Project Proposal

PUSL2021 Computing Group Project (23/AY/AU/M)

Group B70

Advanced Password Authenticator and File Encryption and Decryption Tool

This Software can encrypt and decrypt Files this software is protected by very strong password protection (Explained Bellow)

Key Features

- **Regular Password Rotation**: Every minute, the system modifies the created password. Through reducing the window of vulnerability in the event that a password is compromised, this quick rotation improves security.
- **Hourly Encryption Key Rotation**: The encryption key that is used to safeguard the created passwords is rotated on a regular basis. By making sure that even if an attacker somehow obtains a key, it quickly becomes obsolete, this offers an additional layer of security.
- **Daily Encryption Key Value Modification**: Every day, the system adjusts the encryption key's value in addition to rotating it. By making it incredibly difficult for attackers to predict or reverse-engineer the key's value, this further improves security.

User Input: The user selects one or more files they want to encrypt using the File Encryption/Decryption Tool.

Encryption Algorithm: The tool uses a strong encryption algorithm, such as Advanced Encryption Standard (AES), to transform the content of the selected file(s) into an unreadable format. AES is a widely used symmetric-key encryption algorithm known for its security.

Encryption Key: The user is required to set a secure encryption key or passphrase. The key is used as input to the encryption algorithm. It's essential that the key is strong and not easily guessable.

Key Derivation: The tool derives an encryption key from the user's passphrase. The key derivation process can use techniques like key stretching and salting to strengthen the key.

Encryption Process: The encryption algorithm takes the user's key and the file's content as input and performs mathematical operations to transform the data into ciphertext. The ciphertext appears as random characters and is stored in a new file.

Secure Key Handling: The encryption key is securely managed by the tool. It is not stored in plain text, and the user may be required to enter the key each time they want to decrypt a file.

Decryption:

User Input: The user selects the encrypted file they want to decrypt using the File Encryption/Decryption Tool.

Decryption Algorithm: The tool uses the same encryption algorithm (AES) to reverse the encryption process. This time, it takes the ciphertext from the selected file as input.

Key Input: The user provides the same encryption key that was used for encryption. Without the correct key, decryption is not possible.

Decryption Process: The tool uses the key to perform the reverse operations on the ciphertext, converting it back into the original, readable content of the file.

Secure Key Handling: The decryption key is again managed securely and is not stored in plain text.

Result:

After the decryption process, the user can access the original content of the file, which is in the same format as it was before encryption. The user can now use the file as usual.

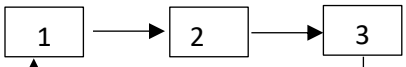
It's important to note that the security of the entire system relies on the strength of the encryption key. If the key is weak or compromised, the security of the encrypted files is also at risk. Users should choose strong, unique keys and keep them confidential to ensure the security

of their encrypted files. Additionally, the File Encryption/Decryption Tool should employ secure key management practices to protect the encryption keys from unauthorized access.

In the event of a hacking attempt, the system dynamically changes its password as a security measure. This password alteration occurs at minute intervals, enhancing security by continuously updating access credentials.

A=#	I=@	Q
B	J	R
C	K	S
D	L	T
E=!	M	U
F	N	V
G	O=$	W
H	P	X
1st Char Set	2nd Char Set	3rd Char Set

In every minute 1st char set changes in to 2nd char set, 2nd char set changes in to 3rd char set, 3rd char set changes in to 1st char set.



After one day the system will change first letter and last letter of this password. According to following system.

As the first step system will get the last letter of the date.

2023/01/08

Last letter is 8.

Day	0	1	2	3	4	5	6	7	8	9
Key	3	2	1	1	2	3	3	2	1	3

Key means char set.

If the day is 8 key = 1

Then the password's firs letter and last letter will change in to 1st char set. This operation will happen in the begin of the day at 00:00h.

This operation will run in in both user's system and authentication software. This will work according to the international time. GSM +05.30h. so there isn't any chance to occur error or password miss matching. Also its impossible to guess or hack password because whenever they are try to hack this password it will take at least one minute to connect to this system. If they try multiple passwords, the system will locks automatically and it will indicate it. This concept created by based on Zero trust concept.

Users will get only two attempts to enter password. This method can use for systems which needs high-information security. If someone try to decode the password, also its not a possible thing because we change this character set in every month.

Determine the total number of combinations for a password of six characters, each of which can be selected from a set of 62 characters. You multiply 62 by 6, which equals:

62^6 = 56,800,235,584

Therefore, you may create around **56.8 billion unique passwords in a month** using a six-character password and changing one character per minute. Password changes at this frequency can greatly improve security.

You may figure out how long it takes by making the following calculation, assuming an attacker can try 1,000 passwords per second, which is a plausible rate for current technology and software:

1,000 attempts per second divided by 56,800,235,584 total passwords equals 56,800,235,584 seconds.

So, it would take approximately 656,059 days to try all 56.8 billion passwords at a rate of 1,000 attempts per second. This is equivalent to roughly 1,798 years.