Pathway For a More Discrete Fintech Application

[1]J Jesy Janet Kumari, [2]Seema Patil, [3]Shobha T, [4]Bhoomika R and [5]G Bhargav Teja
[1]Dept. of AI & ML, New Horizon College of Engineering, Bangalore, India.
[2,3,4,5]Dept. of CSE, The Oxford College of Engineering, Bangalore, India.
[1]ebijesy.j@gmail.com, [2]theseema@gmail.com, [3]theshobha@gmail.com, [4]iambhumi5@gmail.com,
[5]tejagbhargav@gmail.com

Article Info
Jenitta J and Swetha Rani L (eds.), *International Conference on VLSI, Communications and Computer Communication*,
Advances in Intelligent Systems and Technologies,
Doi: https://doi.org/10.53759/aist/978-9914-9946-1-2_28

Abstract— The addition of the Secure Hash Algorithm SHA-256, the Advanced Encryption Standard AES-128, and dynamic polynomialswitchingintheLinearFeedbackShiftRegistersenhancesthesecurityof stream cipher. Numerous studies concluded that this introduction strengthens the stream cipher's resistance to cryptanalysis. In order to provide a distinct understanding of these designs, this study intends to present a thorough assessment that highlights current attempts to put this concept into practice. The process of creating new designs will be aided by this vision.

Keywords—AES-128, Encryption, SHA-256 (Secure Hash Algorithm), Secret Key, LSFR (Linear Feedback Shift Register), Cryptography, Decryption.

I. INTRODUCTION

Cryptography can also be termed as “Cryptology”. [1] It literally means the study of techniques and principals for making the process of communication confidential without the presence of any non-adversarial behavior. It unravels and ravels the content of message from digital data sender and the receiver. Cryptography refers to the science/study of encompassing the method of converting a graspable message into one that ungraspable and reconverting the message back to its original form. Internet and network communication is playing a crucial role to transfer large amount of digital data in copious fields. Digital data might be transmitted through insecure channel from sender to receiver. [2] Different techniques and methods have been using by public and private sectors to protect confidential data from hackers because of the security of digital data is vital issue. One of the most important and well-explored methods for protecting digital data from the hackers is cryptography, which employs crucial dual operations of encryption initially and decryption at the last. Data is encoded using the encryption process so that it cannot be easily read by outsiders. [3] This step has the capacity to transform the original data (Plaintext)into the illegible Cipher text format. The authorized individual must next perform the decryption process. Decryption is contrary of encryption. It is the process to convert ciphertext into plain text without missing any words in the original text. Cryptography uses calculations, certain substitutions, and permutations, either with or without a key, to carry out these operations.

A Linear Feedback Shift Register can be used to create a pseudo-random sequence (LFSR). For both software and hardware implementation, LFSRs are straightforward, quick, and simple. With the same uniform statistical distribution of 0s and 1s as a truly random sequence, they are able to produce pseudo-random sequences. [4] However, due to the ease with which the design of an LFSR of length n-bits maybe discovered by examining the 2n succeeding bits of its sequence using the “Berlekamp-Massey” algorithm, they are not cryptographically secure. [5] LFSR-based stream cyphers are susceptible to a variety of attacks because of their intrinsic linearity, including quick algebraic attack and correlation attack. One of the industry's most secure has hing algorithms is SHA-256. The government mandates that SHA-256 be used by its agencies to secure specific sensitive data.

There are three factors on which the security of SHA-256 is based, firstly, the problem is obtaining the initial data from the hash value is intrinsically impossible. To generate the original data, a brute-force attack would need to be conducted 2256 times. [6] Secondly, it is immensely implausible that two messages will have the same hash value. The possibility of two hash values matching is extremely small and is unimaginably remote. Lastly, a peripheral change to the initial data changes the hash value so significantly that it is not immediately clear that the new hash value is derived from the same the avalanche effect refers to his phenomenon in data. One of them Ost secure hashing algorithms available is SHA-256. [7] The government mandates that SHA-256 be used to secure specific sensitive data by its agencies. Finally, a minor alteration to the source data leads the hash value to vary so enormously that it is difficult to determine from indistinguishable data; this is known as the “Avalanche Effect”.

II. ALGORITHMS

AES (Advanced Encryption Standards)

The Advanced Encryption Standard (AES) algorithm, which was released by the "National Institute of Standards and Technology"(NIST) in the year 2000, is one of the most admired and commonly used symmetric block cypher encryption algorithms in use all over the world. [8] The prime goals of this algorithm are to replace the "Data Encryption Standard" (DES) algorithm after some of its vulnerabilities came to limelight. To introduce a novel block cypher method to encrypt and decrypt data with complicated and powerful structure, NIST invited professionals from everywhere who are involved in encryption and data security. This method, which issued around the world in both hardware and software, has a distinctive structure that makes it ideal for encrypting and decrypting confidential data. [9] When using the AES algorithm to encrypt data, hackers have a rough time decrypting it, till date there is not any evidence to break this algorithm. AES has the capacity to deal with three different key sizes such as AES128,192 and 256 bit and each of these ciphers has 128-bit block size. This paper will provide an overview of AES 128 algorithm and its implementation in an application.

Basic Structures:

"The National Institute of Standards and Technology" (NIST) (Fig 1,2) produced the Advanced Encryption Standard (AES) algorithm, one of them Ost popular and commonly used symmetric block cypher encryption algorithms, in 2000. After various susceptible parts of the DES algorithm surfaced, the primary goals of this algorithm were to replace it. [10] NIST asked specialists in encryption and data security from around the globe to present an ovel block cypher method for encrypting and decrypting data with strong and intricate structure. There is currently no corroboration that this algorithm is shattered. Three unambiguous key sizes, including AES128, 192 and 256bits, can be administered by AES, and each of these cyphers has a 128-bit block size. An overview of the AES 128 algorithm and how it is used in an application will be given in this paper

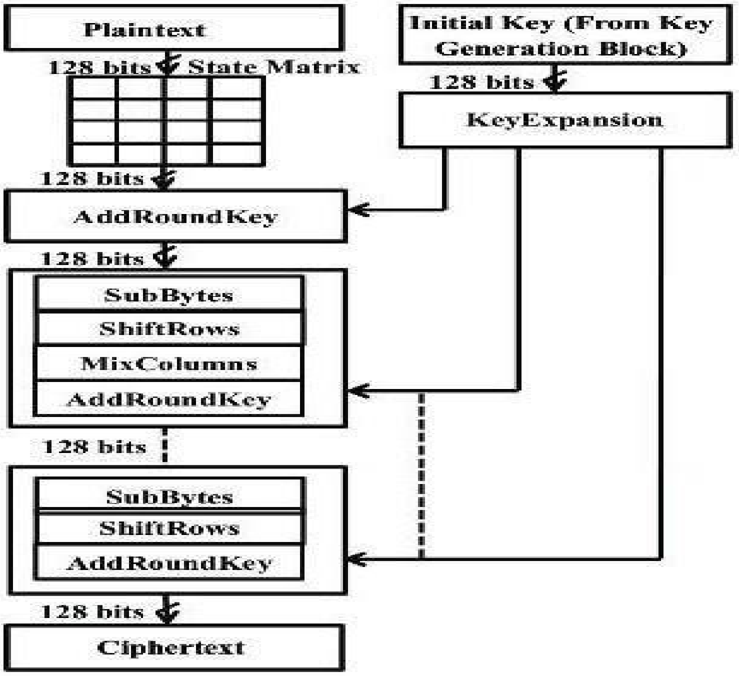


Fig 1. Basic Structure.

Crucial Features of AES

Safety

The capacity of competing algorithms to with stand assault in comparison to other ciphers submitted was to be evaluated. The most crucial aspect of the competition was to be security strength.

Cost

The potential algorithms were to be assessed on their computational and memory efficiency with the goal of being released on a worldwide, nonexclusive, and royalty-free basis.

Implementation

The algorithm's adaptability, suitability for hard ware or software implementation, and general simplicity were factors that needed to be taken into account.

Encryption of AES Algorithm

Encryption is a popular technique that plays a major role to protect data from intruders. To do that it relies on a number of rounds and inside each round comprise off our sub-processes. Four steps that are require to encrypt128-bitblockisas discussed below:

Substitute Bytes Transformation

The initial stage of each iteration’s tarts with Sub Bytes transformation. This stage is depending on non-linear S-box to substitute a byte in the state to another byte. According to diffusion and confusion “Shannon’s Principles” cryptographic algorithm them with as chief important roles to acquire much more security.

Shift Row Transformation

Shift Row follows Sub Byte as the next operation on the state. The main goal of this step is to loop through each row and move the state's bytes to the ‘left’ instead of zero throw. The bytes from zero throw are still present in this process and no permutations are applied. Only one byte is relocated circularly to the ‘left’ in the first row. Two bytes are added to the ‘left’ to move the second row. Three bytes to the ‘left’ are added to the last row. The size of the new state is remaining at its original 16 bytes, even though the bytes in the stare have been moved.

Mix Columns Transformation

The state goes through Mix Column, which is another key stage. The division is done outside of the state. Multiplying each byte from one row by each byte from the state column in a matrix transformation. To put it another way, each state’s column and each row’s matrix transformation must multiply. The output of these multiplications is combined with the upcoming state which creates a new set of four bytes developed by an XOR. The size of the byte, which kept the initial 4*4size, was not altered in this step.

Add Round Key Transformation

The Add Round Key phase of the AES algorithm is crucial. A 4x4 byte matrix is used to structure both the key and the input data, which is also known as the state. When encrypting data, Add Round Key has the capacity to offer significantly more protection. Establishing a secure connection between the key and the ciphered text is the foundation of this procedure. The prior stage is when the encrypted text originates. The key that users specify influences the Add Round Key output precisely. Additionally, the stage makes use of the sub key in conjunction with the state. Rijndael's key schedule is applied to the main key to derive the subkey in each round. Sub key size and state size are same. By merging, the subkey is added.

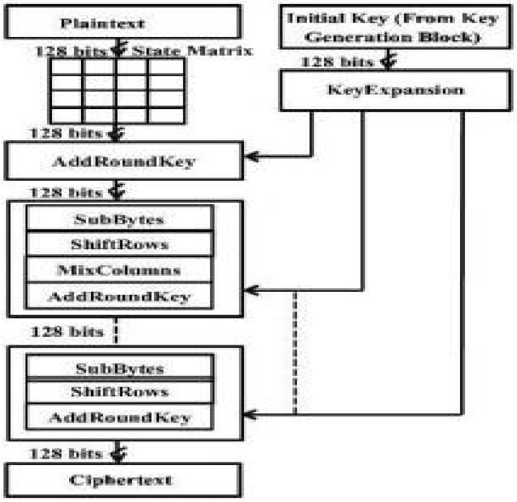


Fig 2. Structure

Decryption of AES Algorithm

The decryption procedure is similar to the encryption process in reverse order. Decryption is the procedure used to recover the encrypted data's original form. The key which was obtained from the data sharer is the one and only foundation of this procedure. In AES algorithm, both the sender and the receiver cipher and decipher the data using the same key. There are three steps in a decryption stage's final round: Inv Shift Rows, Inv Sub Bytes, and Add Round Key.

Applications of AES

AES Encryption and Decryption has many applications. It is used in cases where data is too sensitive that only the authorized people are supposed to access. The following are the various applications of AES: Secure Communication each state's column and each row's matrix transformation must multiply. The size of the byte, which kept the initial 4x4 size, was not altered in this step.

- RFID
- ATM Networks
- Government Documents
- FBI Files
- Image Encryption Secure Storage
- Personal Storage Devices

AdvancementsinAES128

The encryption algorithm used by both the AES-128and AES-256 are almost similar. This algorithm depends on rounds. A round consists of a set of operations which is iterated that many times. This is the only difference betweenAES-128andAES-256.

So, its self-explanatory that if an attack against AES-128 was disclosed or discovered both the AES-128 and AES-256 would be affected. Among AES-128 and AES-256 there exists a clear winner if an attack was successful in for at least ten rounds but less than fourteen. The reason we chose to use AES-128 that its faster as compared toAES-256 and also efficient and not that likely to have a full-on attack deployed against it, because of its stronger key schedule, and this is the exact reason we have also opted to use AES-128 over AES-256.

SHA-256(SecureHashAlgorithm-256)

A hash is a type of "signature" for a text or datafile. It is also sometimes referred to as a cryptographic hash or even as a "digest." Data files can include everything from basic account passwords to advanced cryptographic transactions.

History and Introduction to SHA-256

A family of cryptographic hash functions was released by The National Institute of Standards and Technology, including SHA 256, as a U.S. Federal Information Processing Standard (FIPS).

Other cryptographic hash functions come in a wide range of variations, includingSHA-2, SHA- 1, and SHA-0.

Since SHA-1 was created earlier than SHA-2, itis one of several successors, as is obvious from our observation. One of the successor functions to SHA-1 (grouped and known as SHA-2) isSHA-256, and it is unquestionably one of the most powerful ones accessible. It works well as an AES companion function because of the 256-bitkey.

Encryption and hashing have long been a part of the fundamentals of improved data security models, among the various crypto graphic developments found in network security. The most popular hash algorithm ever employed up to this point is the secure hash algorithm with a digest of 256 bits, or SHA 256. Although there are additional variations, SHA-256 has been at the fore front of applications in the real world.

Hashing

Hashing is essentially the technique of jumbling up raw or unprocessed data so that it cannot be understood by the average user without a secret key and also cannot be recreated back into its original form. It typically accepts a piece of unprocessed data or information and passes it through a function that applies a variety of different numerical and mathematical operations to the plain text. The result of this kind of source code, pseudocode, or function is referred to as the hash value or digest.

Primarily there are two applications of hashing

Password Hashes

The majority of website servers transform or hash user passwords into hash values before storing them on the server for improved security.

Integrity Verification

A hash is shared as the file's bundle when it is uploaded to the website. It needs to be refreshed and compared each time a user requests a download in order to ensure data integrity.

SHA-256

The NSA and NIST collaborated to develop SHA-256 as a successor to the SHA 1 family of encryption algorithms, which was gradually becoming less resistant to brute force attacks as the processing power of users' every day private computers increased quickly. SHA-256is a hierarchical component of the SHA2familyof encryption algorithms.

No matter how large the plaintext or cleartext is, the hash result will always be 256 bits. This is the significance and significance of the 256 in the name of the SHA-256 algorithm. The other SHA family algorithms are somewhat comparable to SHA-256.

Characteristics

The main distinguishing characteristics of SHA-256 make it stand apart from all of its forerunners and descendants. These qualities are:

Message Length

The cleartext or text that needs to be encrypted must have a string length of no more than 264 bits. To maintain the highest level of randomness in the digest, the size must fall within the bounds of the comparison area.

Digest Length

No matter how large the plaintext or cleartext is, the hash result will always be256bits.This is the significance and significance of the 256 in the name of the SHA-256 algorithm. The other SHA family algorithms are somewhat comparable to SHA-256.

Irreversible

The cleartext or text that needs to be encrypted must have a string length of no more than 264 bits. To maintain the highest level of randomness in the digest, the size must fall within the bounds of the comparison area.

Steps involved in the Password Encryption

The main distinguishing characteristics of SHA-256 make it stand apart from all of its forerunners and descendants. These qualities are:

Padding Bits

It (Fig 3) increases the message's size by a minuscule amount, leaving the string's total length exactly 64 bits short of being a multiple of 512 bits. The first bit should be one and the remaining ones filled with zeros when the extra bits are added to the message.

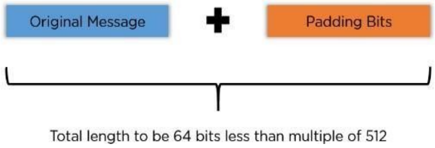


Fig 3. Padding Bits

Padding Length

The (Fig 4) final plaintext can be increased by 64 bits to be a multiple of 512. By using the modulus to the original cleartext without padding, these 64 bits can be computed.

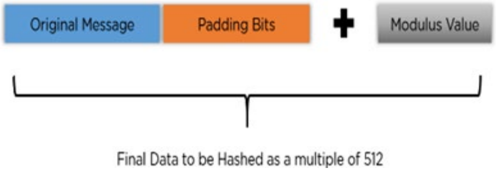


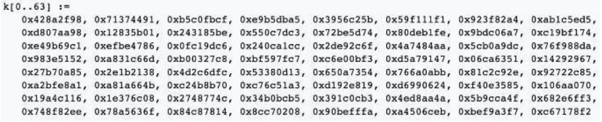
Fig 4. Padding Length

Initializing the Buffers

Default values for eight buffers need to be used in the rounds as follows:

a =
0x6a09e667b =
0xbb67ae85c =
0x3c6ef372d =
0xa54ff53ae =
0x510e527ff =
0x9b05688cg =
0x1f83d9abh = 0x5be
0cd19

One must also store 64 different keys in an array, ranging from K [0] to K [63]. They are initialized as follows in Fig.5:



```
k[0..63] :=
    0x428a2f98, 0x71374491, 0xb5c0fbcf, 0xe9b5dba5, 0x3956c25b, 0x59f111f1, 0x923f82a4, 0xab1c5ed5,
    0xd807aa98, 0x12835b01, 0x243185be, 0x550c7dc3, 0x72be5d74, 0x80deb1fe, 0x9bdc06a7, 0xc19bf174,
    0xe49b69c1, 0xefbe4786, 0x0fc19dc6, 0x240ca1cc, 0x2de92c6f, 0x4a7484aa, 0x5cb0a9dc, 0x76f988da,
    0x983e5152, 0xa831c66d, 0xb00327c8, 0xbf597fc7, 0xc6e00bf3, 0xd5a79147, 0x06ca6351, 0x14292967,
    0x27b70a85, 0x2e1b2138, 0x4d2c6dfc, 0x53380d13, 0x650a7354, 0x766a0abb, 0x81c2c92e, 0x92722c85,
    0xa2bfe8a1, 0xa81a664b, 0xc24b8b70, 0xc76c51a3, 0xd192e819, 0xd6990624, 0xf40e3585, 0x106aa070,
    0x19a4c116, 0x1e376c08, 0x2748774c, 0x34b0bcb5, 0x391c0cb3, 0x4ed8aa4a, 0x5b9cca4f, 0x682e6ff3,
    0x748f82ee, 0x78a5636f, 0x84c87814, 0x8cc70208, 0x90befffa, 0xa4506ceb, 0xbef9a3f7, 0xc67178f2
```

Fig 5. Initialized from K [0] to K [63]

Compression Functions

The whole message is divided into several blocks, each with512 bits. It performs 64 rounds of operations on each of those multiple 512-bit blocks, with the results from each round serving as the input for the following block. The following illustration shows how the SHA-256 compression algorithm works in its entirety (Fig 6):

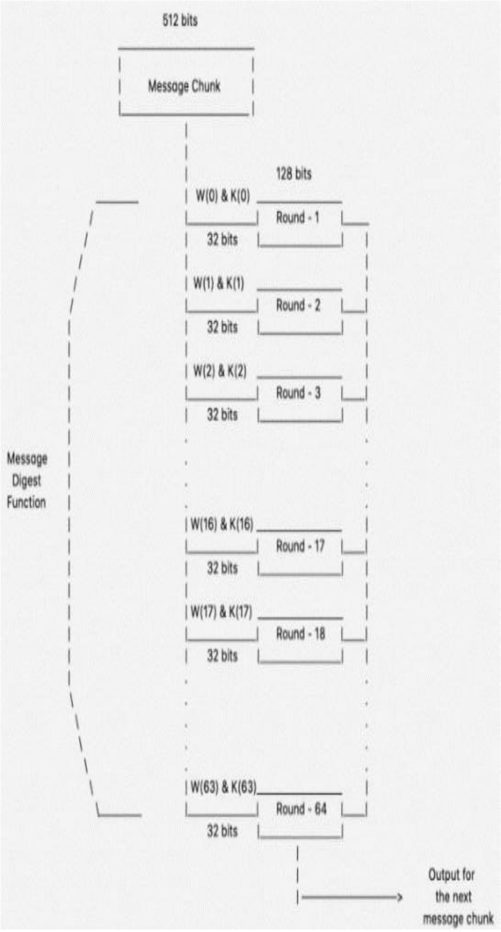


Fig 6. Functions.

Output

The block's final output is used as the input for the following block throughout each iteration. Up to the last 512-bit block, the entire cycle is repeated; at that point, the result is regarded as the final hash digest. Given the name of the algorithm, the digest will have a length of 256 bits.

Applications of SHA-256

- Digital Signature Verification
- Password Hashing
- SSLHandshake
- Integrity Check

LSFR (Linear Feedback Shift Register)

There are two fundamental methods in cryptography for encrypting data: symmetric encryption (also known as secret key encryption) and a symmetric encryption (also called public key encryption). Block cyphers and stream cyphers are the two groups of techniques that make up symmetric encryption. In a stream cypher, the key stream is mixed with plain text bits to create encrypted data.

Cipher text is the name given to the operation's output. Using the same key stream, it can be changed back into its previous state. A Linear Feedback Shift Register can be used to create a pseudo-random sequence (LFSR). For both software and hardware implementation, LFSRs are straightforward, quick, and simple. A feedback shift register comprises of two parts, a shift registers and a feedback function. A shift registers houses organized bits. Its size is expressed in bits; if it has n bits, it is referred to as an-bit shift register. Each time a bit is required, a right shift operation by one bit is performed on the shift register's bits. Then the new left most bit is calculated based on the other bits in the shift register. The tap sequence, as a list of selected bits in the register, is the standard feedback function. One bit, typically the least important bit, is the shift register's output. In stream cyphers, LFSRs are frequently a component of key stream generators. For the components of keystream generators, a set of criteria is taken into account. Period, linear complexity, and statistical metrics of the keystreams are some of these requirements.

The shift register length is measured in bits. If it is 'm' bits long, it is called 'm-bit shift register'. All of the bits in the shift register are shifted one-bit to the right every time a bit is needed. The new left-most bit is computed as a function of the other bits in the register. The feedback function is normally the XOR of selected bits in the register. the list of these bits is called a tap sequence. The output of the shift register is one bit, usually least significant bit. LFSRs are commonly used as part of key stream generators in stream ciphers. Certain criteria are considered for the parts of key stream generators. These criteria include linear complexity period keystreams.

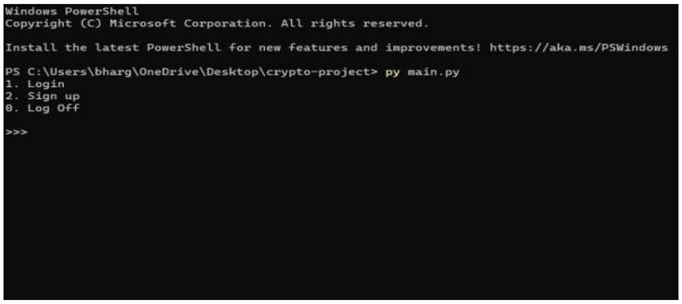
Period

The shift register's period can be described as the length of the output sequence even before it begins to repeat. The output sequence produced by this LFSR has a maximum period of 2n-1if the feedback polynomial of the n-bit LFSR is primitive and its initial state is at an on-zero state. The maximum-length sequence, or m-sequence, is what is known as this sequence. The m-sequences have very good randomization characteristics.

Linear complexity

A crucial parameter for assessing LFSR-based generators is linear complexity, also known as linear span. This is referred to as the shortest LFSR's length (n) that can mimic the generator output. Because a straight forward technique known as the 'Berlekamp-Massey' algorithm can produce an LFSR after examining only 2n bits of the keystream, linear complexity is crucial. The stream cipher is compromised after this LFSR has been produced. It's important to remember that a large linear complexity is not always a sign of a safe generator. Small linear complexity does, however, suggest an unreliable one.

III. RESULTS



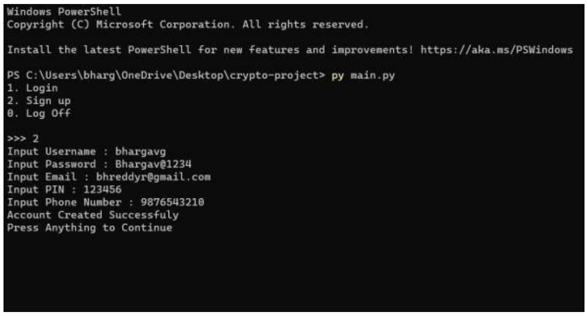
```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\bharg\OneDrive\Desktop\crypto-project> py main.py
1. Login
2. Sign up
0. Log Off

>>>
```

Fig 7. CLI to login, signup, and logoff



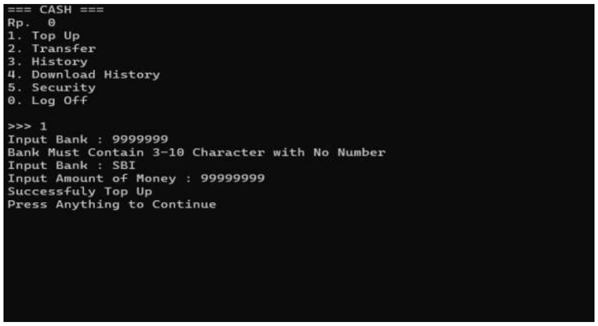
```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\bharg\OneDrive\Desktop\crypto-project> py main.py
1. Login
2. Sign up
0. Log Off

>>> 2
Input Username : bhargavg
Input Password : Bhargav@1234
Input Email : bhreddyr@gmail.com
Input PIN : 123456
Input Phone Number : 9876543210
Account Created Successfuly
Press Anything to Continue
```

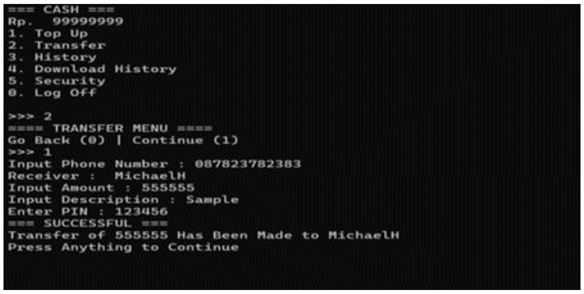
Fig 8. Any new user can create and account by providing username, password, email, phone number.



```
=== CASH ===
Rp.  0
1. Top Up
2. Transfer
3. History
4. Download History
5. Security
0. Log Off

>>> 1
Input Bank : 9999999
Bank Must Contain 3-10 Character with No Number
Input Bank : SBI
Input Amount of Money : 99999999
Successfuly Top Up
Press Anything to Continue
```

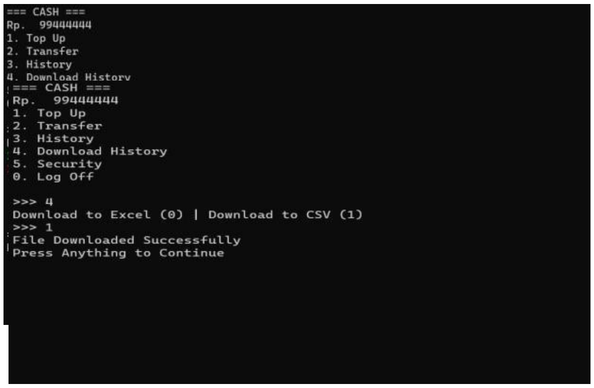
Fig 9. On successful login, the user enters into the dashboard which contains options such as TopUp, Transfer, History, Download History, Security and Logoff.



```
=== CASH ===
Rp.  99999999
1. Top Up
2. Transfer
3. History
4. Download History
5. Security
0. Log Off

>>> 2
==== TRANSFER MENU ====
Go Back (0) | Continue (1)
>>> 1
Input Phone Number : 087823782383
Receiver :  MichaelH
Input Amount : 555555
Input Description : Sample
Enter PIN : 123456
=== SUCCESSFUL ===
Transfer of 555555 Has Been Made to MichaelH
Press Anything to Continue
```

Fig 10. Money Transfer from one account can be done by choosing the option "Transfer" and providing the required details.



```
=== CASH ===
Rp.  99444444
1. Top Up
2. Transfer
3. History
4. Download History
=== CASH ===
Rp.  99444444
1. Top Up
2. Transfer
3. History
4. Download History
5. Security
0. Log Off

>>> 4
Download to Excel (0) | Download to CSV (1)
>>> 1
File Downloaded Successfully
Press Anything to Continue
```

Fig 11. The transfer history can be available in the "History Section" which projects the time, date, sender, receiver, and account details.

IV. CONCLUSION

Internet and network usage are growing quickly. A significant amount of digital data is exchanged daily between users. Certain data must be protected from intrusion because it is sensitive. To prevent unwanted access to original data, encryption technologies are essential. There are numerous types of algorithms available to encrypt data.

One of the most effective algorithms is the Advanced Encryption Standard (AES) algorithm, which is extensively used in hardware and software. With a 128- bit block cypher, this technique can handle keys with varied sizes, such as 128, 192, and 256 bits. In order to assess the effectiveness of the AES algorithm to encrypt data under various conditions, a number of key elements of the AES algorithm are explained in this study. Research findings (Fig 7, 8,9,10, 11,12) indicate that AES has a considerably greater capacity to offer security when in comparison with other algorithms like DES, 3DES, etc.

The secured hash algorithm, also known as SHA, strives to offer an additional layer of protection to the vast and growing amount of data you must manage. All of the more modern hashing schemes will eventually have a flaw that hackers and attackers can exploit. There are three factors on which the security of SHA-256 is based, firstly, the problem is obtaining the initial data from the hash value is intrinsically impossible. To generate the original data, a brute-force attack would need to be conducted 2256 times.

Secondly, it is immensely implausible that two messages will have the same hash value. The possibility of two hash values matching is extremely small and is unimaginably remote. Lastly, a peripheral change to the initial data changes the hash value so significantly that it is not immediately clear that the new hash value is derived from the same the avalanche effect refers to this phenomenon in data.

One of the most secure hashing algorithms available is SHA-256. The government mandates that SHA-256 be used to secure specific sensitive data by its agencies. Finally, a minor alteration to the source data leads the hash value to vary so enormously that it is difficult to determine from indistinguishable data; this is known as the “Avalanche Effect”.

References

[1] A Handbook of Applied Cryptography by Alfred J.Menezes, Paul C. Van Oorschot and Scott A. Vanstone,CRC Press Series on Discrete Mathematics and ItsApplications.

[2] Foundations of Cryptography (Basic Tools) OdedGoldreichCambridge2001

[3] F. Al-Shaikhli, M.A.AlahmadandK.Munthir,"HashFunction of Finalist SHA-3: Analysis Study,"InformationTechnology (IJACSIT), Vol. 2, 2013,StallingsW(2006).

[4] Cryptography & Network Security: Principles &Practices, Pearson EducationIndia.

[5] Singh, G. (2013). A study of encryption algorithms (RSA, DES, 3DES and AES) for information security.InternationalJournalofComputerApplications.

[6] SHA-1hashfunctionunderpressure–HeiseSecurity.

[7] ClassificationandGenerationofDisturbanceVectorsforCollisionAttacksagainstSHA-1.

[8] Cryptography:A NewDimensionin ComputerDataSecurity;AGuidefortheDesignand ImplementationofSecure Systems, by Carl H. Meyer and Stephen M.Matyas.

[9] Codesand Cryptography,by Dominic Welsh.Oxford,England:ClarendonPress,1988.257

[10] SpecificationfortheAdvancedEncryptionStandard(AES), Federal Information Processing StandardsPublication197,Nov.2001