBAYBNVBSQWVWOHWDIZWRBBNPBPOOUWRPAWXAW
PBWZWMYPOBNPBBNWJPAWWRZSLWZQJBNWIAXAWPBSALIBNXWA
BPIRYRPOIWRPQOWAIENBVBNPBPUSREBNWVWPAWOIHWOIQWAB
JPRZBNWFYAVYIBSHNPFFIRWVVBNPBBSVWXYAWBNWVWAIENBV
ESDWARUWRBVPAWIRVBIBYBWZPUSREUWRZWAIDIREBNWIATYV
BFSLWAVHASUBNWXSRVWRBSHBNWESDWARWZBNPBLNWRWDWAPR
JHSAUSHESDWARUWRBQWXSUWVZWVBAYXBIDWSHBNWVWWRZVIB
IVBNWAIENBSHBNWFWSFOWBSPOBWASABSPQSOIVNIBPRZBSIR
VBIBYBWRWLESDWARUWRBOPJIREIBVHSYRZPBISRSRVYXNFAI
RXIFOWVPRZSAEPRIKIREIBVFSLWAVIRVYXNHSAUPVBSVWWUU
SVBOICWOJBSWHHWXBBNWIAVPHWBJPRZNPFFIRWVV
```

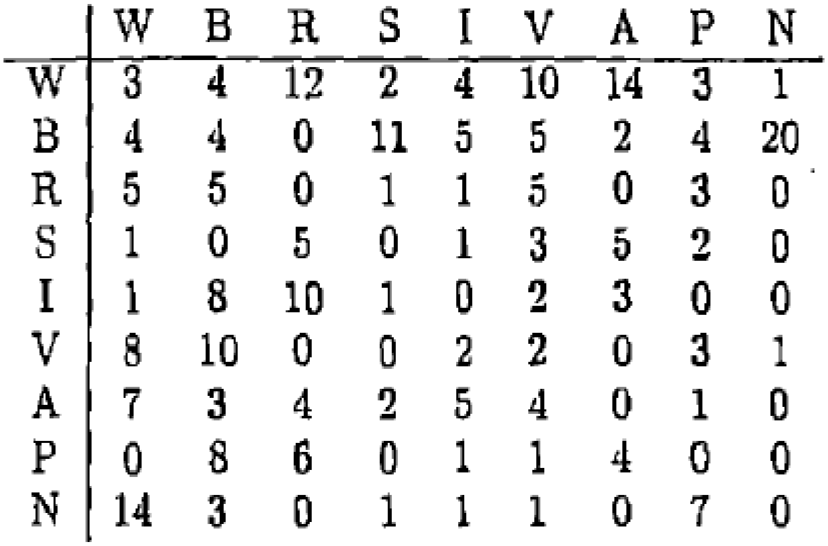
[44]

Figure 14: Sample encrypted passage

W	B	R	S	I	V	A	P	N	O
76	64	39	36	36	35	34	32	30	16

Table 3: Frequently used characters.

The frequency analysis of frequently used characters is mentioned in table 3, and, to decode it, the frequency analysis for each character with another character (pair) can be determined as shown in figure 15.



	W	B	R	S	I	V	A	P	N
W	3	4	12	2	4	10	14	3	1
B	4	4	0	11	5	5	2	4	20
R	5	5	0	1	1	5	0	3	0
S	1	0	5	0	1	3	5	2	0
I	1	8	10	1	0	2	3	0	0
V	8	10	0	0	2	2	0	3	1
A	7	3	4	2	5	4	0	1	0
P	0	8	6	0	1	1	4	0	0
N	14	3	0	1	1	1	0	7	0

[44]

Figure 15: Matrix analysis.

After this, the knowledge of the language and frequency analysis can be used to review the plain text as “We hold these truths to be self-evident that all men are created equal that they are endowed by their creator with certain unalienable rights that among these are life liberty and the pursuit of happiness that to secure these rights governments are instituted among men” [44].

Block Ciphers: In all of the above methods, cryptanalysis was one of the successful attack methods as the specific cipher character was coming from one particular plain text only,which made it possible to decode not only that character but also the other character by analyzing the cryptanalysis. Therefore, to protect from cryptanalysis, the block ciphers were developed in such a way that if one character were changed, the whole block would be affected. Thismakes it more difficult to crack the cipher text using cryptanalysis.

CHAPTER 4

DES and AES Cryptosystems

4.1 Overview

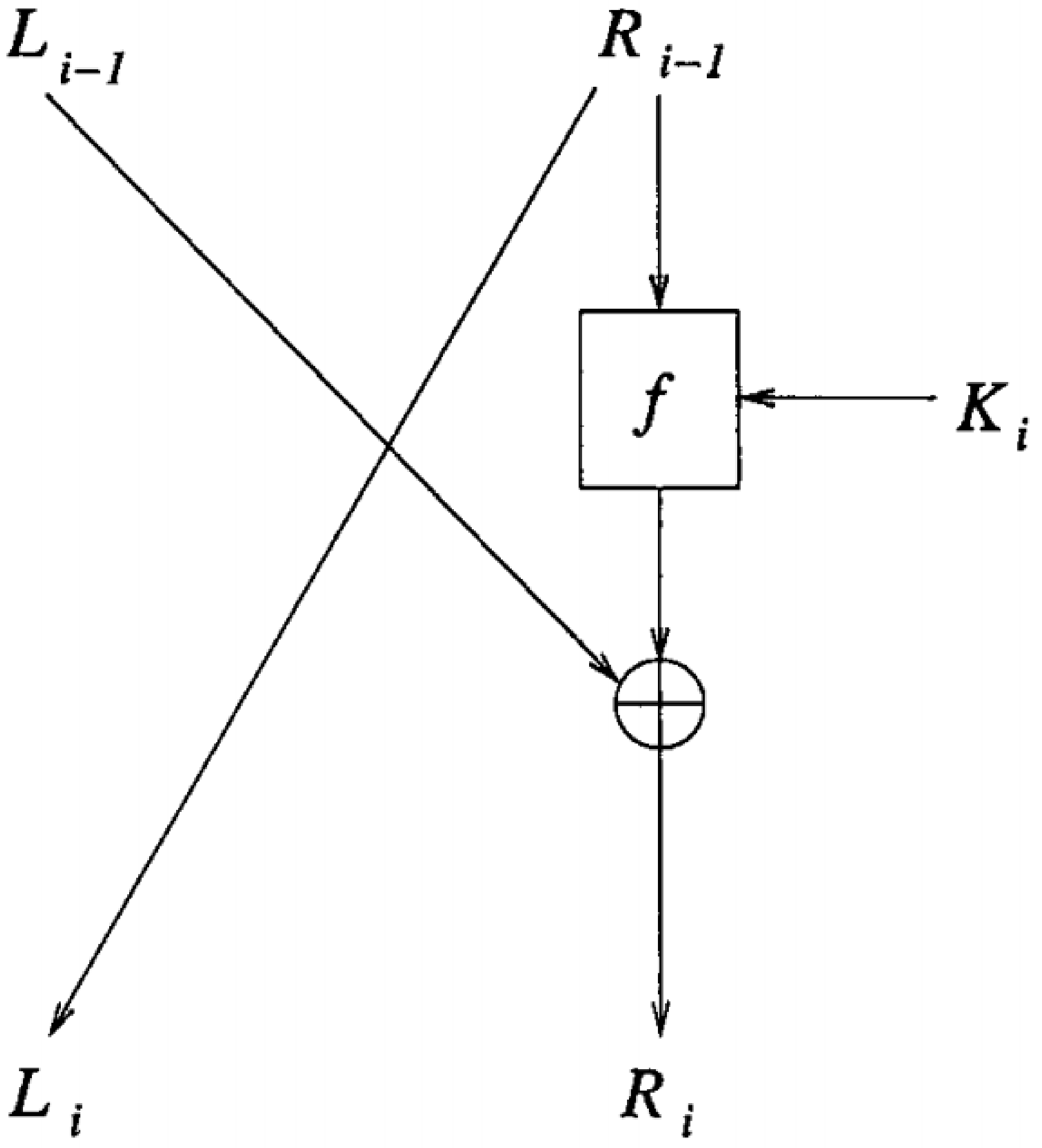
DES (1973) and AES (1997) are block ciphers. DES stands for Data Encryption Standards, and AES stands for Advanced Encryption Standards. DES is a symmetric key cryptosystem. Originally the DES was introduced with 56 bits key size. It was sufficient enough until the computational power was not sufficient enough to launch a successful brute force attack. as the computational power increased over the period, DES became vulnerable and gradually obsolete.

AES is a symmetric key encryption. It has three different versions based on the key length. It can have a key length of 128, 192 and 256 bits. DES and AES have different Block Size. DES has a Block Size of 64 bits whereas AES has a Block Size of 128 bits. Security wise, DES has been proven inadequate, and AES is considered more secure compared to DES mainly because of the larger key space.

The primary difference between DES and AES is that in DES the data block is cut into two parts whereas in AES the whole data block is considered as one single matrix. Based on speed, DES is comparatively slow compared to AES encryption. Lastly, DES works on Feistel Cipher structure whereas AES is based on the substitution and permutation principle. DES and AES both are considered very important encryptions of their time. AES and DES have been explained in detail with their weaknesses in this chapter. AES and DES were researched and developed as recommended by the NIST (National Institute of Standards and Technology). Both of these private key cryptosystems are almost obsolete for usage due to the successful attacks on these encryption methods by many attackers.

4.1 DES Cryptosystem

DES is a block cipher. In this cryptosystem, the blocks are encrypted separately. In DES, the input message is processed as L_0R_0, and the message has 12 bits. L_0 and R_0 both have 6 bits, and they are first and last 6 bits respectively. The ith round produces output as L_i and R_i from the input L_{i-1} and R_{i-1}.This process continues for all rounds as shown in the figure below.



[44]

Figure 16: DES Block Diagram.

This is a sample picture to briefly describe the methodology used in DES to make it a block cipher. As in this figure, it can be observed that Li-1 is being fed to generate Ri; in the same way, Li would be inserted to create the Li+1. Therefore, each character is linked now with each other, and changing one character would affect the whole block of characters.

Weakness

Brute force attack:

Overall, DES was a good cryptosystem in 1973, but due to the development of more efficient and better computational processors over time, the brute force attack became the biggest threat to this cryptosystem, and it gradually became non-usable. Adi Shamir et al. claimed to break 16 rounds of DES with the use of $2^{\wedge 49}$ chosen texts [50], and this attack is called differential cryptanalysis. Mitsuru Matsui published a paper on the linear cryptanalysis attack method for DES encryption. Another attack on the DES that is also important to note is called the Devis attack. This attack is limited to DES. In this attack, 2^50 chosen texts were required with a 51% success rate [52, 53].

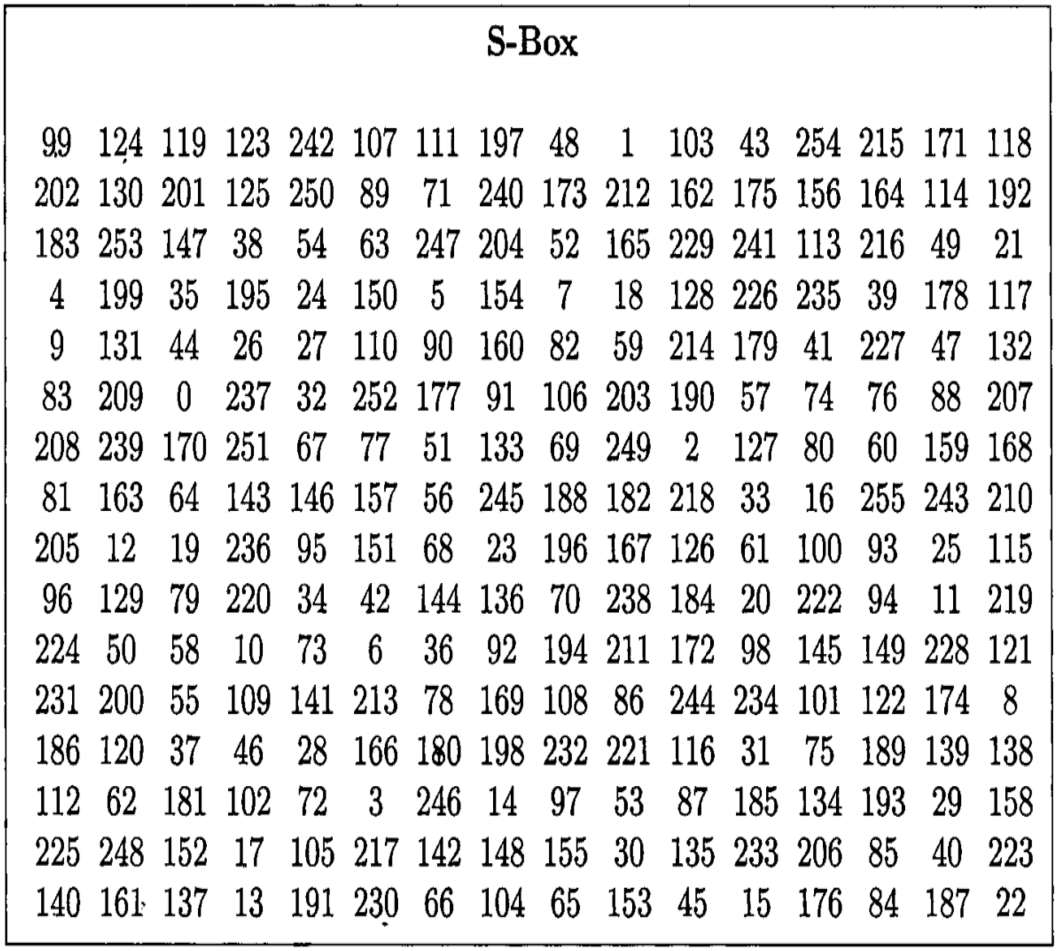
4.3 AES Cryptosystem

The AES was developed by Joan Daeman and Vincent Rijmen [49]. Advanced Encryption Standard (Rijndael): National Institute of Standards & Technology (NIST) requested the development of an alternative for DES in 1997. The NIST suggested that the algorithm should protect the cryptosystem through 128, 192, and 256 bits of the key. It should be operational for 128 input bits, and at the same time, it should be compatible with a varied range of different hardware. In AES, four layers were introduced: byte substitution transformation, shift row transformation, mix column transformation, and the fourth round addition of the round key layer.

These four layers are explained in detail in this chapter. The different key sizes of AES is considered one of the drawbacks for hardware compatibility.

4.3.1 The Byte Sub Transformation (BS):

This was added to protect the cryptosystem from differential and linear crypto analysis attack. In this first step, every byte is changed to another byte using the S box. S box is a matrix where all characters are changed to a specific string of values for the second round (SR).



S-Box

99	124	119	123	242	107	111	197	48	1	103	43	254	215	171	118
202	130	201	125	250	89	71	240	173	212	162	175	156	164	114	192
183	253	147	38	54	63	247	204	52	165	229	241	113	216	49	21
4	199	35	195	24	150	5	154	7	18	128	226	235	39	178	117
9	131	44	26	27	110	90	160	82	59	214	179	41	227	47	132
83	209	0	237	32	252	177	91	106	203	190	57	74	76	88	207
208	239	170	251	67	77	51	133	69	249	2	127	80	60	159	168
81	163	64	143	146	157	56	245	188	182	218	33	16	255	243	210
205	12	19	236	95	151	68	23	196	167	126	61	100	93	25	115
96	129	79	220	34	42	144	136	70	238	184	20	222	94	11	219
224	50	58	10	73	6	36	92	194	211	172	98	145	149	228	121
231	200	55	109	141	213	78	169	108	86	244	234	101	122	174	8
186	120	37	46	28	166	180	198	232	221	116	31	75	189	139	138
112	62	181	102	72	3	246	14	97	53	87	185	134	193	29	158
225	248	152	17	105	217	142	148	155	30	135	233	206	85	40	223
140	161	137	13	191	230	66	104	65	153	45	15	176	84	187	22

[44]

Figure 17: Sample image of S-box from Trappe Wade.

The output of the S box is a 4 x 4 matrix. This step is required to transform the input into specific bytes through the use of the S box. This round produces a total of 16 outputs of bytes which are processed in the next round or the next layer as follows in figure 18.

$$\begin{pmatrix} b_{0,0} & b_{0,1} & b_{0,2} & b_{0,3} \\ b_{1,0} & b_{1,1} & b_{1,2} & b_{1,3} \\ b_{2,0} & b_{2,1} & b_{2,2} & b_{2,3} \\ b_{3,0} & b_{3,1} & b_{3,2} & b_{3,3} \end{pmatrix}$$

[44]

Figure 18: Matrix of S-box output.

4.3.2 The Shift Row Transformation (SR):

This layer was introduced to diffuse bits over multiple rounds. In this step all the rows of this matrix are rotated or shifted cyclically. In this round, the values received from the first layer are shifted cyclically to the left by an offset of 0, 1, 2, and 3 to obtain the matrix as shown in figure 19

$$\begin{pmatrix} c_{0,0} & c_{0,1} & c_{0,2} & c_{0,3} \\ c_{1,0} & c_{1,1} & c_{1,2} & c_{1,3} \\ c_{2,0} & c_{2,1} & c_{2,2} & c_{2,3} \\ c_{3,0} & c_{3,1} & c_{3,2} & c_{3,3} \end{pmatrix} = \begin{pmatrix} b_{0,0} & b_{0,1} & b_{0,2} & b_{0,3} \\ b_{1,1} & b_{1,2} & b_{1,3} & b_{1,0} \\ b_{2,2} & b_{2,3} & b_{2,0} & b_{2,1} \\ b_{3,3} & b_{3,0} & b_{3,1} & b_{3,2} \end{pmatrix}$$

[44]

Figure 19: Shifting the values cyclically.

4.3.3 The Mix Column Transformation (MC):

This layer works with layer 2 to complete the process of layer 2. In this layer the matrix values received from the step (shift row transformation step) are mixed into a specific column. The chosen matrix column is chosen based on the requirement, and it may not be same every time. In this round, the values received from layer 2 are multiplied by a binary matrix as shown in figure 20. This matrix can be changed as per the requirement of the algorithm and it is very easy to change this matrix based on the requirement of the new algorithm. This mix column transformation is one of the important feature in this encryption which provide strength to this encryption.

$$\begin{pmatrix} 00000010 & 00000011 & 00000001 & 00000001 \\ 00000001 & 00000010 & 00000011 & 00000001 \\ 00000001 & 00000001 & 00000010 & 00000011 \\ 00000011 & 00000001 & 00000001 & 00000010 \end{pmatrix} \begin{pmatrix} c_{0,0} & c_{0,1} & c_{0,2} & c_{0,3} \\ c_{1,0} & c_{1,1} & c_{1,2} & c_{1,3} \\ c_{2,0} & c_{2,1} & c_{2,2} & c_{2,3} \\ c_{3,0} & c_{3,1} & c_{3,2} & c_{3,3} \end{pmatrix}$$

$$= \begin{pmatrix} d_{0,0} & d_{0,1} & d_{0,2} & d_{0,3} \\ d_{1,0} & d_{1,1} & d_{1,2} & d_{1,3} \\ d_{2,0} & d_{2,1} & d_{2,2} & d_{2,3} \\ d_{3,0} & d_{3,1} & d_{3,2} & d_{3,3} \end{pmatrix}.$$

[44]

Figure 20: Mix column transformation.

4.3.4 Add Round Key (ARK):

In this layer, the round key is XORed with the values received from the mix-column transformation layer. In this round, the bytes received from round 3 are XORed with the key. The purpose of this round is to restrain the linearity attack which can compromise encryption.

$$\begin{pmatrix} d_{0,0} & d_{0,1} & d_{0,2} & d_{0,3} \\ d_{1,0} & d_{1,1} & d_{1,2} & d_{1,3} \\ d_{2,0} & d_{2,1} & d_{2,2} & d_{2,3} \\ d_{3,0} & d_{3,1} & d_{3,2} & d_{3,3} \end{pmatrix} \bigoplus \begin{pmatrix} k_{0,0} & k_{0,1} & k_{0,2} & k_{0,3} \\ k_{1,0} & k_{1,1} & k_{1,2} & k_{1,3} \\ k_{2,0} & k_{2,1} & k_{2,2} & k_{2,3} \\ k_{3,0} & k_{3,1} & k_{3,2} & k_{3,3} \end{pmatrix}$$

$$= \begin{pmatrix} e_{0,0} & e_{0,1} & e_{0,2} & e_{0,3} \\ e_{1,0} & e_{1,1} & e_{1,2} & e_{1,3} \\ e_{2,0} & e_{2,1} & e_{2,2} & e_{2,3} \\ e_{3,0} & e_{3,1} & e_{3,2} & e_{3,3} \end{pmatrix}.$$

[44]

Figure 21: Addition of round key.

Weakness

AES encryption was cracked much faster by researchers at Microsoft and various universities, and it is no more secure after advanced computational power. [38] Another weakness of AES encryption is its less hardware-compatible due to four different versions of the key lengths. Further, the AES was very slow .

Chapter 5

RSA Algorithm

The RSA algorithm is basically a public key encryption cryptosystem. With Public Key Cryptosystems the encrypting key is publicly available, and the decrypting key is only available to the authorized user. After the failure of Symmetric Key encryptions, researchers developed an idea to come up with Public Key encryption.

The Public Key Cryptosystem was first publicly introduced by a researcher named Diffie-Hellman [45]. In 1997, Rivest, Shamir, and Adleman proposed the idea that factorization of integers into their prime factors is hard, and they introduced the encryption algorithm named after their first initials as the RSA Algorithm. In this algorithm, the person who is supposed to receive an encrypted cipher text chooses two large distinct prime numbers "p" and "q" and multiplies them to get the value known as "n."

Then, an encryption exponent “e” must be chosen which satisfies the condition that the greatest common divisor of e, (p-1) and (q-1) equals to 1. The pair (n, e) is sent to the person who is supposed to send the secret message (plain text). Now this person writes a message “m” and computes “c” as under,

$C = m^{e\,(}$mod n) and sends this C back to the original person as the encrypted message.

As the “p” and “q” are known to this person, he can find the decryption exponent d = 1 (mod ((p-1) (q-1)) and find the original plain text “m” using the equation, $m = c^{d}$ (mod n) to decrypt the message “m”. Although RSA is a good encryption method, it is still not safe anymore, and its weaknesses are mentioned below. RSA algorithm has three different types of vulnerabilities and these are Coppersmith Attack, Boneh Attack and Weiner Attack. These all three attacks are mentioned below.

Weakness: The RSA algorithm has a few flaws:

(1) **Coppersmith Attack:** It was found that, if "n" has "m" digits, and if the first or last quarter of "m" is known along with "p," it is possible to efficiently factor "n" and decrypt the message. Reference: DOI: 10.3844/jcssp.2006.665.671 Journal of Computer Science Volume 2, Issue 8.

(2) **Boneh Attack:** Boneh found that if (n,e) is the RSA public key, the "n" has "m" digits, and the last m/4 digits of decryption exponent "d," it is possible to find "d" in a time that efficiently is linear in elope base 2[46].

(3) **Weiner Attack:** Weiner found that if the exponent "e" is not a substantially large number, it is possible to crack the RSA algorithm [47].

CHAPTER 6

HASH FUNCTIONS

6.1 Overview

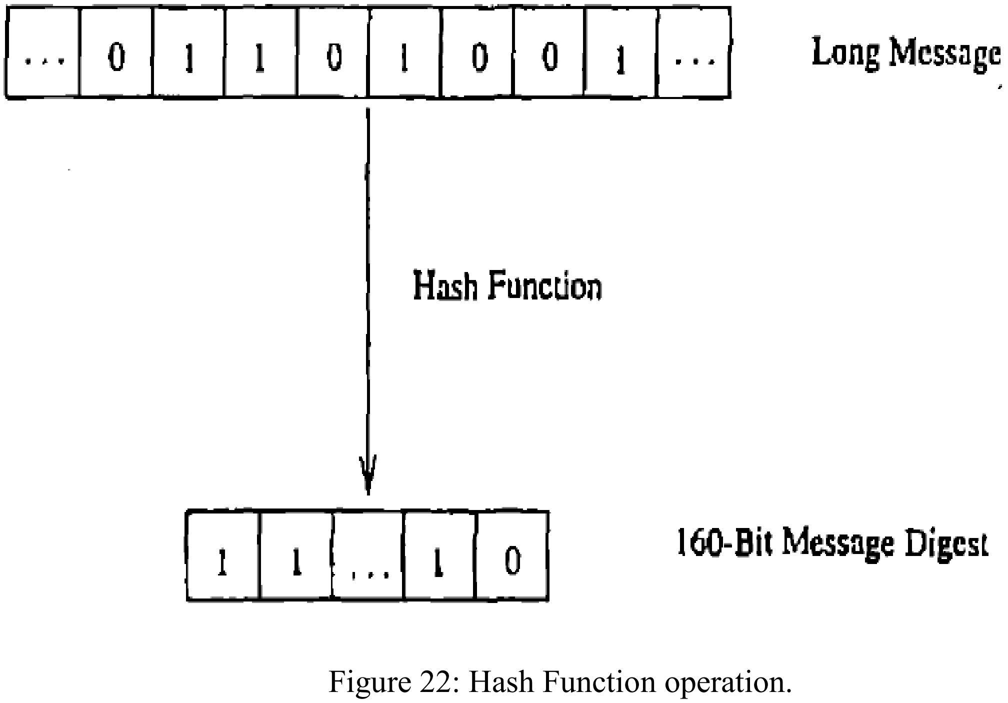
The Hash Function is a primary component of multiple cryptographic algorithms. In this function, the input message has an arbitrary length, and it produces an output message as a fixed length. Hash is considered as a one-way function.

The Hash Function must suffice three main conditions,

(1) For any message "m," the message digest h(m) has to be calculated very fast.

(2) For any given message “y” it is computationally infeasible to find an m’ with h(m’) = y.

(3) It has to be computationally infeasible to search message1 and message2 with h(message1) = h(message2)to make it strongly collision free.



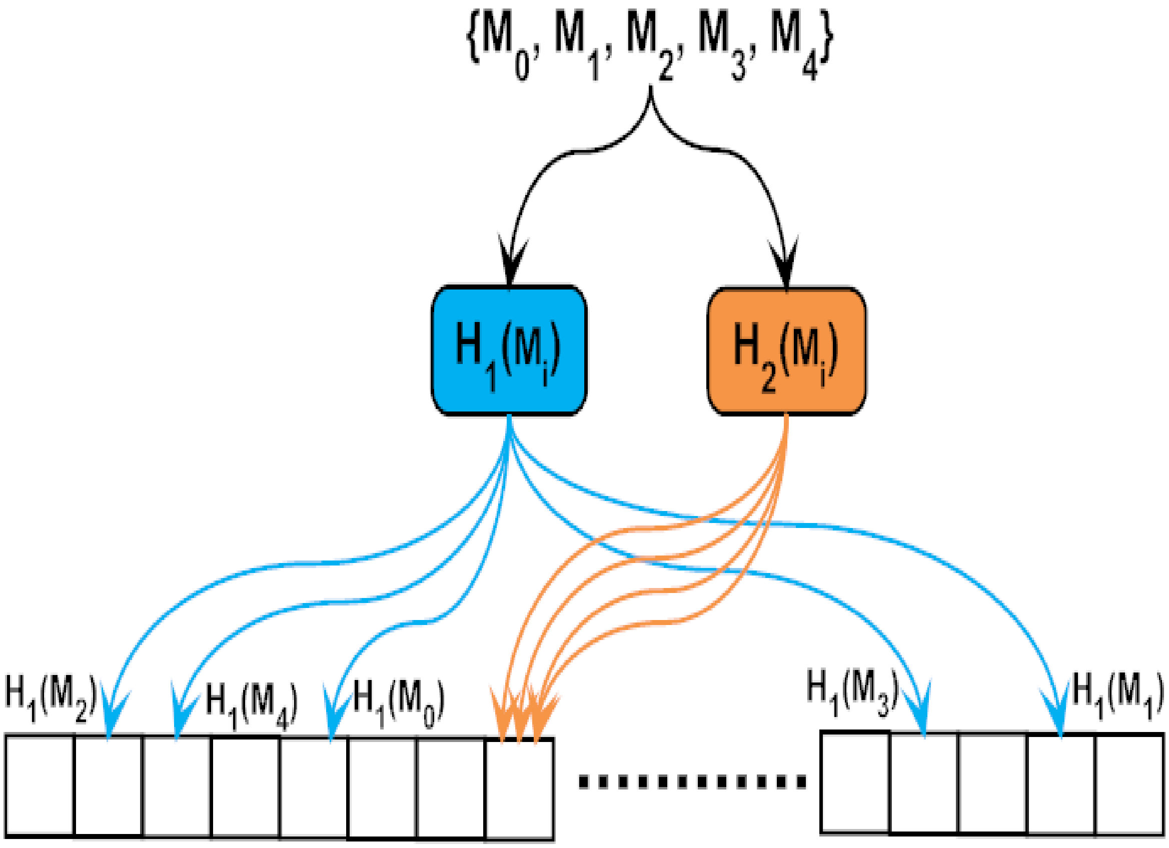
[44]

Figure 22: Hash Function operation.

The Hash Function is also called a collision free function because of this property. Computationally it is almost impossible to find the same h (m1) = h (m2).

6.2 Hash Function efficiency

Figure 23, shows the data distribution of the Hash Function.



[48]

Figure 23: Hash Function data distribution.

The Hash Function produces the Hash values for every element within a data set. The Hash Function is a fast math operation. It is a deterministic and very stable operation. While Hashing, the Hash Function distributes the data as per its algorithm, and this algorithm plays an essential role in its efficiency. Based on the type of requirements, the Hash Function algorithms are specially developed to protect it from potential attacks and to increase its efficiency.

6.3 Hash Function Weakness

As the Hash Function takes an arbitrary input length and provides a fixed range of output, there exist infinite collisions, which means different inputs might end up with the same output.

To compromise the Hash Function, it is necessary to find a couple of input strings which produce the same result as the Hash output. This is known as Hah-Collision. This kind of attack can be launched by some software which can compare two Hashes such as file integrity checks or password Hashes, etc.

Collision Attack of Hash Function: In this attack, the goal is to find a couple of inputs which can produce the same data. For this kind of attack, the attacker has to choose an arbitrary H(A), and H(B) where they are H(A) and H(B) are same[54].

Pre-image Attack: In this attack, the Hash value is specified and calibrated with multiple inputs [54]. This is called a pre-image attack because it is kind of an attack where the Hash value is decided first, and on the basis of the value of the Hash value it is set or calibrated with the plaintext.

Birthday Attack: This is an attack linked with the mathematics of probability theories in detail. In this attack in a group of randomly grouped people whose total number of people is "n", some pair of people would have the same birthday. It means there is a 50% chance to break the collision resistance [54].

CHAPTER 7

WHIRLPOOL CRYPTOSYSTEM

7.1 Overview

This cryptosystem was designed by Vincent Rijmen who was co-creator of AES encryption, and Paulo Barreto in 2000 [39]. The New European Schemes have recommended this cryptosystem for Signature, Integrity, and Encryption (NESSIE) [39]. This cryptosystem was developed using NIST (National Institute of Science and Technology) standards [39].

As of now, no vulnerabilities have been observed or found by anyone;therefore, it is considered the most secure and advanced encryption methods. The Hash Function focuses on recurring usage of the compression function which processes two inputs which are values from the previous step, known as the chaining variable and a "b" bit block that produces an output of n-bit. The last value of the chaining variable is considered as the Hash value. The mathematical form can be represented as in figure 24 which is mentioned in William Stallings's research (The Whirlpool Secure Hash Function) . Generally b > n; therefore compression is required. As an overview, mathematically the Hash Function can be described as shown in figure 24.

$$
\begin{aligned}
CV_0 &= IV = \text{initial } n\text{-bit value} \\
CV_i &= f(CV_{i-1}, Y_{i-1}), \quad 1 \le i \le L \\
H(M) &= CV_L
\end{aligned}
$$

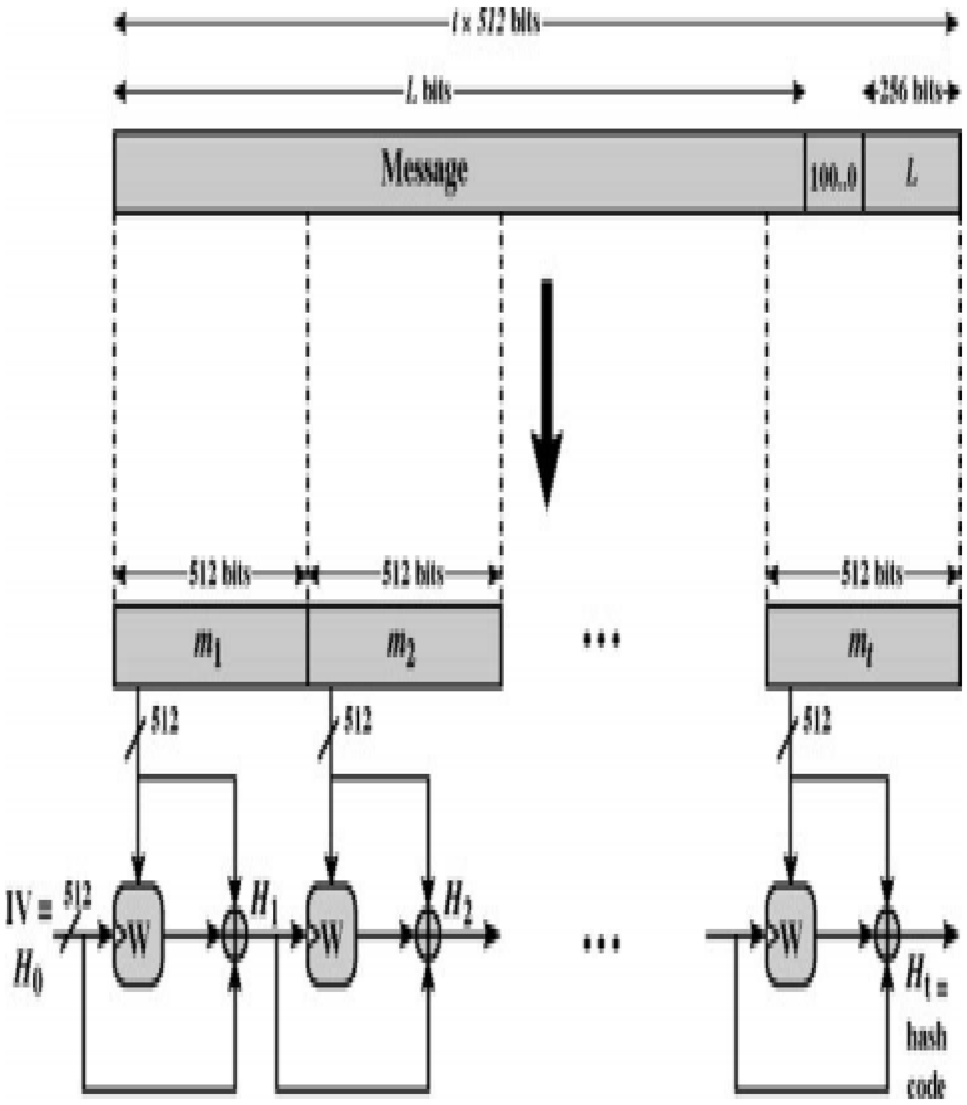
[44]

Figure 24: Hash Function mathematical formula.

7.2 The Whirlpool HASH Structure

In this encryption, the message is split in the sequence of blocks m_1, m_2, m_3,….m_t. The Hash Function for this encryption can be expressed shown in figure 25.

H_0 as an initial value, $H_i = E\ (H_{i-1,}\ m_i)\_ \oplus H_{i-1} \oplus mi_{=}$ intermediate value and H_t = Hash code value.



[39]

Figure 25: Message Digest Generating using Whirlpool Encryption.

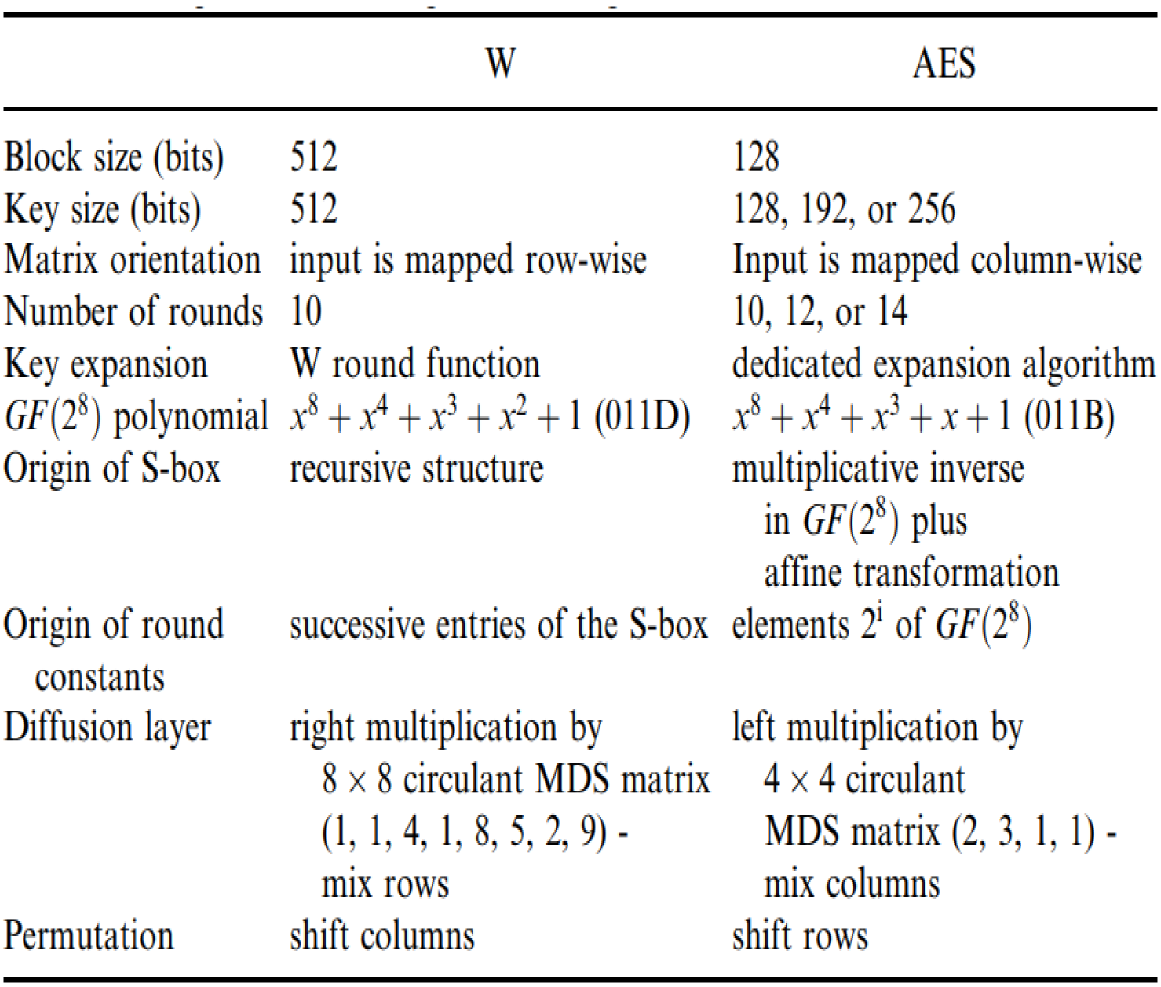
7.3 Whirlpool Algorithm Tasks

This structure performs four tasks. They are (1) appending the padding bits (2) length requirement (3) Hash matrix and (4) W block processing. All four steps are designed very carefully to overcome all the attacks which were successfully launched on previous encryption methods over time. In task 1, the additional 0 bits are added to make the blocks in the odd multiple of 256. If any message is an even multiple of 256, the message is combined with 256 bytes of value 0 to make it an odd multiple of 256. If any message has an odd number of 256 bits, it is padded with 512 bits. Thus, the number of padding bits is 1 to 512 bits. The additional bits are added as one "1" bit, and the rest are "0". In task 2, which is length requirement, 256 bits are appended to the message. Therefore, the result of the first two steps produces an integer which would be a multiple of 512 bits. In the third task, the Hash matrix is introduced, and the matrix is computed with every bit as "0". This would be 8 x 8 matrix. in the fourth task, the message is processed into 512-bits and provided as input to the W box.

7.4 Block Cipher W

The Block cipher W is the main reason for enhanced security of Whirlpool encryption compared to other MD family encryptions such as AES encryption. The comparison between cipher W and AES encryption is more important to understand Whirlpool encryption security enhancement with details. Whirlpool Encryption has a block size of 512 bits whereas AES has a block size of 128 bits. Both have different key sizes. Whirlpool has 512 bits key size whereas AES has 128, 192 and 256 bits key size. This is one of the weaknesses of AES compared to Whirlpool encryption due to small key space.

Further, both have different shifting concepts. In Whirlpool encryption, the columns are shifted whereas in AES rows are shifted.



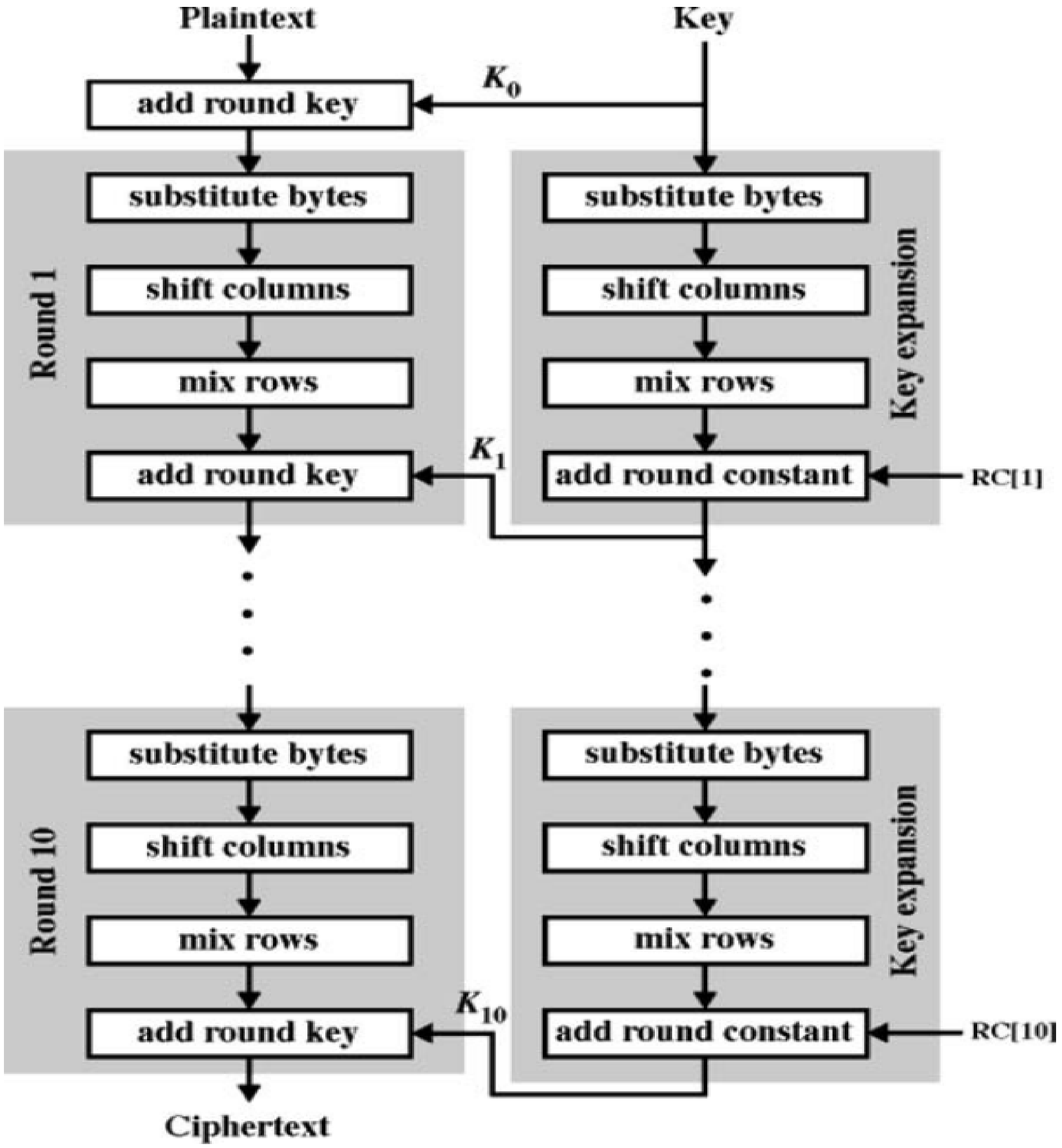
	W	AES
Block size (bits)	512	128
Key size (bits)	512	128, 192, or 256
Matrix orientation	input is mapped row-wise	Input is mapped column-wise
Number of rounds	10	10, 12, or 14
Key expansion	W round function	dedicated expansion algorithm
$GF(2^8)$ polynomial	$x^8+x^4+x^3+x^2+1$ (011D)	$x^8+x^4+x^3+x+1$ (011B)
Origin of S-box	recursive structure	multiplicative inverse in $GF(2^8)$ plus affine transformation
Origin of round constants	successive entries of the S-box	elements 2^i of $GF(2^8)$
Diffusion layer	right multiplication by 8×8 circulant MDS matrix (1, 1, 4, 1, 8, 5, 2, 9) - mix rows	left multiplication by 4×4 circulant MDS matrix (2, 3, 1, 1) - mix columns
Permutation	shift columns	shift rows

[39]

Figure 26: W block of the Whirlpool encryption and AES comparison.

Here, 512 bits block size of W cipher provides better security compared to the small key size of 128, 192 and 256 . Further, as the key size is fixed (i.e. 512 bits), its implementation is easy and provides better compatibility with different hardware. For example it works well for different processors whereas in AES and other MD family members different key sizes and small key sizes lead to less security and more compatibility issues over a different kind of hardware. As the number of rounds in Whirlpool encryption is fixed at 10, it again provides easy implementation compared to AES where a number of rides have multiple options which limit its hardware compatibility.

W operates on a state of 8 X 8 bytes. The more the state representation differs from a square, the slower the diffusion and the more rounds the cipher needs. For a block length of 512 bits, the Whirlpool developers could have defined a Rijndael operating on a state of 4 X 16 bytes, but that cipher would have needed many rounds, and it would have been very slow. [39]



[39]

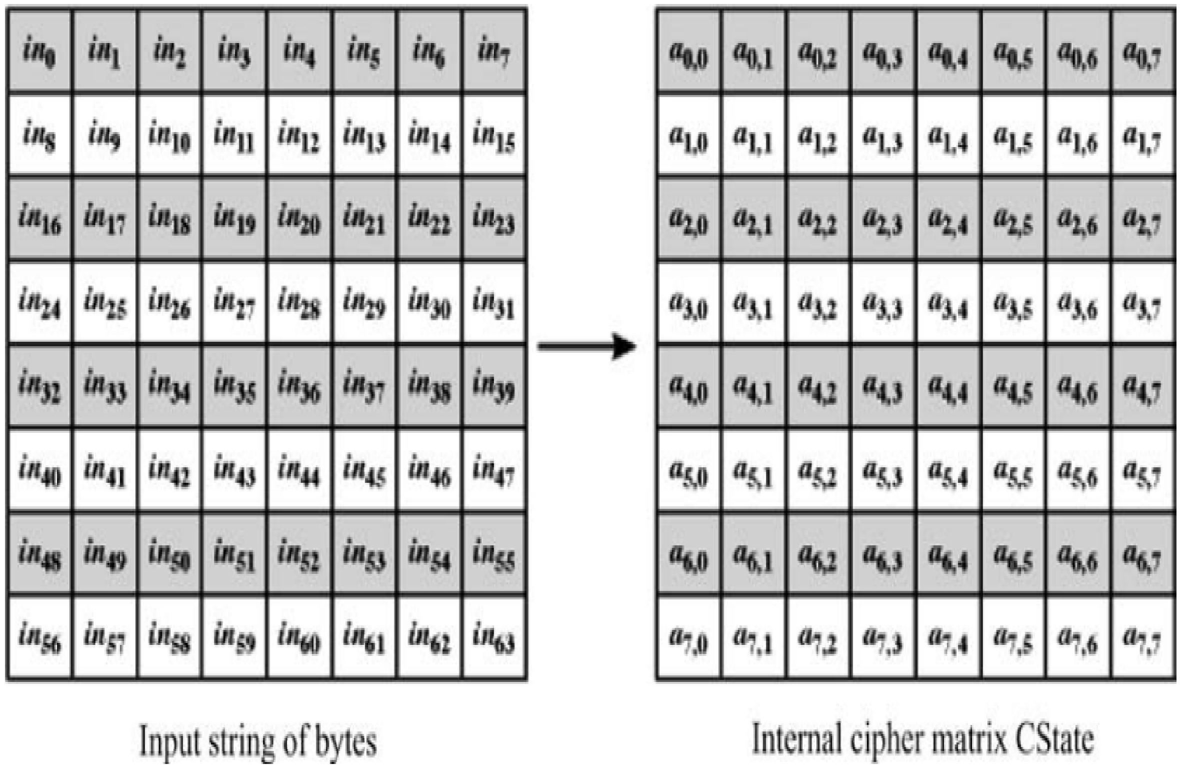
Figure 27: W block of the Whirlpool encryption.

The Whirlpool has four different transformations. They are Add Round Key (AK), Substitution of Bytes (SB), Shifting of Columns (SC), and mixing of rows (MR). For r as a round function RF and W (K), the formula can be written as mentioned in The Whirlpool Secure Hash Function by William Stallings. Here, K_r is the round key matrix to corresponding round r. K is the key input for the overall algorithm.

$$RF(\mathbf{K_r}) = \mathbf{AK}[\mathbf{K_r}] \circ \mathbf{MR} \circ \mathbf{SC} \circ \mathbf{SB}$$

$$W(\mathbf{K}) = \left(\overset{10}{\underset{r=1}{\mathrm{O}}} RF(\mathbf{K}_r) \right) \circ AK(\mathbf{K}_0)$$ [39]

Figure 28: Equations for the first round of Whirlpool encryption.



in_0	in_1	in_2	in_3	in_4	in_5	in_6	in_7
in_8	in_9	in_{10}	in_{11}	in_{12}	in_{13}	in_{14}	in_{15}
in_{16}	in_{17}	in_{18}	in_{19}	in_{20}	in_{21}	in_{22}	in_{23}
in_{24}	in_{25}	in_{26}	in_{27}	in_{28}	in_{29}	in_{30}	in_{31}
in_{32}	in_{33}	in_{34}	in_{35}	in_{36}	in_{37}	in_{38}	in_{39}
in_{40}	in_{41}	in_{42}	in_{43}	in_{44}	in_{45}	in_{46}	in_{47}
in_{48}	in_{49}	in_{50}	in_{51}	in_{52}	in_{53}	in_{54}	in_{55}
in_{56}	in_{57}	in_{58}	in_{59}	in_{60}	in_{61}	in_{62}	in_{63}

Input string of bytes

$a_{0,0}$	$a_{0,1}$	$a_{0,2}$	$a_{0,3}$	$a_{0,4}$	$a_{0,5}$	$a_{0,6}$	$a_{0,7}$
$a_{1,0}$	$a_{1,1}$	$a_{1,2}$	$a_{1,3}$	$a_{1,4}$	$a_{1,5}$	$a_{1,6}$	$a_{1,7}$
$a_{2,0}$	$a_{2,1}$	$a_{2,2}$	$a_{2,3}$	$a_{2,4}$	$a_{2,5}$	$a_{2,6}$	$a_{2,7}$
$a_{3,0}$	$a_{3,1}$	$a_{3,2}$	$a_{3,3}$	$a_{3,4}$	$a_{3,5}$	$a_{3,6}$	$a_{3,7}$
$a_{4,0}$	$a_{4,1}$	$a_{4,2}$	$a_{4,3}$	$a_{4,4}$	$a_{4,5}$	$a_{4,6}$	$a_{4,7}$
$a_{5,0}$	$a_{5,1}$	$a_{5,2}$	$a_{5,3}$	$a_{5,4}$	$a_{5,5}$	$a_{5,6}$	$a_{5,7}$
$a_{6,0}$	$a_{6,1}$	$a_{6,2}$	$a_{6,3}$	$a_{6,4}$	$a_{6,5}$	$a_{6,6}$	$a_{6,7}$
$a_{7,0}$	$a_{7,1}$	$a_{7,2}$	$a_{7,3}$	$a_{7,4}$	$a_{7,5}$	$a_{7,6}$	$a_{7,7}$

Internal cipher matrix CState

[39]

Figure 29: Whirlpool matrix structure.

In this Whirlpool matrix structure, the process of encryption of plaintext is described. Each input of plaintext is divided into a size of 512 bits and treated as 8 X 8 matrix of values, which is known as C-state. The input of first 8 bytes of a 512 bits plaintext is processed for encryption in the first row of C-State and so on. This linear representation of linear byte stream can be expressed as mapping function μ. Therefore, for all rows 0 to 7, and byte array X with elements X_k of values from 0 to 63 the corresponding matrix A with values $a_{i,j}$ would be as shown in figure 30.

$$\mathbf{A} = \mu(X) \Leftrightarrow a_{i,j} = x_{8i+j}.$$

[39]

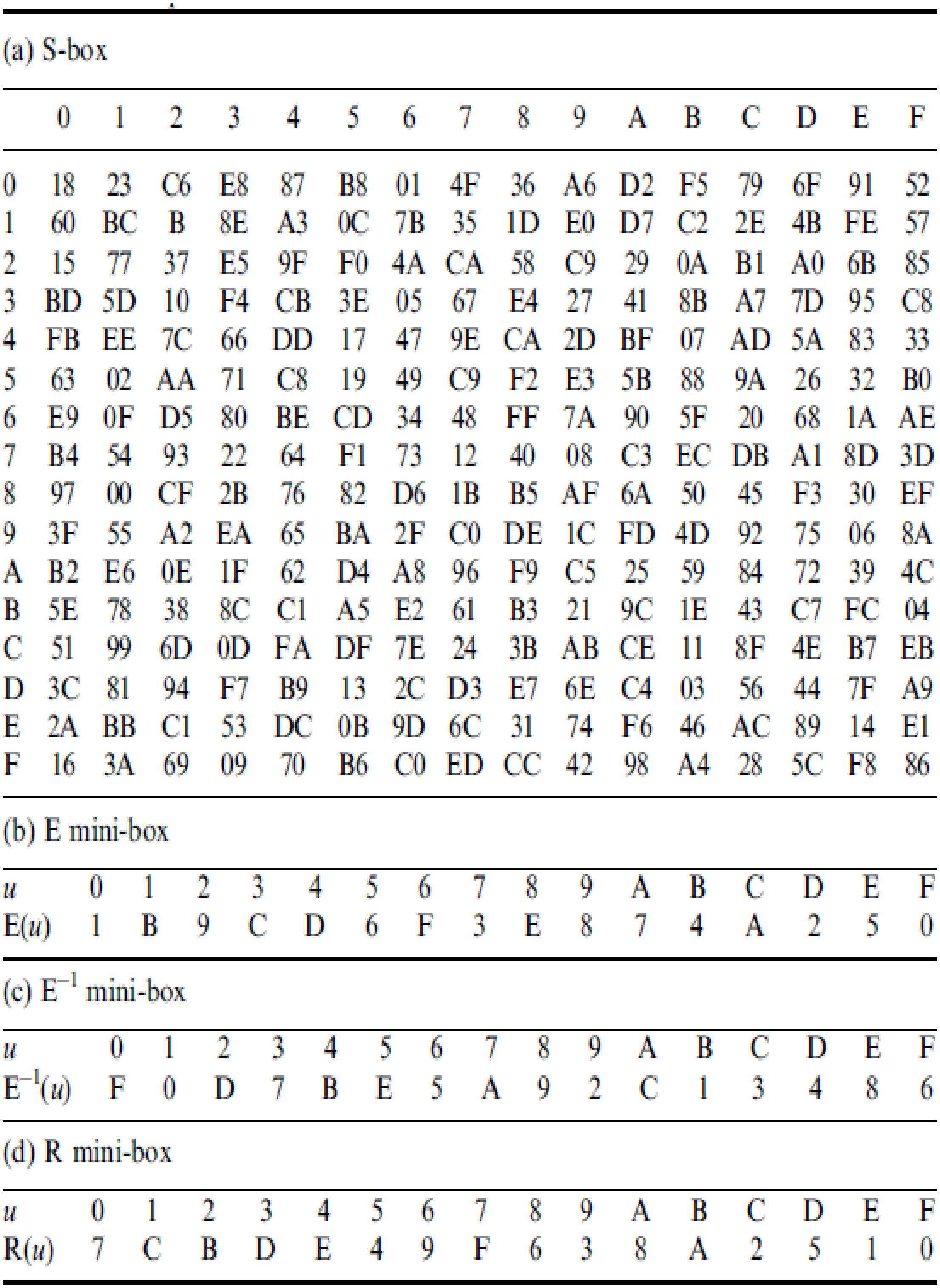
Figure 30: Equation for the Whirlpool matrix.

7.5 Whirlpool Encryption Layers

Whirlpool Encryption has a total of four layers, and they are Non-linear Substitute Byte Function Layer, Permutation Layer, Diffusion Layer MR, and Adding Key Layer AK. Each layer is important, and they have been added to make the Whirlpool encryption cryptosystem more and more robust and to overcome past attacks on various encryption methods.

7.5.1 Non-Linear Substitute Byte Function Layer:

This layer is introduced to provide nonlinear mapping. The bytes generated in the above steps are basically in the format of 16 X 16 matrix byte values called an S-box. This nonlinearity feature is important to resist linear-attacks. The idea behind this layer is to substitute the original bits with a pre-decided S-box value based on the matrix of the S-box. The S-box contains a total of 256 different values, and these values correspond to specific values inside the 16 X 16 matrix while processing input in this layer.



(a) S-box

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	18	23	C6	E8	87	B8	01	4F	36	A6	D2	F5	79	6F	91	52
1	60	BC	B	8E	A3	0C	7B	35	1D	E0	D7	C2	2E	4B	FE	57
2	15	77	37	E5	9F	F0	4A	CA	58	C9	29	0A	B1	A0	6B	85
3	BD	5D	10	F4	CB	3E	05	67	E4	27	41	8B	A7	7D	95	C8
4	FB	EE	7C	66	DD	17	47	9E	CA	2D	BF	07	AD	5A	83	33
5	63	02	AA	71	C8	19	49	C9	F2	E3	5B	88	9A	26	32	B0
6	E9	0F	D5	80	BE	CD	34	48	FF	7A	90	5F	20	68	1A	AE
7	B4	54	93	22	64	F1	73	12	40	08	C3	EC	DB	A1	8D	3D
8	97	00	CF	2B	76	82	D6	1B	B5	AF	6A	50	45	F3	30	EF
9	3F	55	A2	EA	65	BA	2F	C0	DE	1C	FD	4D	92	75	06	8A
A	B2	E6	0E	1F	62	D4	A8	96	F9	C5	25	59	84	72	39	4C
B	5E	78	38	8C	C1	A5	E2	61	B3	21	9C	1E	43	C7	FC	04
C	51	99	6D	0D	FA	DF	7E	24	3B	AB	CE	11	8F	4E	B7	EB
D	3C	81	94	F7	B9	13	2C	D3	E7	6E	C4	03	56	44	7F	A9
E	2A	BB	C1	53	DC	0B	9D	6C	31	74	F6	46	AC	89	14	E1
F	16	3A	69	09	70	B6	C0	ED	CC	42	98	A4	28	5C	F8	86

(b) E mini-box

u	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
E(*u*)	1	B	9	C	D	6	F	3	E	8	7	4	A	2	5	0

(c) E^{-1} mini-box

u	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$E^{-1}(u)$	F	0	D	7	B	E	5	A	9	2	C	1	3	4	8	6

(d) R mini-box

u	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
R(*u*)	7	C	B	D	E	4	9	F	6	3	8	A	2	5	1	0

[39]

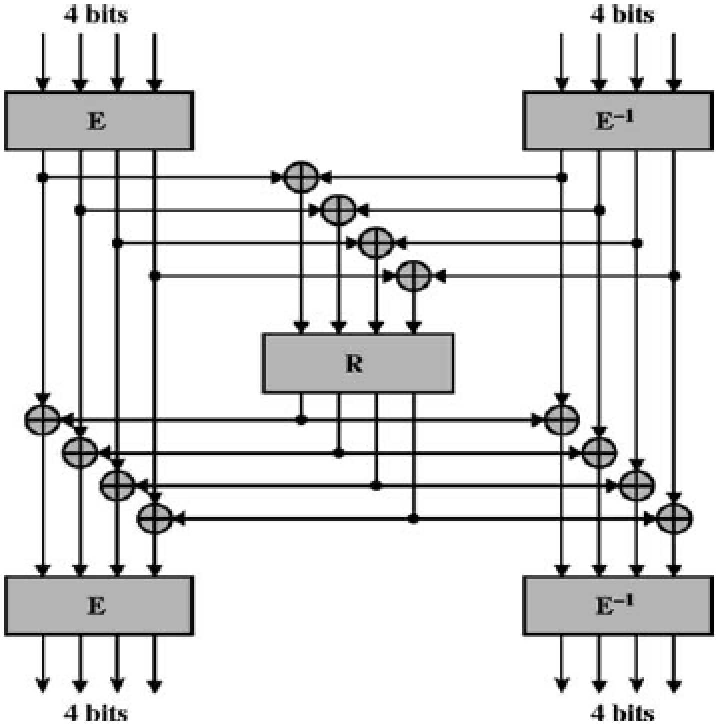
Figure 31: Whirlpool S-box.

In this S box, each C-state is mapped onto a row value and column value. For doing this, the rightmost four digits are considered as a column value, and the leftmost four are regarded as the row value. The Substitution Byte function can be described in the relation of input matrix A and output matrix B shown in figure 33.

$$\mathbf{B} = SB(\mathbf{A}) \Leftrightarrow b_{i,j} = S[a_{i,j}], \quad 0 \le i, j \le 7.$$

[39]

Figure 32: The Byte Substitution Function



[39]

Figure 33: Implementation of Whirlpool CS Box.

For the creation of the S box, two nonlinear layers, each containing 4 X 4 S boxes, are required. These boxes are separated by a 4 X 4 randomly generated box. The purpose of these boxes is to map a 4-bit input onto a 4-bit output.

"The SB function is designed to introduce nonlinearity into the algorithm. This means that the SB function should exhibit no correlations between linear combinations of input bits and linear combinations of output bits. Also, differences between sets of input bits should not propagate into similar differences among the corresponding output bits; put another way, small input changes should cause large output changes. These two properties help to make W resistant against linear and differential cryptanalysis."---- Source: The Whirlpool Secure Hash Function- William Stallings [39].

7.5.2 Permutation Layer SC

This layer is also known as the permutation layer. It shifts the column and causes a circular downward shift of all column of c-state; however, the first column is not included in this. For the second column, the downward shift is performed which is 1 byte. For the third one it would be a 2-byte shift and so on. Considering this, the SC layer can be described as shown in figure 34.

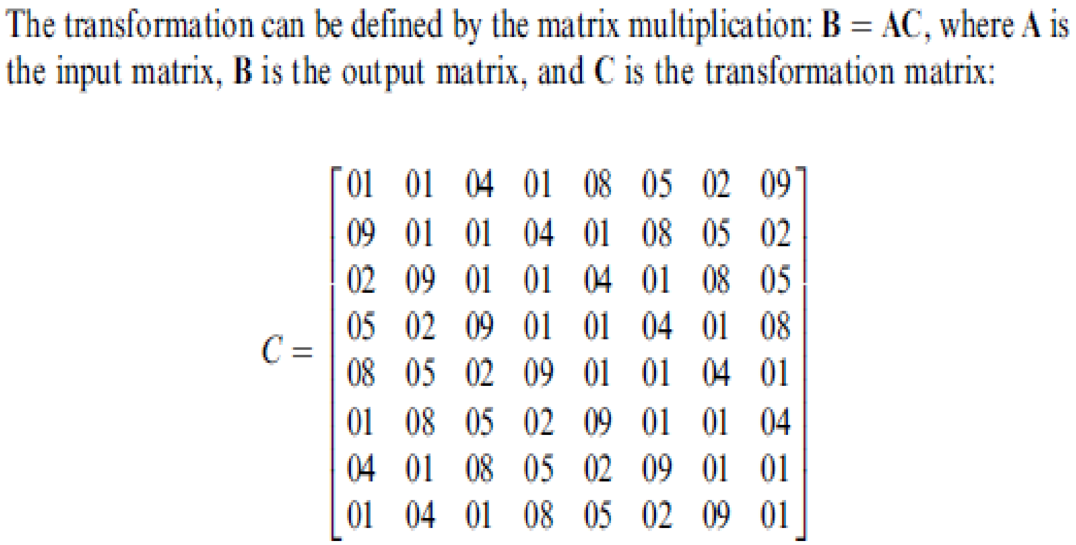
$$\mathrm{B} = SC(\mathrm{A}) \Leftrightarrow b_{i,j} = a_{(i-j) \bmod 8, j} \quad 0 \leq i, j \leq 7.$$

[39]

Figure 34: SC layer formula.

7.5.3 The Diffusion Layer (Mixing of Rows- MR Layer)

This layer is also known as the Diffusion layer. Diffusion is a cryptographic property introduced by Claude Shannon [55]. According to Shannon, diffusion means influencing many cipher texts by a single plaintext digit and thus protecting the overall statistical structure of the plaintext. the purpose of this layer is to diffuse the values which means mixing the rows, and this kind of step was designed in order to make the Whirlpool Encryption Cryptosystem more robust against linear attacks.



The transformation can be defined by the matrix multiplication: **B** = **AC**, where **A** is the input matrix, **B** is the output matrix, and **C** is the transformation matrix:

$$C = \begin{bmatrix} 01 & 01 & 04 & 01 & 08 & 05 & 02 & 09 \\ 09 & 01 & 01 & 04 & 01 & 08 & 05 & 02 \\ 02 & 09 & 01 & 01 & 04 & 01 & 08 & 05 \\ 05 & 02 & 09 & 01 & 01 & 04 & 01 & 08 \\ 08 & 05 & 02 & 09 & 01 & 01 & 04 & 01 \\ 01 & 08 & 05 & 02 & 09 & 01 & 01 & 04 \\ 04 & 01 & 08 & 05 & 02 & 09 & 01 & 01 \\ 01 & 04 & 01 & 08 & 05 & 02 & 09 & 01 \end{bmatrix}$$

[39]

Figure 35: Transformation matrix.

Every value in this product matrix is populated as the summation of a multiplication of values of one column and one row. In this C matrix, every element of every row is generated using a circular right shift of the previous row.

7.5.4 AK (Add Round Key Layer):

The objective of this layer is XOR operation of the 512 bits from C-state with the round key of 512 bits. This function can be expressed as shown in figure 35. Here the B is the output matrix of the next layer, and A is the input matrix. The values of the AK layer are fed to the Block cipher W.

$$\mathbf{B} = AK[K_i](\mathbf{A}) \Leftrightarrow b_{i,j} = a_{i,j} \oplus k_{i,j}, \quad 0 \leq i, j \leq 7.$$

[39]

Figure 35: Formula for Addition of key.

Block Cipher W

As shown in the above figure of W block, expansion is processed by the use of the block cipher with a constant round serving as the round key for expansion. In this step, the bits expand to 512-bit output as depicted in the W block image. "*Although W is similar to AES, it is not simply an extension. In fact, AES is one version of the cipher Rijndael, which was submitted as a candidate for the AES. The Rijndael proposal for AES defined a cipher in which the block length and the key length can be independently specified to be 128, 192, or 256 bits. The AES specification uses the same three key size alternatives but limits the block length to 128 bits. AES operates on a state of 4 x 4 bytes. Rijndael with block length 192 bits operates on a state of 4 x 6 bytes. Rijndael with block length 256 bits operates on a state of 4 x 8 bytes" William Stallings [39]*

7.6 Performance of Whirlpool

As of now, no vulnerabilities have been reported by any researchers and the NIST (National Institute of Standards and Technology) considers it to be of good performance [39]. *"One study that has been completed was reported in [7]. The authors compared Whirlpool with several other secure Hash Functions, including all of the versions of SHA. The authors developed multiple hardware implementations of each Hash Function and concluded that, compared to SHA-512, Whirlpool requires more hardware resources but performs much better in terms of throughput."--- William Stallings [39].*

CHAPTER 8

Akash Rao Secured Password Algorithm

Alphanumeric passwords are often difficult to remember and therefore people have to retrieve their passwords. On the other hand, graphical passwords provide better memorability & usability [10]. In this present thesis, it is proposed that alphanumeric passwords created from pictorial inputs are stronger than pictorial passwords alone and alphanumeric passwords alone. Alphanumeric passwords have less memorability compared to graphical passwords [1]. But graphical passwords are vulnerable to shoulder surfing attack. Therefore, many researchers suggested different ideas such as disguising, Gaze-based input, grouping, moving to other locations, etc. However, they are still vulnerable to shoulder surfing attack. Therefore, I am using graphical passwords with human perception. In earlier methods, the images were only moved on different locations on the screen and shoulder surfing was vulnerable to them. But as every human think differently, everyone's thoughts and perception are different; I am adding the human factor in my model as human perception.

I want to propose a model to create complex alphanumeric passwords through easily memorable pictures, human perception, and alphanumeric inputs. The user would be provided many pictures on the screen at the same time, and the user would choose his picture password from each screen, and based on his own selection the user would response with a passphrase as per the perception, including a few answers based on the confidential information. The user would generate a different word for each picture image. Let’s understand the new algorithm through figure 36.

Now, for this picture, even though someone would be able to peer onto someone’s computer screen, the eavesdropper would not be able to figure out that for what picture, the user has set up some passcode to be converted to the password. Unlike another method, the user would not choose the picture and click the picture because this causes mouse arrow movement and helps the eavesdropper to see the selected picture.

The user would choose one of the animals from this picture mentally and co-relate with some other word related to that picture. At this time, even if the attacker comes to know the chosen animal, the attacker would face confliction with his perception for many possible words related to that picture. First, the attacker would not come to know which animal is chosen for a passcode. Secondly, he would never know the co-related word (passcode) for that animal.

In addition to such user image perceptions, some questions are also introduced to generate a more complex password and to restrict access to legitimate users only who are familiar with confidential details of the genuine user. These answers are used to shift the characters also, and the only purpose of shifting the character is to protect the algorithm from a dictionary attack where the attacker simply launches all dictionary words to compromise. By shifting the letters, the dictionary attack would no longer remain possible.

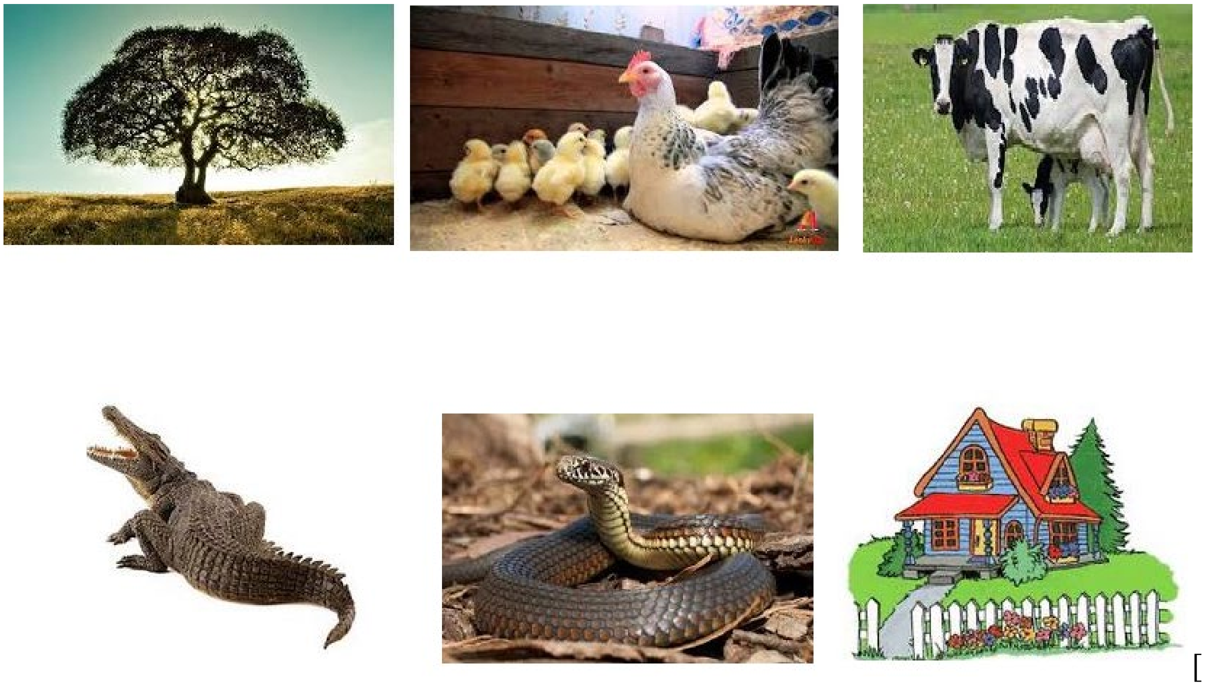
To make it more randomized as well as unique, the letters are shifted with a unique number related to the answers of the user. The number is the remainder of the responses of questions, such as the user's whole birthday and user's father's birthday, divided by the total number of characters in English, i.e., 26.

After shifting, the string is split into ten chunks, and each chunk is separately encrypted by Whirlpool encryption. After encryption, all 128 character long strings are merged to generate the large unique password of 1280 characters. This new algorithm is developed very carefully and cyber-attacks such as dictionary attack, shoulder surfing attack, brute force attacks, linear attacks have been taken into consideration while developing this new algorithm.

8.1 Generating input string

In this step, the user provides answers based on perceptions and factual details. For this purpose, many pictures are shown to the user, and the user must respond for one picture or a group of pictures or for all pictures based on the perception.

Question 1: Narrate your response for the given image/images?



[12]

Figure 36: Collage 1.

For the given picture, the user may choose a different image/images and reply based on perception. For example, for the cow in the above picture, the user may populate many things, and each is different as mentioned below.

1. Mother (In Indian civilization, a cow is honored as a mother)
2. Beef
3. Meat
4. Food

5. Four (it has four legs)
6. Two (pair of horns)
7. Herbivores
8. Animal
9. Milk
10. Vegan
11. Dung
12. Grass
13. mammal
14. Some word related to the user's thoughts or experience. For example, I may choose "attacker," "dodge," "danger," "escape," "disappear" or "father" because cows have attacked me twice in the past, and both times my dad saved me.

If someone chose the crocodile, the response may be as follows:

1. Reptile
2. Carnivores
3. Leather
4. Water
5. Death

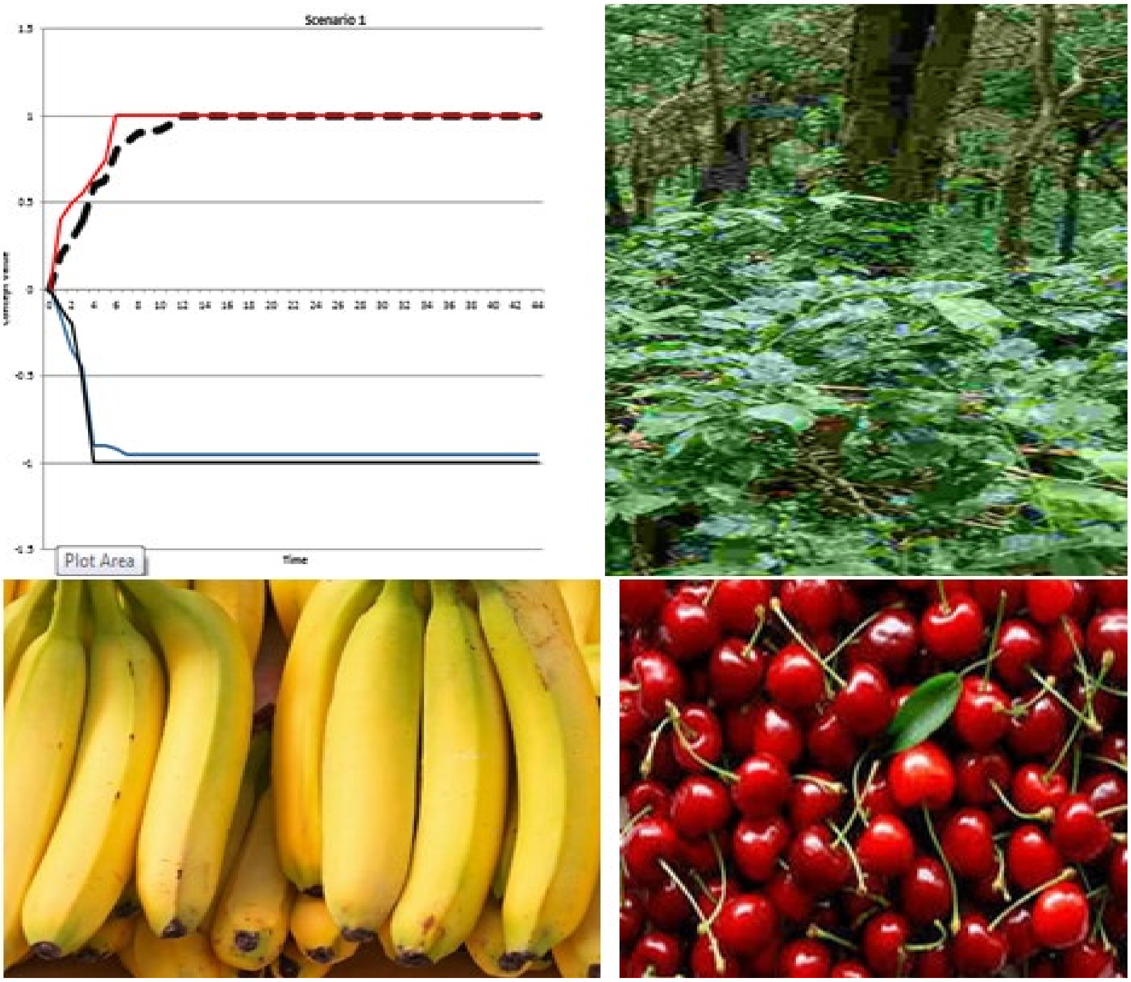
After this picture, a personal question may be asked such as

Question 2: The happiest day in your life

This is very vague and random, and that is what I want. Someone may write a numeric answer such as a date, and someone else may write the alphabetical answer such as "my graduation day" or "my marriage day." Someone may write something related to that day such as a gift received on that day. Such answers are subjective in nature and a shoulder surfing attack fails in this method as the user does not hover the mouse and choose the specific image as the response to graphical authentication; instead, the user would response based on his perception for his chosen graphical passwords among the other available distractors. This method makes it extremely random, vague and challenging for the attacker to figure out or determine the actual graphical authentication image of the user for a shoulder surfing attack and after that to predict the response of a user based on the user's perception.

Sample answer: birthday

Question 3: Narrate your response.



[12]

Figure 37: Collage 2.

For the tree in the picture, many people may have different perceptions such as:

1. Tree
2. Ecology
3. Food
4. Fruits/ apples/ walnuts/ leaf
5. Wood
6. oxygen
7. Birds and nest
8. Monkey
9. Squirrel
10. Chlorophyll
11. Forest

Similarly, for other pictures, there may be several other perceptions. Sample answers are still subjective for everyone as these answers are purely based on the perception. This idea was introduced to provide extreme randomness and, at the same time, to provide memorability to the user.

Sample answers:

(1) Business performance

(2) Group

(3) Fruits

(4) Greenery

(5) Cherry

My answer is Ecology

Question 4: Your birthday in DDMMYYYY format

Sample answers:

(1) 21021986

(2) 02011945

(3) 04121962

(4) 02032000

(5) 12121997

(6) 24122005

Question 5: What are your father's birthplace and birth year?

Sample Answer:

(1) Norfolk and 1900.

(2) 1900 Norfolk

(3) Norfolk 1900

(4) USA 1900.

(5) Mexico 2001

(6) South Africa 1987

(7) 1980 Sudan

(8) 1990 hospital

(9) 1995 my hometown

(10) 1945 my grandmother’s home

(11) At his village 1977

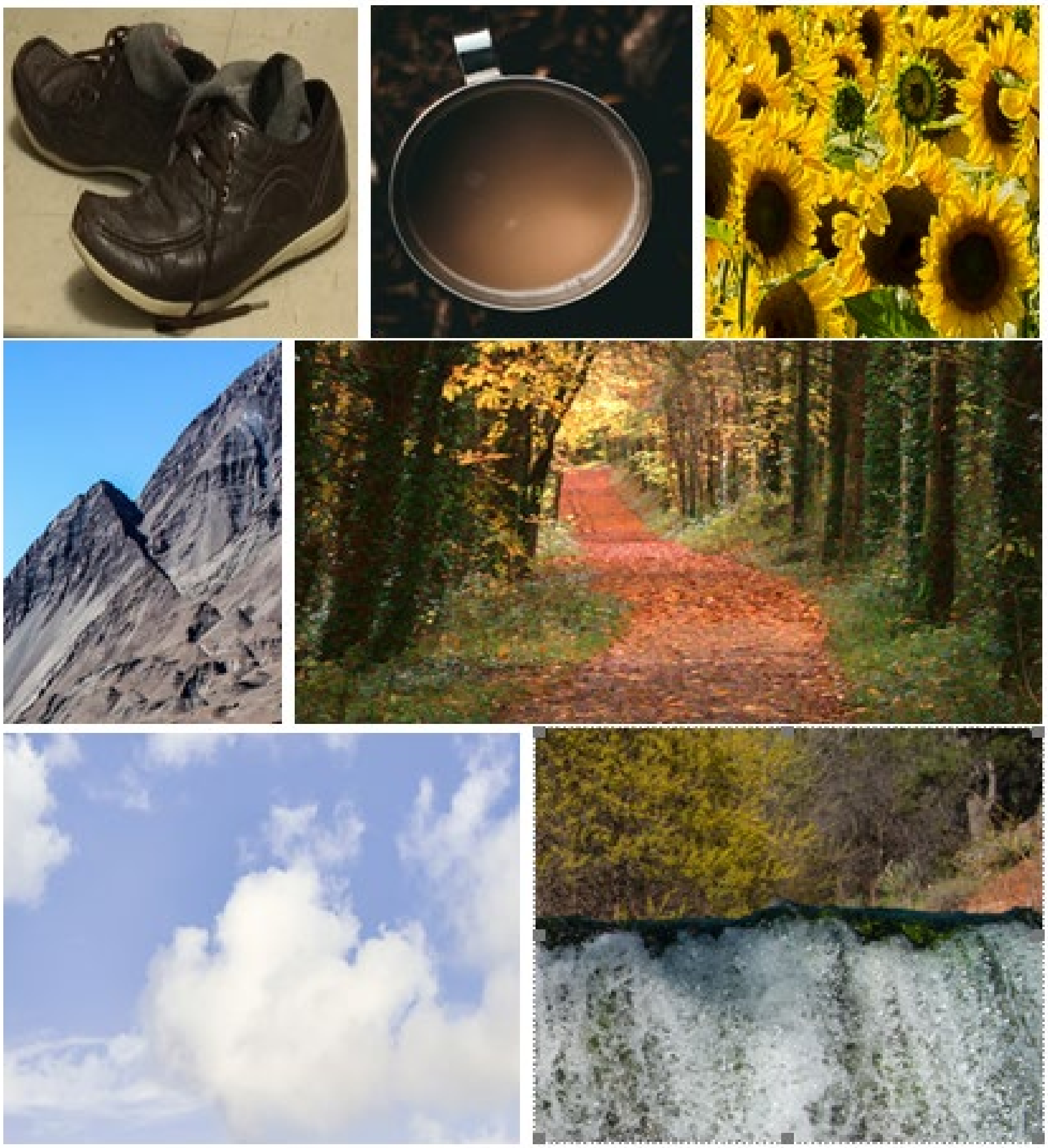
(12) 1978 place don’t know

(13) 1987 TX

(14) 1977 VA

(15) Russia 1968

Question 6: Narrate your response.



[12]

Figure 38: Collage 3.

My answer: My answer is related to all seven images. Someone may write any kind of such things, a short word or a big paragraph; my proposed algorithm is designed such that it can consider all inputs and form a unique outcome.

Sample response:

(1) Clouds

(2) Spring

(3) Forest

(4) Path

(5) Mountain

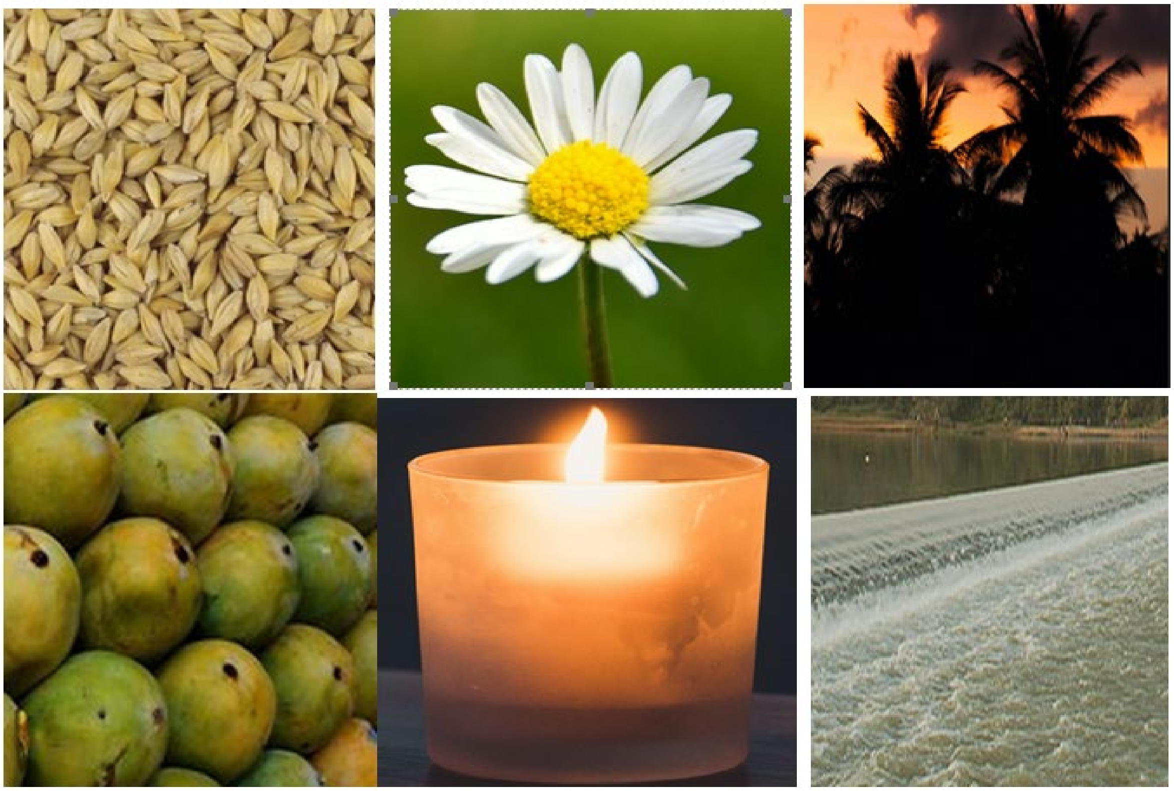
(6) Shoes

(7) Tea

(8) Flowers

My answer is hard work.

These pictures are a good methods for making the responses extremely randomized. Another sample picture can be prepared as follows. These pictures are prepared in such a way that most of the images in a collage would give a different kind of message. Further, these pictures are freely available at free-images.com [12]. Images give multiple perceptions; for example, for figure 39, one of the picture is mangos. For some, the perception may be fruits, food, plurality, group, crowd, green, and safe, etc. Similarly, for the candle in collage 4 in figure 39, someone's perception based response may be candle, light, life, hope, optimism, night, divinity, and death, etc. However, the included responses are not limited. A user can have any kind of response based on his perception related to experiences, thoughts, belief, and prejudice, etc.



[12]

Figure 39: Collage 4.

Sample answers:

(1) Diversity

(2) Plurality

(3) Group

(4) Optimistic

(5) Candle

(6) Light

(7) Hope

(8) Flower

(9) Happiness.

After all these answers the string of responses is:

Milkbirthdayecology21021986Norfolkand1900hardworkDiversity

8.2 Shifting of alphabets

This step is significant, and it is introduced to protect from dictionary attack and linear attack. In this step, make the number string from answers of question numbers 4 and 5. In this step, it is necessary to shift the letters by the number of the remainder left after dividing by 26.

As the answer in 4 and 5 are 21021986 and 1900, the number shift would be calculated as:

Shift = 210219861900 mod 26

= 22

All the letters of the generated string from step 1 would be shifted by 22.

milkbirthdayecology21021986norfolkand1900hardworkdiversity

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
1	2	3	4	5	6	7	8	9	1	1	1	1	1	1	1	1	1	1	2	2	2	2	2	2	2

Table 4: Frequency analysis of letters.

Here, every letter is shifted by 22 places and starts from the letter "A" in the rotation. After shifting, the string becomes a very different string, which is mentioned below:

"Iehgxenpdzwuaykhkcu21021986jknbkhgwjz1900dwnzskngzeranoeapu"

It is easy to shift the strings through various programs in different languages. A sample program is available online on many websites [41].

```
#include <iostream>
using namespace std;
  // This function receives text and shift and
// returns the encrypted text
string encrypt(string text, int s)
```

```
{
    string result = "";
      // traverse text
    for (int i=0;i<text.length();i++)
    {
        // apply transformation to each character
        // Encrypt Uppercase letters
        if (isupper(text[i]))
            result += char(int(text[i]+s-65)%26 +65);
      // Encrypt Lowercase letters
// This step is for encrypting all lower case
// return value required
    else
        result += char(int(text[i]+s-97)%26 +97);
    }
      // Return the resulting string
    return result;
}
  // Driver program to test the above function
int main()
{
    string text="ATTACKATONCE";
    int s = 4;
    cout << "Text : " << text;
    cout << "\nShift: " << s;
    cout << "\nCipher: " << encrypt(text, s);
    return 0;
}
```

8.3 Splitting the above string into 10 chunks.

This step is significant and is directly related to the strength of the final password. In the final step, all the chunks would be encrypted through Whirlpool encryption, and each encrypted fragment would be transformed into a 128 character long string. Therefore, to increase or decrease the final length of the password, this step can be adjusted as per the requirement. Whirlpool encryption generates a 128 character long encrypted string irrespective of the length of the input string. Therefore, to randomize we can split the chunks into any proportion as desired.

Here, I have divided chunks into even parts and the 10th chunk would be small, equal or larger compared to the other nine chunks as the final output of step 2 may or may not be in a multiple of ten. The ten chunks for our string are shown in table 5.

Chunk	Data
1	Iehgxe
2	npdzwu
3	aykhkc
4	u21021
5	986jkn
6	bkhgwj
7	z1900d
8	wnzskn
9	gzeran
10	oeapu

Table 5: Splitting the strings into ten chunks.

In this step, it is effortless to split the string in chunks and it can be programmed as per the requirement. A sample program in C programming language is included below and is available on many websites [40].

```
#include <stdio.h>
#include <string.h>
 int main()
{
    char str[100];
    char splitStrings[10][10]; //can store 10 words of 10 characters
    int i,j,cnt;
    printf("Enter a string: ");
    gets(str);
    j=0; cnt=0;
    for(i=0;i<=(strlen(str));i++)
    {
        // if space or NULL found, assign NULL into splitStrings[cnt]
        if(str[i]==' '||str[i]=='\0')
        {
            splitStrings[cnt][j]='\0';
            cnt++;  //for next word
            j=0;    //for next word, init index to 0
//j= 0 is necessary.
        }
        Else
// This program belongs to https://www.geeksforgeeks.org/caesar-cipher/
        {
            splitStrings[cnt][j]=str[i];
            j++;
//just increasing the value of j by 1.
        }
// index is 0
    }
    printf("\nOriginal String is: %s",str);
    printf("\nStrings (words) after split by space:\n");
    for(i=0;i < cnt;i++)
        printf("%s\n",splitStrings[i]);
    return 0;
// This program belongs to https://www.geeksforgeeks.org/caesar-cipher/
}
```

[40]

8.4 Encryption of the chunks and merging outputs

As discussed earlier, Whirlpool encryption provides unique cipher texts for all the given input; the encrypted pieces would produce a unique and distinct cipher text which would be our password. This encryption can be done with many programming languages, and many websites provide such encryption free of cost.

In step 4, each chunk has been encrypted separately to avoid a linear-attack and then all encrypted results of 128 characters have been merged to generate a 1280 character long password.

step 4 is significant because it makes the algorithm extremely strong by providing the protective measures of Whirlpool encryption.

The whole string has been encrypted in chunks to avoid the linear-attack as by doing so there is no way possible for an attacker to generate the 1280 character long password by encrypting the original string through encryption. For Whirlpool encryption each chunk is a separate input, and every fragment is encrypted separately to produce ten different 128 character long lines.

Chunk No	**Data**	**Encrypted cipher text**
1	Iehgxe	7B592BC402218759B937425E742497806D20454139F19ABEDC73F404CDC3E24F10F32769D0926A0562D5D319FCE21291C88DB0BAE6E12F312712B5282AFF8A41
2	npdzwu	4CE9A5590B83177FD94906A523DF43FBF73574E5743D15A036C86E2D1D97DFA48EF4DD6B3459E0028EA51B61AC6D5ADDD8670C3D49A49EA378C7285788BF6CE1
3	aykhkc	B02675B1008AD11620B5011A055515C23F6B53A4355A220B4E0F2604A0D451EAC117D8916899DCABD574E919F4745E9B67EAA9AD48994B8A5B28D569B56A31D2
4	u21021	D4D02636D3856134E3B95E0247F89FCF2E408C2C614CC93F6FAC2E7BAB9903BC8B43D198E79FDDBE0A018A8E877D7702BB063C220899BDFF5EB7D4E5FF124EA3

5	986jkn	455A4A282FBA8010A91E956021A0F91CBD53481C2279120773D23B06B95B367D2A1763EEB6011989EB3A65E23E1EBE394AAAB8D0442E390AAF5A3FD8FBDFDB76
6	bkhgwj	ADA02278D2EE7BED82A7AF86C0ADF649C00A6D8C8685E5022FDF3D41C358D1CCB54622BC12FA643E58AF8C3C5E368CDD5D8CE639D12478E3099F742A7E73CD10
7	z1900d	71906328F523016C5D9E2997268E0FEE29429850ED9A0B99F27F95328C9341E1AEFA02622120F175E1E13A821E4D3A9C911B75A41CB2C2EA77174C1643A02AFB
8	wnzskn	C462C373B5827A247335C72C49712BE86250E9B5EDA0D76D296110EBF9E948E12D416293C4EC16F48213D9C79F2CD56B1993BCDF2AE5B49541714AD355DFE86D
9	gzeran	5CA12123CA7280553A1F0E7819958C24835777D5C425F02FEEB1CD21EE588498304599DBFAEC08A723575265C5C62D2E9BADA8875B9C5363B0F6E17FA35AA6C7
10	oeapu	F4118B95A62AD6D51CB1014DD3B50DCD9A476E7698364FD1F9651E01E68AD0A1456414C57CA64F676A5BFCEAFD0B2B72342DFA7CF40

Table 6: Encrypted chunks.

8.5 Final Output

```
        7B592BC402218759B937425E742497806D20454139F19ABEDC73F404CDC3E24F10
F32769D0926A0562D5D319FCE21291C88DB0BAE6E12F312712B5282AFF8A414CE9A559
0B83177FD94906A523DF43FBF73574E5743D15A036C86E2D1D97DFA48EF4DD6B3459E0
028EA51B61AC6D5ADDD8670C3D49A49EA378C7285788BF6CE1B02675B1008AD11620
B5011A055515C23F6B53A4355A220B4E0F2604A0D451EAC117D8916899DCABD574E919
F4745E9B67EAA9AD48994B8A5B28D569B56A31D2D4D02636D3856134E3B95E0247F89F
CF2E408C2C614CC93F6FAC2E7BAB9903BC8B43D198E79FDDBE0A018A8E877D7702BB
```

```
063C220899BDFF5EB7D4E5FF124EA3455A4A282FBA8010A91E956021A0F91CBD53481C
2279120773D23B06B95B367D2A1763EEB6011989EB3A65E23E1EBE394AAAB8D0442E39
0AAF5A3FD8FBDFDB76ADA02278D2EE7BED82A7AF86C0ADF649C00A6D8C8685E502
2FDF3D41C358D1CCB54622BC12FA643E58AF8C3C5E368CDD5D8CE639D12478E3099F7
42A7E73CD1071906328F523016C5D9E2997268E0FEE29429850ED9A0B99F27F95328C934
1E1AEFA02622120F175E1E13A821E4D3A9C911B75A41CB2C2EA77174C1643A02AFBC4
62C373B5827A247335C72C49712BE86250E9B5EDA0D76D296110EBF9E948E12D416293C
4EC16F48213D9C79F2CD56B1993BCDF2AE5B49541714AD355DFE86D5CA12123CA7280
553A1F0E7819958C24835777D5C425F02FEEB1CD21EE588498304599DBFAEC08A723575
265C5C62D2E9BADA8875B9C5363B0F6E17FA35AA6C7F4118B95A62AD6D51CB1014DD
3B50DCD9A476E7698364FD1F9651E01E68AD0A1456414C57CA64F676A5BFCEAFD0B2
B72342DFA7CF40AB49F3427D35294BDA3BC                                   [14]
```

CHAPTER 9

WHY ONLY WHIRLPOOL ENCRYPTION?

(1) Whirlpool offers 512 bits Hash code length which is the longest among all encryptions including MD family cryptosystems. This is the longest SHA encryption [39].

(2) Whirlpool encryption is resistant to all usual attacks and weaknesses to which all other encryptions are vulnerable except Whirlpool encryption [56, 57]

(3) Whirlpool encryption provides better compatibility for hardware and software due to the AES encryption based W cipher block [39].

(4) MD1, MD2, MD3, MD4, and MD5 have been developed as a successor of the past version to rectify vulnerabilities or weaknesses. The lastly developed MD family encryption MD5 is discovered with two messages having the same message digest on the order of 2^{64} operations, and the difficulty to find a message with given digest is on 2^{128} operations. Thus, previous MD family encryptions are no safer or more secure; no such events have been found for Whirlpool encryption [39].

(5) For the Hash value of any n-bit substring, the expected workload of generating a collision is of the order of $2^{(n/2)}$ executions [39].

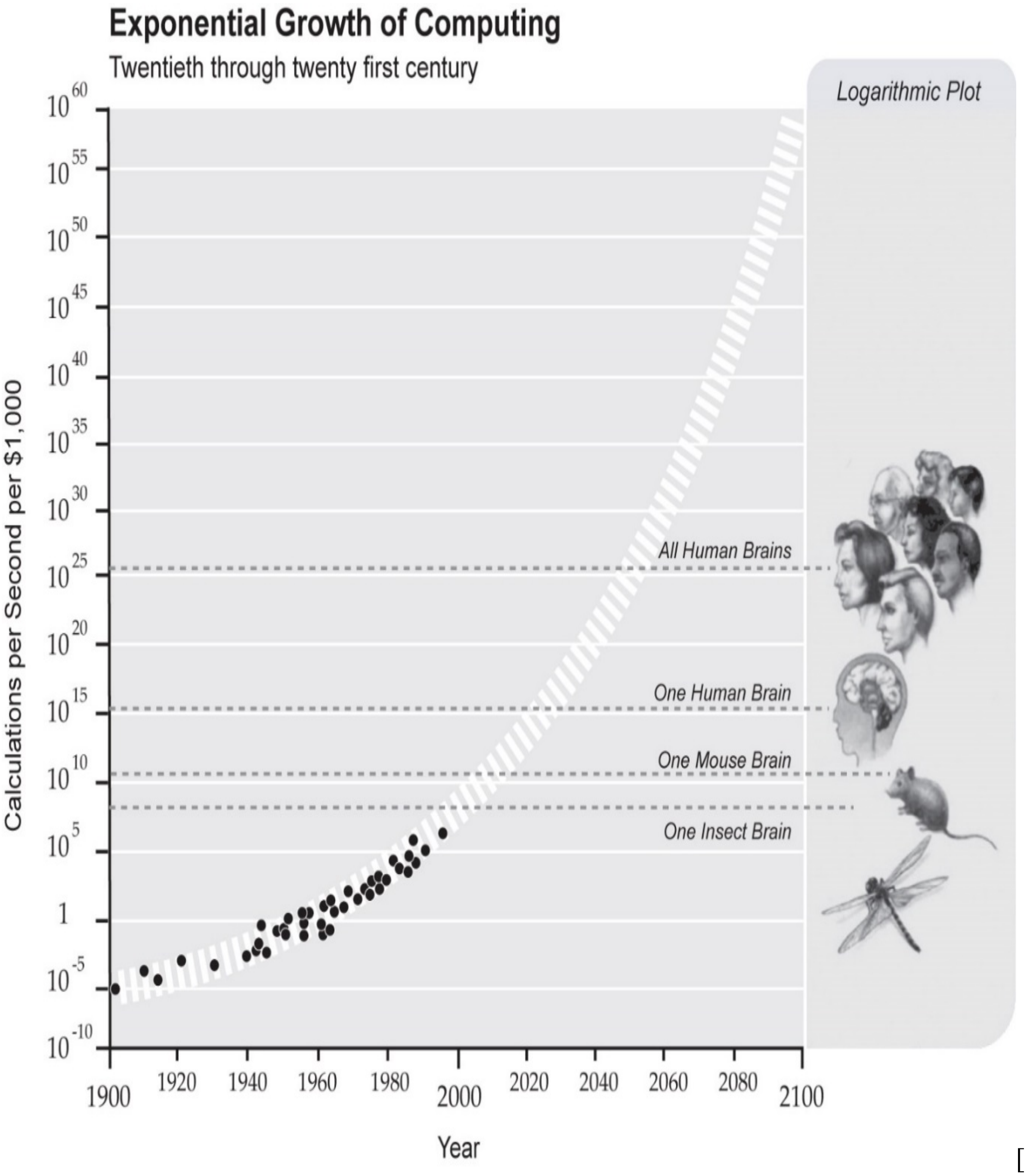
(6) The Whirlpool encryption is resistant to linear and differential attacks because it is not possible to find systematic correlations among any linear combinations for input bits and any linear combination of bits of the Hash result [58].

CHAPTER 10

COMPUTATIONAL SPEED TO ATTACK PASSWORDS

In today's era, the computational speed of computers is very high, and it will be more and more efficient in the future. The computational speed of computers at their inception was very low compared to today, but consistent research and enhanced processors has increased computational speed exponentially. This increased speed provides a fast and efficient password cracking mechanism. Computational speed has dramatically increased over time; therefore, more and more advanced password techniques have to be developed.

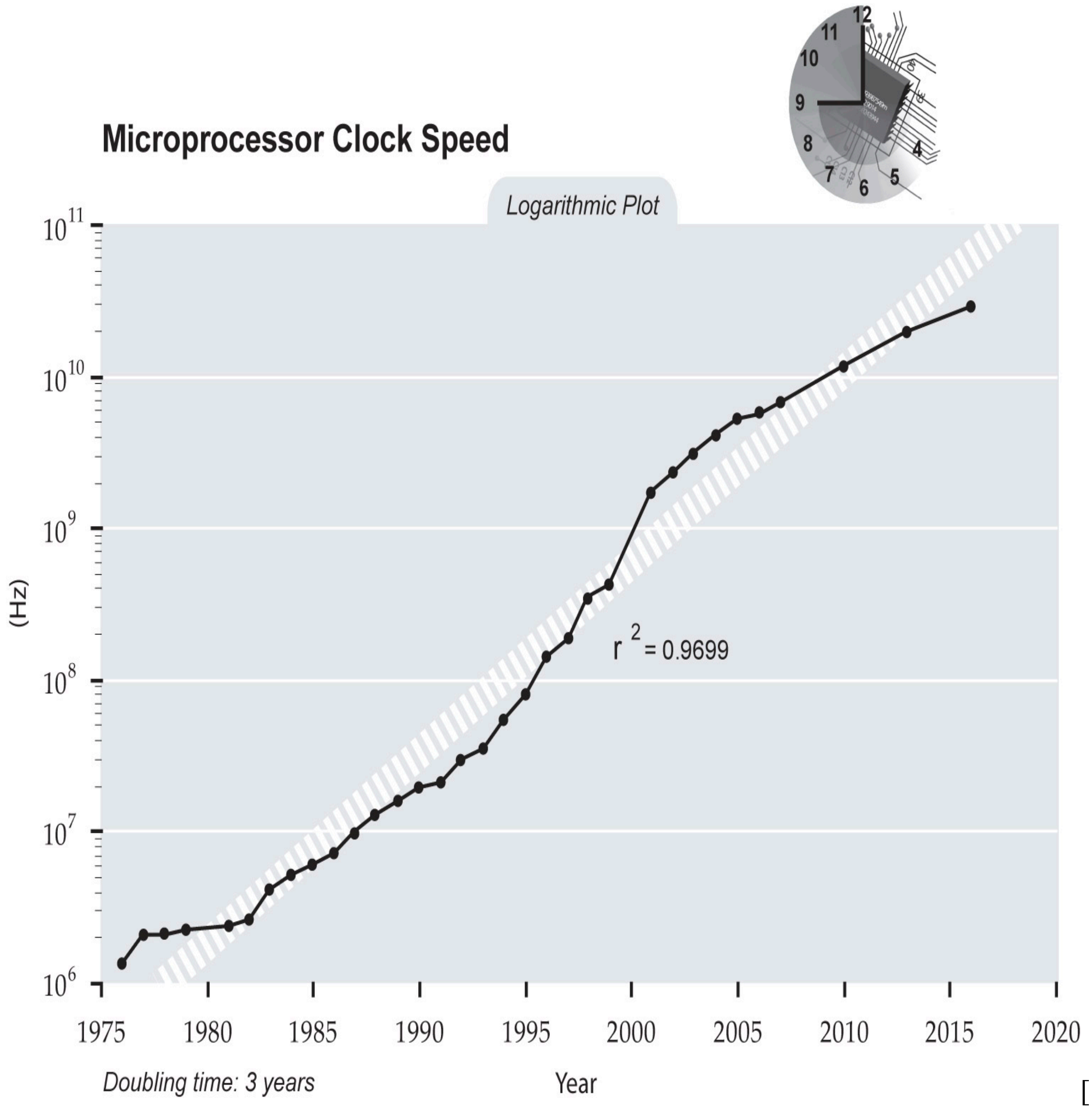
Computational speed has continuously risen since 1900, the inception phase of computers. Due to exhaustive current research in various computer parts, the efficiency of the computer and its computational power will definitely keep increasing. The continuously rising trend of computational speed is a potential threat to current password standards. Attackers apply various methods to compromise passwords, and often they use computers and botnets to attack passwords and compromise security systems. Therefore, with rising computational speed, it is necessary to develop effective password generating methods to provide better security to computers.



[15]

Figure 40: Computational speed development chart

Figure 41 indicates that the Clock Speed of Microprocessors has increased rapidly, which again indicates the need for more enhanced and difficult password development techniques.

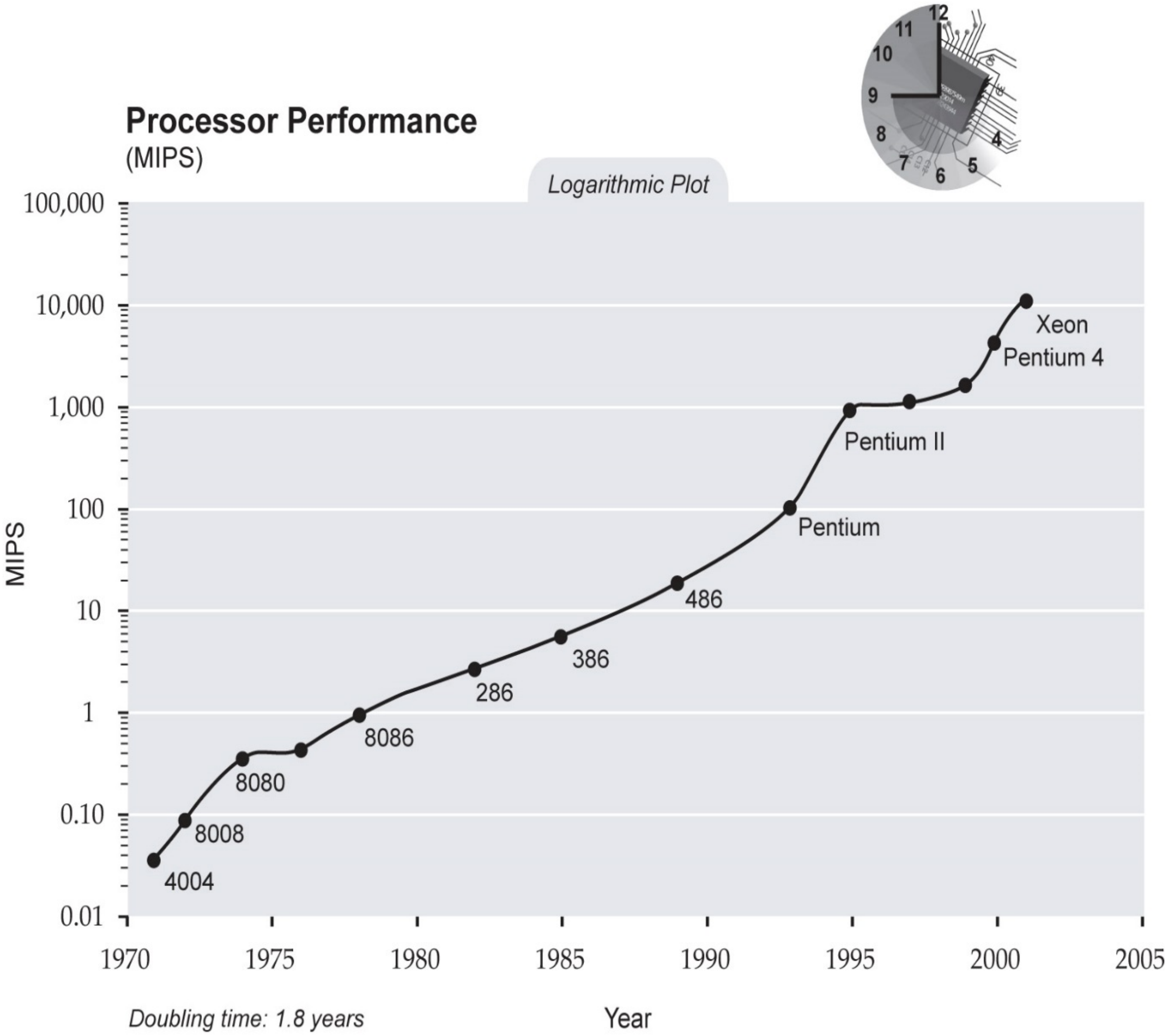


[15]

Figure 41: Microprocessor Clock Speed

The clock speed of Microprocessors is continuously increasing, and the graph shows that it is doubling almost every three years. Starting from 1975, when the speed was around 10^6 Hz, continuous research on the microprocessor has helped scientists drastically enhance microprocessor clock speed. Microprocessor clock speed has reached very close to 10^11 Hz.

Further, due to better Microprocessors and enhanced clock cycles, Microprocessors consistently show an exponential graph of performance. Computational speed is invertible proportionate to password effectiveness.



[15]

Figure 42: Microprocessor Performance

The graph shows that Microprocessor performance is almost doubled every couple of years. As the computer has become more and more advanced, the password must be strengthened accordingly to mitigate the risks of compromising the password using the computer.

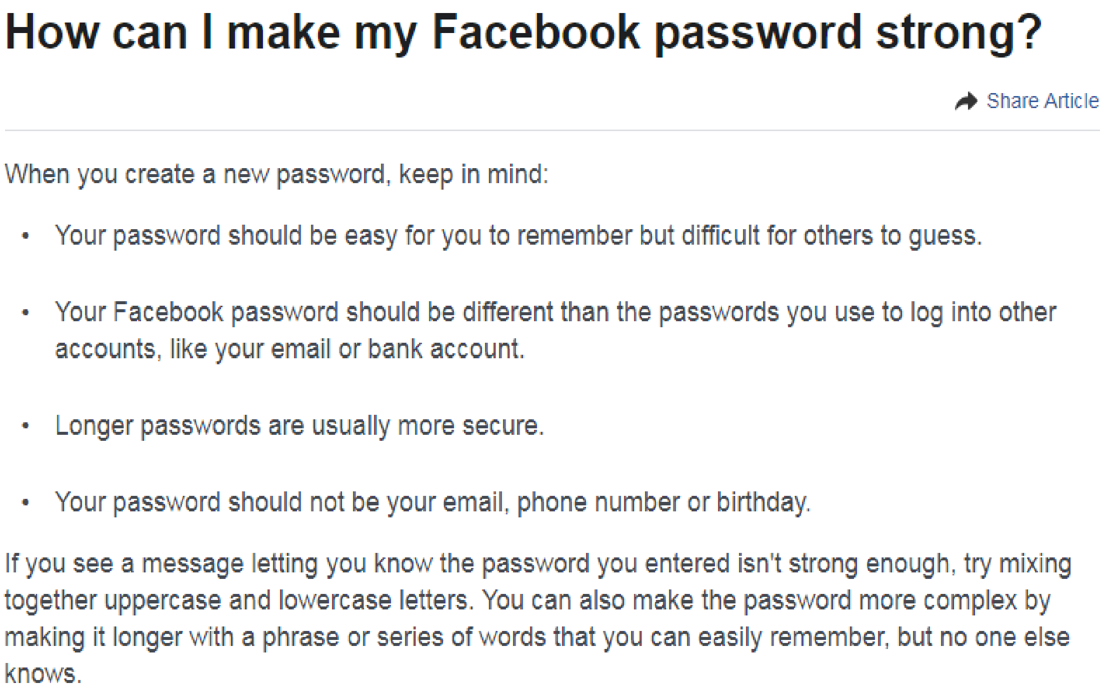
CHAPTER 11

ATTACK THROUGH MODERN COMPUTER AND SUPERCOMPUTER

Overview

Presently, there is no authentication technique existing where graphical authentication (based on human perception) and the Whirlpool encryption both are part of an authentication method. This research has been developed considering the extreme level of security and consistently increasing computational power to compromise any authentication algorithm. Graphical authentication is rarely used and even then only for limited uses such as Android applications. Graphical authentication is not very common because it is still vulnerable to shoulder surfing attacks. On the other hand, encryption techniques are used for securing/protecting files by transforming their data into encrypted forms.

Further encryption is also used to transfer the data from one place to another. Currently, encryption is not designed as an authentication technique itself with memorability. Therefore, this thesis is unique, and no similar methods or models focusing on strong passwords and memorability are available for comparison. However, in the research focusing on secured password systems, the strength of present passwords is analyzed. Currently, most of websites and applications have password length up to a maximum of fifteen characters. Often this kind of password system allows users to make their passwords in a combination of different characters, numbers and special characters. Social websites, such as Facebook.com, recommend the user make an easy password easily remembered. In comparison to this concept, the present thesis focuses on memorability and provides the same through graphical authentication. on the other hand, Facebook recommends that the chosen password should be easy to remember by the user but it should be difficult for others to guess. In such a scenario, users might write some passwords, and though it may be difficult for someone to predict or guess it, it would be very vulnerable to a dictionary attack. A dictionary attack would compromise all such passwords.



How can I make my Facebook password strong?

When you create a new password, keep in mind:

- Your password should be easy for you to remember but difficult for others to guess.
- Your Facebook password should be different than the passwords you use to log into other accounts, like your email or bank account.
- Longer passwords are usually more secure.
- Your password should not be your email, phone number or birthday.

If you see a message letting you know the password you entered isn't strong enough, try mixing together uppercase and lowercase letters. You can also make the password more complex by making it longer with a phrase or series of words that you can easily remember, but no one else knows.

[60]

Figure 43: Social networking website requirements for password.

Current password rules stress that the password length should be a length of varied range for different applications. Different applications have different requirements or expectations. Presently, authentication is required for various applications such as logging into online bank accounts, credit card accounts, online payments, etc. with specific password rules. Most banks require the password to be from six to ten characters. Email platforms also focus on password strength, and the popular email website Gmail.com requires that the user make a password at least eight characters long, and Gmail allows a maximum password length up to 15 characters. Gmail requires that the user have at least one upper case letter, lower case letter, number, etc. These kinds of rules are intended to help the user make complicated passwords [61]. In case of textual passwords, the length of the password and number of characters plays huge role for its strength.

Present password strength:

To demonstrate the new algorithm, the computational speed [15] of modern computers must be considered. *"On a modern computer (8 core, 2.8 GHz) using the SHA512 Hashing algorithm, it takes about 0.0017 milliseconds to compute a Hash. This translates to about 1.7*10^-6 seconds per password or 588235 passwords per second." [15]*

Various applications allow a varied range of password range from a small key space to a maximum of ten characters. These applications allow characters from A to Z and 0 to 9. For better password-protection, applications must have lengthy passwords [60]. The strength of various passwords depends on password length and the number of allowed characters. The strength of a password will increase if the number of characters are allowed to choose from increases because there is number of different combinations of characters. Further, if more characters are allowed in the password length, the password will be stronger because, again, there is a larger number of different combinations of characters in the password.

While designing this new algorithm, cyber-attacks such as linear attacks, shoulder surfing attacks, brute force attacks, dictionary attacks, and crypto analysis attacks have been taken into consideration and the proposed new algorithm (Akash Rao Secured Password Algorithm) has been found immune to all such kind of attacks. Further, Akash Rao Secured Password Algorithm has been developed with Whirlpool encryption which is extremely safe and no vulnerabilities have been found for Whirlpool encryption till now.

It is important to study and analyze the attack on current password expectations or rules with the current computational power of modern computers and the computational power of a supercomputer. Attacks on present passwords through modern computers and supercomputers are mentioned below, and the new algorithm is also demonstrated later in this chapter.

Attack to present passwords through the modern computer (8 core, 2.8 GHz) and Supercomputer

Attacking through Modern computer:

Graphical authentication provides better memorability to users [1] and the present password techniques, which are based on alphanumeric passwords, do not provide such memorability, which is definitely an important feature. It is important to mention that the new algorithm focuses on memorability along with high security compared to present password standards. As per the computational speed of modern computers (8 core and 2.8 GHz) and supercomputers (100000 times more efficient than modern computers) the computational speed can be calculated as per the computational speed. As present password patterns have different specifications, it is a good idea to check for the most robust password specification computational speed for a modern computer as well as a supercomputer. The maximum time for the fifteen character long present passwords would be 1.7 * 10 $^{\wedge-6}$ * 15$^{\wedge 94}$ seconds which comes to 19240691029805037337007333436724712465667387379695449527876792609264676671364113921243512017448266 years which is 20.52 times smaller compared to the new algorithm computational speed.

Attacking through Supercomputer:

Similarly, the supercomputer will require 1.7 * 10 $^{\wedge-11}$ * 15$^{\wedge 94}$ seconds which comes to 192406910298050373370073334367247124656673873796954495278767926092646766713641139212435120174 years which is around 20.27 times less period compared to the new algorithm. Thus, the present passwords would be compromised about 20 times faster compared to the new algorithm.

Attack on the proposed algorithm through modern computer (8 core, 2.8 GHz) and Supercomputer

Attacking through Modern computer:

To demonstrate the new algorithm, the computational speed [15] of modern computers must be considered. As mentioned earlier, the modern computer requires 1.7*10^-6 seconds per password [15]. The computational time required to compromise the new algorithm through the modern computer (8 core, 2.8 GHz) and supercomputer can be calculated in the same manner. For the new algorithm, the modern computer will require total computational time as follows

Computational speed = 1.7 * 10^ (-6) * 1280^36 seconds = 3901227004523352918491380377084313232309086716997815172879365899556307085313039066463723997970573331 Years [59].

Therefore, it is almost impossible for the modern computer to crack the password, and this is 20.52 times more years compared to the present password computational time as mentioned earlier. Thus, the modern computer will require around 20.52 times more years to crack this new algorithm, so the new algorithm is around 20 times more secure compared to present password standards.

Attacking the password through Supercomputer

As per the computational speed given for a supercomputer [15], the total time for a supercomputer to attack the password can be calculated in the same manner as the calculation for modern computers and supercomputers. The computational time for attacking the new algorithm can be calculated as follows:

Computational time = 1.7 * 10(-6) * 1280^36 * 10^ (-5) = 3901227004523352918491380377084313232309086716997815172879365899556307085313039066463723997970 years [59]. This calculation shows that the total number of years to compromise the new algorithm is around 20 times more years compared to the present password standards by an attack through a supercomputer.

The Summary table comparing present passwords and Akash Rao Secured Password Algorithm on various aspects.

No.	Comparison of present passwords and new algorithm		
		Present passwords	**Akash Rao Secured Password Algorithm**
1	Memorability	No	Yes
2	Concurrent authentication through Graphics and textual passwords both?	No	Yes
3	Does require multiple confidential information to create and break password	No	Yes
4	Encryption	No	Yes
5	Sufficiently long?	No (ranges from 4 to 15 characters)	Yes- 1280 characters
6	Dictionary Attack vulnerability	Vulnerable	Not vulnerable
7	Shoulder surfing vulnerability	Vulnerable	Not vulnerable
8	Brute Force Attack vulnerability	Around 20 times less secured compared to new algorithm	Around 20 times more secured compared to present passwords.
9	Computational time to attack though modern computer	Less time required. Around 20.52 times less years required compared to new algorithm	Extremely safe. Around 20.52 times more years compared to present passwords
10	Computational time to attack though Super computer	Less time required. Around 20.27 times less years required compared to new algorithm.	Extremely safe. Around 20.27 times more years compared to present passwords.

Table: 7 Summary table comparing present passwords and Akash Rao Secured Password algorithm.

Thus the newly developed Akash Rao Secured Password Algorithm provides a better solution not only with more secure throughput but also with better memorability.

CHAPTER 12

CONCLUSION AND FUTURE WORK

Summarizing Conclusion

In this thesis, an overview of graphical authentication was provided. This content encompassed various graphical authentication methods proposed by several researchers including their failures and weaknesses. Among these authentications methods, grouping for finding the targets and moving the targets is more important for the current research. Graphical authentication was introduced as an alternative to textual passwords. The primary purpose of researching graphical authentication from various researchers was to find an alternative for textual passwords which can provide better memorability. Graphical passwords provide better memorability compared to textual passwords [1] and, therefore, in the current research graphical authentication techniques have been investigated and analyzed.

After choosing graphical authentication considering its better memorability, the idea was further developed to use graphical authentication and consider the potential for shoulder surfing attacks. Therefore, in this research, to make it extremely difficult for the attacker (eavesdropper) to launch a shoulder surfing attack, the idea was developed in such a way that the user would use graphical authentication but the user would not hover the mouse to select or choose any graphical image. The user would like the response in the provided collage based on the perception only. This kind of idea makes it extremely difficult for someone to predict a user's password as the shoulder surfing attack is curbed because the user is not selecting an image on the computer screen and the user’s responses are based on his or her perception only. The idea was further developed to protect the algorithm from a potential dictionary attack or brute force attack. To protect from a dictionary attack, the concept of shifting the user's response character by character by a specific number of shifts was developed. To make it extremely randomized yet unique for the user, the number of shifts is generated based on the responses of the user which are unique for the user's confidential information. After shifting, the generated string is split into ten chunks, and each chunk is encrypted to generate a unique line which cannot be easily compromised by the attacker.

In this research, various encryption methods have been studied along with their weaknesses. Important encryption methods for the current research is MD family encryption and the concept of a Hash Function. After considering all the various encryption techniques and their potential weaknesses and successful attacks, the Whirlpool encryption has been chosen to encrypt the chunks. To overcome the linear-attack on the shifted string, the string has been split into ten pieces, and each chunk has been encrypted through Whirlpool encryption individually. By doing this, there is no way possible for the attacker to reach the final encrypted string by encrypting the original line. Because for Whirlpool encryption, each input is separate and irrespective of the length of information (all lengths within $2^{\wedge 256}$), it produces 512 bits message digest which means it generates 128 characters from total 36 different characters (26 English letters and ten numbers 0 to 9). After encrypting each chunk separately through Whirlpool encryption, the generated encrypted outputs are merged into one large string which is almost impossible for modern computers and supercomputers to crack through a brute force attack.

After developing this new algorithm (Akash Rao Secured Password Algorithm), the attack time for a modern computer (8 core, 2.8 GHz) as well as a supercomputer (one hundred thousand times more efficient than modern computers) was determined based on their computational speed. After calculating the speed, it is found that it is almost impossible for a modern computer as well as a super computer to compromise the password through a brute force attack for the newly developed Akash Rao Secured Password Algorithm.

Scope for Future Research Work:

The present research is thorough and leaves limited room for technical advancement. The current research has excluded the implementation of software for this new algorithm, and every step of the new algorithm has been done entirely manually and on an encryption website [14]. To make this new algorithm more efficient and time-saving, proper software can be implemented in the future. In addition to software implementation, psychometric, psychological, and psychiatric studies may help focus more on human perception. Tests like the Rorschach test can help researchers understand and improve user input based on perception. Also, such studies can increase understanding and protect a system from an attacker's perception.

REFERENCES

[1] Susan Wiedenbeck et al., "Authentication Using Graphical Passwords: Effects of Tolerance and Image Choice" Proceeding SOUPS '05 Proceedings of the 2005 symposium on Usable privacy and security Pages 1-12,Jul 2005

[2] Jain, A., Hong, L. and Pankanti, S. Biometric identification. CACM 43, 2 (2000), 91-98

[3] Coventry, L., De Angeli, A. and Johnson, G. Usability and biometric verification at the ATM interface. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI'03) (Fort Lauderdale, FL, USA, April 5-10, 2003). ACM Press, New York, NY, 153-160.

[4] Coventry, L., De Angeli, A. and Johnson, G. Usability and biometric verification at the ATM interface. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI'03) (Fort Lauderdale, FL, USA, April 5-10, 2003). ACM Press, New York, NY, 153-160.

[5] Jain, A., Hong, L., and Pankanti, S. Biometric identification. CACM 43, 2 (2000), 91-98.

[6] Brostoff, S. and Sasse, M.A. Are Passfaces more usable than passwords: A field trial investigation. In People and Computers XIV - Usability or Else: Proceedings of HCI 2000 (Bath, U.K., Sept. 8-12, 2000). Springer Verlag, 405- 424.

[7] A Study of Various Passwords Authentication Techniques by Aakansha Gokhale, Vijaya Waghmare

[8] Arash et al., International Journal of Computer Science and Information Security, 6(2) · December 2009 with 688 Reads

[9] Int. J. Pure Appl. Sci. Technol., 1(2) (2010), pp. 60-66 International Journal of Pure and Applied Sciences and Technology ISSN 2229 – 6107

[10] Usability Comparison of Over-the-Shoulder Attack-Resistant Authentication Schemes- Ashley Cain

[11] Survey on the Use of Graphical Passwords in Security- Haichang Gao et al

[12] www.free-images.com

[13] https://asecuritysite.com/encryption/whirl as under,

[14] https://www.browserling.com/tools/whirlpool-Hash

[15] https://thycotic.force.com/support/s/article/Calculating-Password-Complexity

[16] Authentication Using Graphical Passwords: Effects of Tolerance and Image Choice by Susan Wiedenbeck, Jim Waters, Jean-Camille Birget, Alex Brodsky, Nasir Memon

[17] A Study of Various Passwords Authentication Techniques by Aakansha Gokhale, Vijaya Waghmare

[18] Authentication Schemes for Session Passwords using Color and Images M Sreelatha et al.

[19] A Novel Soft Computing Authentication Scheme for Textual and Graphical Passwords- P.S.V Vachaspati et al.

[20] Authentication Scheme for Shoulder surfing using Graphical and Pair Based scheme- Ankush et al.

[21] Accurate Visual Memory for Previously Attended Objects in Natural Scenes- Andrew Hollingworth et al.

[22] The Design and Analysis of Graphical Passwords Ian Jermyn et al.

[23] Shoulder Surfing Defense for Recognition based Graphical Passwords Rohit Ashok Khot et al.

[24] familiarity-based graphical authentication Karen Renaud et al.

[25] Visual Passwords: Cure-All or Snake-Oil? Karen Renaud et al.

[26] Graphical Passwords: Learning from the First Twelve Years- Sonia Chiasson et al.

[27] Accurate visual memory for previously attended objects in natural scenes- Hollingworth Andrew et al.

[28] Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems - Antonella De Angeli et al.

[29] F. Craik and J. McDowd. Age recall and recognition. Journal of Experimental psychology: Learning, Memory, and Cognition, 13(3):474{479, July 1987

[30] I. Jermyn, A. Mayer, F. Monrose, M. Reiter, and A. Rubin. The design and analysis of graphical passwords. In 8th USENIX Security Symposium, August 1999.

[31] Do Background Images Improve "Draw a Secret" Graphical Passwords? Paul Dunphy et al.

[32] S Wiedenbeck, J Waters, JC Birget, A Brodskiy and N Memon. Authentication using graphical passwords: effects of tolerance and image choice. SOUPS'05, CMU, USA. ACM Press

[33] A. Stubble eld and D. Simon. Inkblot Authentication, MSR-TR-2004-85. Technical report, Microsoft Research, 2004.

[34] P. Dunphy and J. Yan. Do background images improve \Draw a Secret" graphical passwords? In 14th ACM Conference on Computer and Communications Security (CCS), October 2007

[35] Comparison Based Analysis of Different Cryptographic and Encryption Techniques Using Message Authentication Code (MAC) in Wireless Sensor Networks (WSN) by Sadaqat Ur Rehman et al.

[36] Cryptanalysis of MD2 by Lars Knudsen et al.

[37] Analysis and Design of Cryptographic Hash Functions Bart PRENEEL

February 2003

[38] A Guide to Hash Algorithms by Britt Savage (GIAC) in 2003

[39] The Whirlpool Secure Hash Function by William Stallings.

[40] https://www.includehelp.com/c-programs/c-program-to-split-string-by-space-into-words.aspx

[41] https://www.geeksforgeeks.org/caesar-cipher/

[42] Brute-force and dictionary attack on Hashed real-world passwords- B Brumen et al.

[43] https://www.nsa.gov/Portals/70/documents/about/.../wwii/german_cipher.pdf

[44] Introduction to Cryptography with Coding Theory – Wade Trappe

[45] Diffie-Hellman: Key Exchange and Public Key Cryptosystems Sivanagaswathi Kallam

[46] Twenty Years of Attacks on the RSA Cryptosystem- Dan Boneh

[47] A Generalized Wiener Attack on RSA- Johannes Blomer et al.

[48] http://www.partow.net/programming/Hashfunctions/

[49] https://www.nytimes.com/2000/10/03/business/technology-us-selects-a-new-encryption-technique.html

[50] https://www.abebooks.com/book-search/author/biham-eli-adi-shamir/

[51] Linear Cryptanalysis method for DES cipher- Mitsuru Matsui 1998

[52] Optimal Resistance against the Davies and Murphy Attack by Donald Davis et al.

[53] https://paginas.fe.up.pt/~ei10109/ca/des-vulnerabilities.html

[54] https://www.recordskeeper.co/blog/Hash-function-attacks/

[55] Communication Theory of Secrecy Systems -By C. E. SHANNON

[56] Black-Box Analysis of the Block-Cipher-Based Hash-Function Constructions from PGV by J. Black

[57] Hash Functions based on block ciphers: a synthetic approach by Bart Preneel

[58] Preneel, B. 1993. Differential Cryptanalysis of Hash Functions Based on Block Ciphers, ACM Conference on Computer and Communications Security, pp. 183–188

[59] https://web2.0calc.com/

[60] https://www.facebook.com/help/124904560921566?helpref=topq

[61] https://support.google.com/accounts/answer/32040?hl=en

[62] https://www.thebalance.com/create-secure-credit-card-pin-or-password-960788

[63] https://www.betterbuys.com/estimating-password-cracking-times/

[64] https://www.rsaconference.com/writable/presentations/file_upload/cryp-203.pdf

VITA

Old Dominion University
Department of Electrical and Computer Engineering
Norfolk, VA 23529

Akash Harendrakumar Rao Alias Brahmbhatt received a Bachelor of Engineering in Electronics and Communications Engineering from Gujarat University in 2011 with excellent academic performance. After graduation, he enhanced skills in the manifold and worked in the industries in varied domains. Currently he is pursuing a Master of Science in Electrical and Computer Engineering and holds a 4.0 GPA overall.