ABSTRACT

In today's Modern Age, where everything we do is tracked by someone or the other by legal or illegal means. Privacy and data security is a major concern for many. Leaked Passwords, Images, or messages cause a lot of trouble for many people. These leaks could happen via System hack, People taking screenshots, unauthorized person reading text within your system (Shared PC). The website WallPart (intentionally not linked to) claims to be "the world's largest online shop of posters...with over 10 billion images." What they do not tell you is that their database is filled with stolen and copyrighted images from photographers around the world. Leaked Passwords lead to many compromised accounts all over the world. Even One-One messages are being seen by some 3rd party over the internet.

Almost 4 out of 5 online users have same password for almost all the webIDs. This leads to a hectic security issue which the service provider face, be it google or Facebook. They are big tech giants and can still give provident security to the users, but not every webId is secure from cyber-attacks. We must not take this lightly that someone can breech our webId and take our personal data. Hackers need not to attack the most secure webId like Gmail or yahoo, but any other id i.e. that has the same password because it's convenient to have a common password. hackers make use of this common mistake every web user do. That is to have a common password everywhere. They can retrieve password from less secure webId and then use them to access strongly secure sites. We can avoid it, web vulnerability, by having many and multiple password on all WebId.

These are some of the problems that we may face one day. In order to overcome such problems faced by the technology users the SecureVault (Data security software) Window PC based application is not only Intuitive in use but also plays a pivotal role in privacy security. This Secure Vault software serves the purpose of storing multiple password just by remembering one password to login in the software, By using this software, it is easy we can have multiple Passwords on various webID, just having one unique VaultID and a simple secure password for the software, can provide a person a great edge of security in the world of internet.

This Project aims to provide a safe and easy way to store passwords, Messages and Images, Thus Protecting the privacy of User in windows Environment. Existing softwares either are expensive or does not contain all the features in one container which is not convenient for any user. The online tools pose a risk of data being stolen and many users mistrust Cloud Storage. This Project proposes to solve this by providing an offline software with all the features of text and image encryption. It also provides an encrypted way of sharing the information. This Software achieve this by using various cryptographic algorithm such as RSA, AES and substitution ciphers. This software can successfully store the information on the device and is capable of retrieving it to 100% accuracy. The Software takes at max 100MB of RAM space even while doing heavy computations. This Software can handle text of 100MB and Images of JPG and PNG type, which are the most common format for images. It performs good even on old end laptop that supports x64 windows operating system.

LIST OF CONTENTS

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

1.1 DOMAIN INTRODUCTION

In this world of growing technologies everything is digitalized. With large number of works opportunities, the data Human mind should keep track of has also increased. Manual handling of the employee records poses huge difficulties and challenges. The use of paper work for handling the process of storing the information of the new and existing password could lead to human error, papers may end up in the wrong hands and moreover its time consuming, Thus, there is a need of software that can handle the WebId and password of large number of WebId. Similarly, we might need to keep some textual information in our system that we would not want to share, and some textual information that we want to share among a few. This could be a daunting task and not so easy for a normal user. This software can provide message security for the user and they will be able to encrypt the message with the same password.

1.2 PROJECT INTRODUCTION

The main objective of this project is to provide a user friendly yet less time-consuming process of storing Password information of multiple WebIds, Encryption of private messages using a single password of user's own, and a different password for sharing a private message, The file generated will be readable only by this software, This software will allow multiple Users on a same system. It will also provide the feature of Storing of images in the system itself but in an encrypted format that is unreadable by any software present in the system, user can share that file as well and thus protect or choose to share password to only a limited no. of users that the user feel worthy of seeing, it's will not be possible for a third person to look into the image without knowing the password that was set by the first user. This also increase the security for the cases where the hardware itself gets stolen or lost. It assures the user that only user can see the data and no one else.

Some of the project's scope are :

- Access to information and resources
- Ability to accommodate large user base
- Secure Password protection
- Secure Messages and provide storing and secure sharing
- Secure Images and provide storing and secure sharing
- Easy to use Interface
- Scalable software

The goal of the project is to deliver an Application software that can keep the password, message and image information of the user safe and retrievable, only by authorized people.

The objectives of the system are as follows:

- Design a system-based application Window to enter requirements like employee's web ID details and Password details.
- Well-designed database to store User information.
- A user friendly front-end environment for the user to interact.

1.3 OUTLINE OF PROJECT

The project describes a small,in size, software which would be useful to any person what uses internet on daily basis. The user can have a look who uses the software

and can also have multiple accounts, along with many WebIds and Password. Just only one VaultID and password. User could also Store or share their private messages as well as images.

- Cryptography or cryptology (from Ancient Greek: κρυπτός, romanized: kryptós "hidden, secret"; and γράφειν graphein, "to write", or -λογία -logia, "study", respectively) is the practice and study of techniques for secure communication in the presence of third parties called adversaries. More generally, cryptography is about constructing and analyzing protocols that prevent third parties or the public from reading private messages; various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation are central to modern cryptography. Modern cryptography exists at the intersection of the disciplines of mathematics, computer science, electrical engineering, communication science, and physics. Applications of cryptography include electronic commerce, chip-based payment cards, digital currencies, computer passwords, and military communications.
- Cryptography prior to the modern age was effectively synonymous with encryption, the conversion of information from a readable state to apparent nonsense. The originator of an encrypted message shares the decoding technique only with intended recipients to preclude access from adversaries. The cryptography literature often uses the names Alice ("A") for the sender, Bob ("B") for the intended recipient, and Eve ("eavesdropper") for the adversary. Since the development of rotor cipher machines in World War I and the advent of computers in World War II, the methods used to carry out cryptology have become increasingly complex and its application more widespread.
- Modern cryptography is heavily based on mathematical theory and computer science practice; cryptographic algorithms are designed around computational hardness assumptions, making such algorithms hard to break in practice by any adversary. It is theoretically possible to break such a system, but it is infeasible to do so by any known practical means. These schemes are therefore termed computationally secure; theoretical advances, e.g., improvements in integer

factorization algorithms, and faster computing technology require these solutions to be continually adapted. There exist information-theoretically secure schemes that provably cannot be broken even with unlimited computing power—an example is the one-time pad—but these schemes are more difficult to use in practice than the best theoretically breakable but computationally secure mechanisms.

- The growth of cryptographic technology has raised a number of legal issues in the information age. Cryptography's potential for use as a tool for espionage and sedition has led many governments to classify it as a weapon and to limit or even prohibit its use and export. In some jurisdictions where the use of cryptography is legal, laws permit investigators to compel the disclosure of encryption keys for documents relevant to an investigation. Cryptography also plays a major role in digital rights management and copyright infringement of digital media. The first use of the term cryptograph (as opposed to cryptogram) dates back to the 19th century—originating from The Gold-Bug, a novel by Edgar Allan Poe.
- Until modern times, cryptography referred almost exclusively to encryption, which is the process of converting ordinary information (called plaintext) into unintelligible form (called ciphertext). Decryption is the reverse, in other words, moving from the unintelligible ciphertext back to plaintext. A cipher (or cypher) is a pair of algorithms that create the encryption and the reversing decryption. The detailed operation of a cipher is controlled both by the algorithm and in each instance by a "key". The key is a secret (ideally known only to the communicants), usually a short string of characters, which is needed to decrypt the ciphertext. Formally, a "cryptosystem" is the ordered list of elements of finite possible plaintexts, finite possible cyphertexts, finite possible keys, and the encryption and decryption algorithms which correspond to each key. Keys are important both formally and in actual practice, as ciphers without variable keys can be trivially broken with only the knowledge of the cipher used and are therefore useless (or even counter-productive) for most purposes. Historically, ciphers were often used directly for encryption or decryption without additional procedures such as authentication or integrity checks. There are two kinds of cryptosystems: symmetric and asymmetric. In symmetric systems the same key (the secret key) is used to encrypt and decrypt

a message. Data manipulation in symmetric systems is faster than asymmetric systems as they generally use shorter key lengths. Asymmetric systems use a public key to encrypt a message and a private key to decrypt it. Use of asymmetric systems enhances the security of communication. Examples of asymmetric systems include RSA (Rivest–Shamir–Adleman), and ECC (Elliptic Curve Cryptography). Symmetric models include the commonly used AES (Advanced Encryption Standard) which replaced the older DES (Data Encryption Standard).

- In colloquial use, the term "code" is often used to mean any method of encryption or concealment of meaning. However, in cryptography, code has a more specific meaning. It means the replacement of a unit of plaintext (i.e., a meaningful word or phrase) with a code word (for example, "wallaby" replaces "attack at dawn").
- Cryptanalysis is the term used for the study of methods for obtaining the meaning of encrypted information without access to the key normally required to do so; i.e., it is the study of how to crack encryption algorithms or their implementations. Some use the terms cryptography and cryptology interchangeably in English, while others (including US military practice generally) use cryptography to refer specifically to the use and practice of cryptographic techniques and cryptology to refer to the combined study of cryptography and cryptanalysis. English is more flexible than several other languages in which cryptology (done by cryptologists) is always used in the second sense above. RFC 2828 advises that steganography is sometimes included in cryptology.
- The study of characteristics of languages that have some application in cryptography or cryptology (e.g. frequency data, letter combinations, universal patterns, etc.) is called cryptolinguistics.
- Symmetric-key cryptography refers to encryption methods in which both the sender and receiver share the same key (or, less commonly, in which their keys are different, but related in an easily computable way). This was the only kind of encryption publicly known until June 1976.
- Symmetric key ciphers are implemented as either block ciphers or stream ciphers. A block cipher enciphers input in blocks of plaintext as opposed to individual characters, the input form used by a stream cipher.

- The Data Encryption Standard (DES) and the Advanced Encryption Standard (AES) are block cipher designs that have been designated cryptography standards by the US government (though DES's designation was finally withdrawn after the AES was adopted). Despite its deprecation as an official standard, DES (especially its still-approved and much more secure triple- DES variant) remains quite popular; it is used across a wide range of applications, from ATM encryption to e-mail privacy and secure remote access. Many other block ciphers have been designed and released, with considerable variation in quality. Many, even some designed by capable practitioners, have been thoroughly broken, such as FEAL.
- Stream ciphers, in contrast to the 'block' type, create an arbitrarily long stream of key material, which is combined with the plaintext bit-by-bit or character-by-character, somewhat like the one-time pad. In a stream cipher, the output stream is created based on a hidden internal state that changes as the cipher operates. That internal state is initially set up using the secret key material. RC4 is a widely used stream cipher. Block ciphers can be used as stream ciphers.
- Cryptographic hash functions are a third type of cryptographic algorithm. They take a message of any length as input, and output a short, fixed length hash, which can be used in (for example) a digital signature. For good hash functions, an attacker cannot find two messages that produce the same hash.
- MD4 is a long-used hash function that is now broken; MD5, a strengthened variant of MD4, is also widely used but broken in practice. The US National Security Agency developed the Secure Hash Algorithm series of MD5-like hash functions: SHA-0 was a flawed algorithm that the agency withdrew; SHA-1 is widely deployed and more secure than MD5, but cryptanalysts have identified attacks against it; the SHA-2 family improves on SHA-1, but is vulnerable to clashes as of 2011; and the US standards authority thought it "prudent" from a security perspective to develop a new standard to "significantly improve the robustness of NIST's overall hash algorithm toolkit." Thus, a hash function design competition was meant to select a new U.S. national standard, to be called SHA- 3, by 2012. The competition ended on October 2, 2012 when the NIST announced that Keccak would be the new SHA-3 hash algorithm. Unlike block and stream ciphers that are invertible, cryptographic