WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Quantum Encryption A Boon or Bane on Environment

Neelanjan Manna

Metapyxl

ABSTRACT

The process of converting information into a secret code that conceals its true meaning is known as encryption. Cryptography is the study of information encryption and decryption. In the world of computers, ciphertext refers to encrypted data and plaintext to unencrypted data.

Introduction

Steganography is the art of hiding a message inside of another message or a tangible thing. In electronic and computing contexts, a computer file, message, image, or video is hidden within another file, message, image, or video. Steganography is a combination of the Greek words steganós (v), which means "covered or veiled," and -graphia (v), which means "writing."

The phrase was first used by Johannes Trithemius in his Steganographia, a treatise on steganography and cryptography that was published as a book on magic in 1499. Typically, the concealed messages are disguised as (or integrated into) something else, such as photographs, articles, shopping lists, or other cover text. A private letter, for instance, might have the concealed message written in invisible ink between the lines that can be seen.

Advanced Encryption Standard (AES)

The U.S. National Institute of Standards and Technology's (NIST) Advanced Encryption Standard (AES) is a specification for the encryption of electronic data that was created in 2001. Even though it is more difficult to develop, AES is commonly used because it is significantly stronger than DES and triple DES.

Remember these things

- Block cypher AES is used.
- The key can have a size of 128/192/256 bits.
- chunks of data with a 128 bit encryption are used.
- This indicates that it receives 128 bits as input and generates 128 bits of encrypted cypher text as output. According to the substitution-permutation network theory, which AES relies on, the input data is replaced and shuffled through a series of connected operations.

According to the key length, the number of rounds will vary as follows:

- 10 rounds with a 128-bit key
- 12 cycles for a 192-bit key
- 14 cycles for a 256-bit key
- Developing round keys

All the round keys from the key are calculated using a Key Schedule algorithm. Therefore, several different round keys that will be used in the corresponding round of the encryption are created using the original key.

AES uses a grid of 16 bytes per block in a column major configuration for encryption.

B0 | B4 | B8 | B12 | B1 | B5 | B9 | B13 | B2 | B6 | B10| B14 | B3 | B7 | B11| B15
Four steps are included in each round:

- SubBytes\sShiftRows
- Add Round Key using MixColumns
- The MixColumns round does not appear in the final round.

The substitution and permutation operations of the method are carried out by SubBytes, ShiftRows, and MixColumns, respectively.

SubBytes: This action carries out the substitution.

In this stage, one byte is replaced with another. It is carried out utilising a lookup table also known as the S-box. This substitution is carried out in such a way that no single byte is ever replaced both independently and by another byte that complements the current byte.

The permutation is applied in the next two steps.

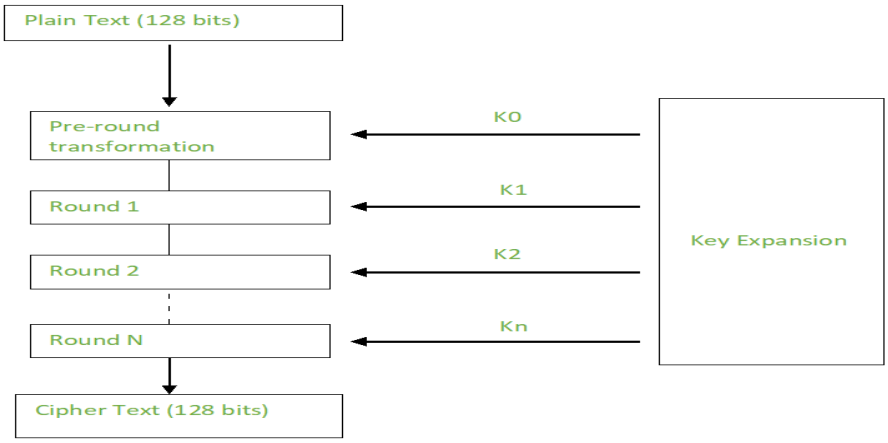
ShiftRows: This action is exactly what it says. The number of shifts for each row varies.

There is no shift in the first row.

- One shift to the left moves the second row.
- Two times to the left, the third row is moved.
- Three times to the left, the fourth row is moved.
- (There is a left circular shift.)

[b0 | b1 | b2 | b3] [b0 | b1 | b2 | b3] | b4 | b5 | b6 | b7 | -> | b8 | b9 | b10 | b11 | | b10 | b11 | b8 | b9 | [b12 | b13 | b14 | b15] [b15 | b12 | b13 | b14]
MixColumns: This step essentially involves multiplying matrices. Each column is multiplied by a particular matrix, changing the order of each byte in the column as

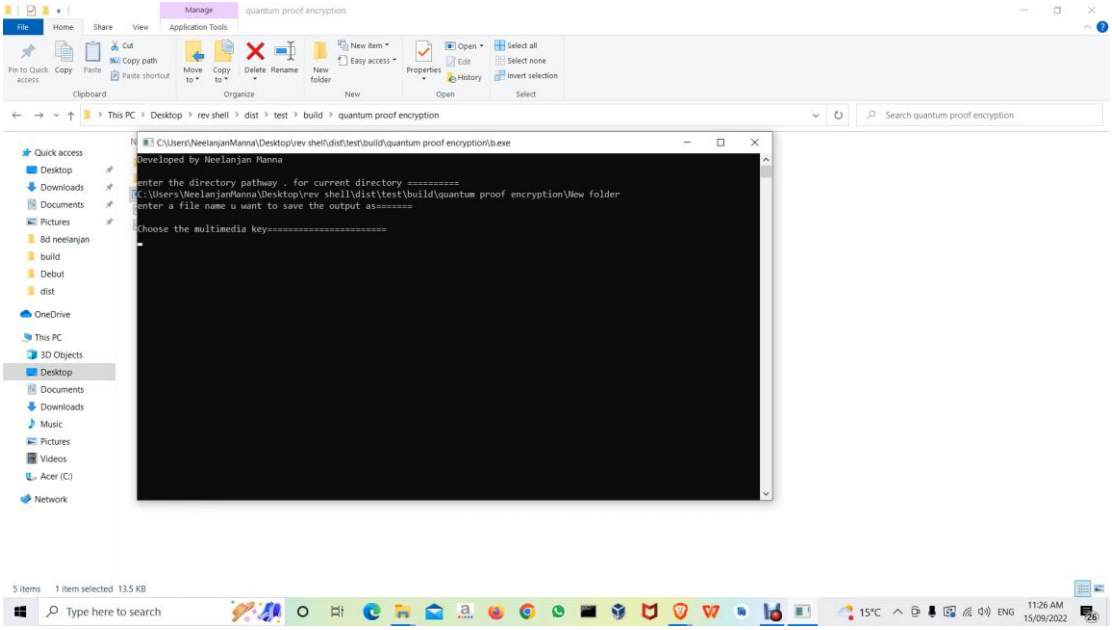
128 bits of encrypted data are returned as output after each cycle. This procedure is continued until all of the data that needs to be encrypted has gone through it.



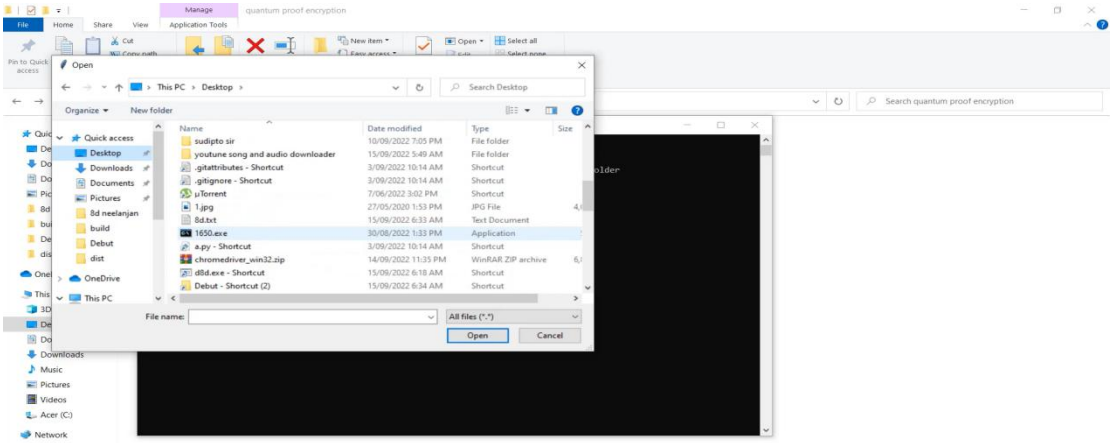
Methodology of encrypting a multimedia file with another multimedia file

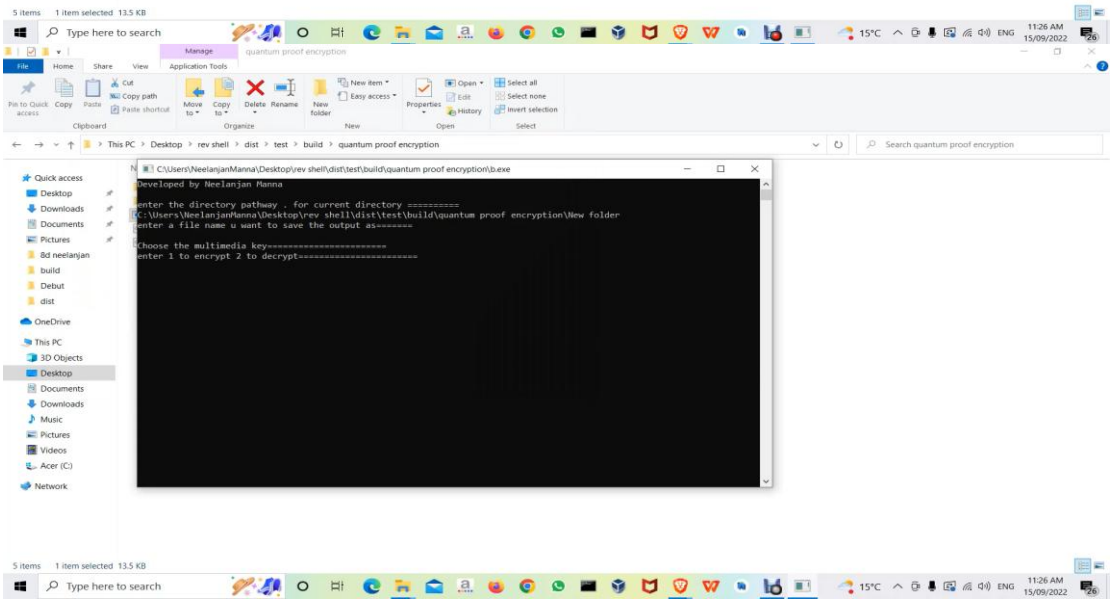
The author has created a novel method for transforming a key file as large as one gigabyte into a sha 512 hash of same capacity and size. After then, this file is used to encrypt any other multimedia files that may be found in the digital realm, such as music, documents, etc.

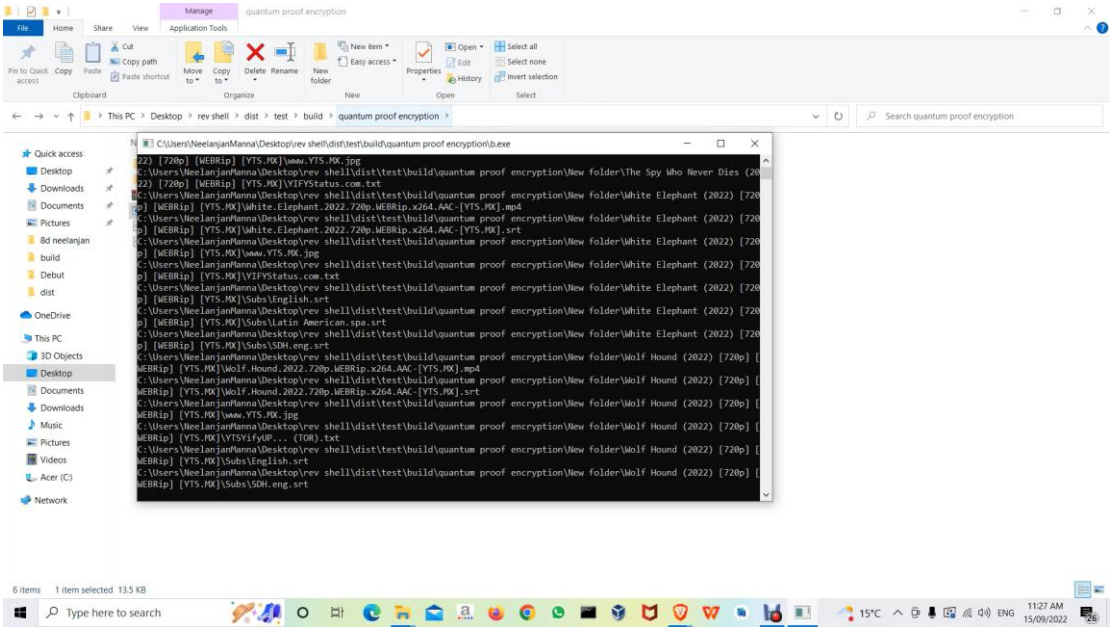
Modus operandi or method of operation

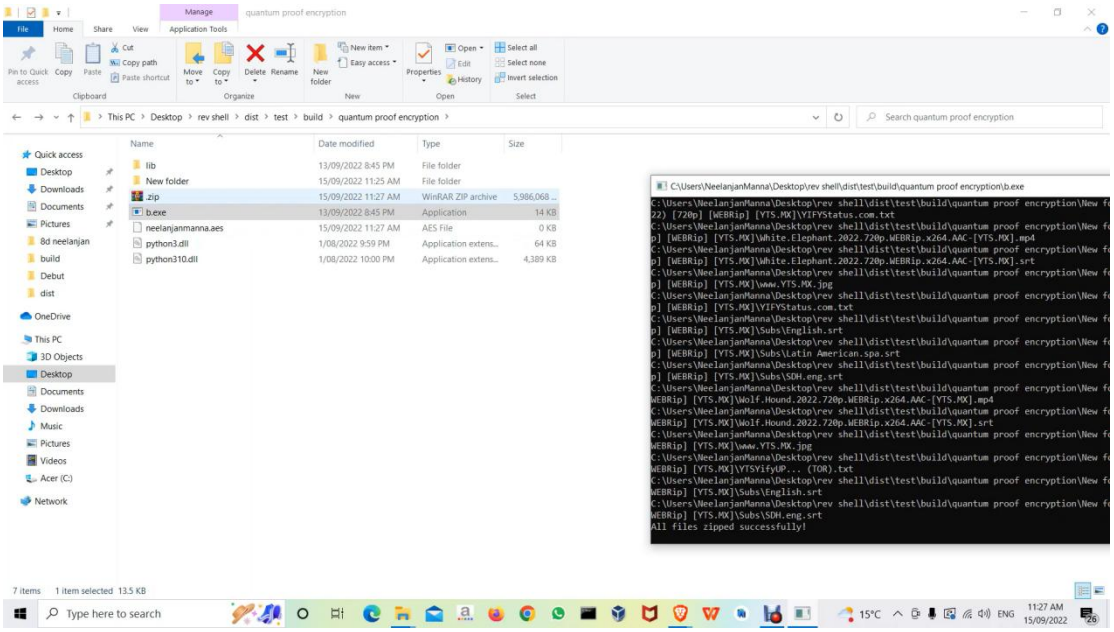


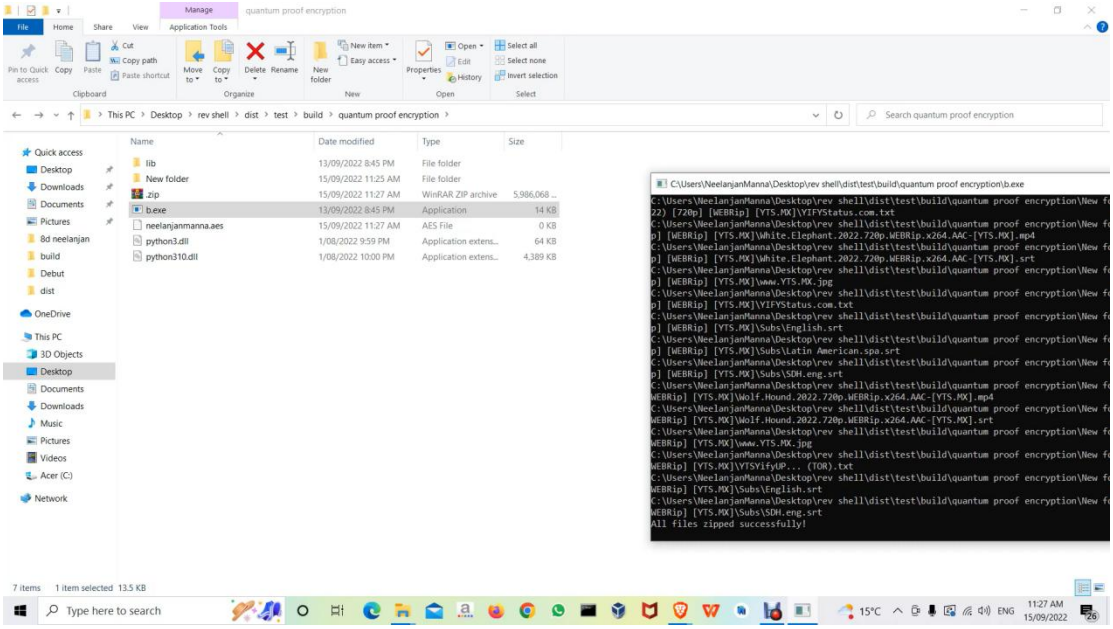
Choose the multimedia file as key to be used as the encryption secret

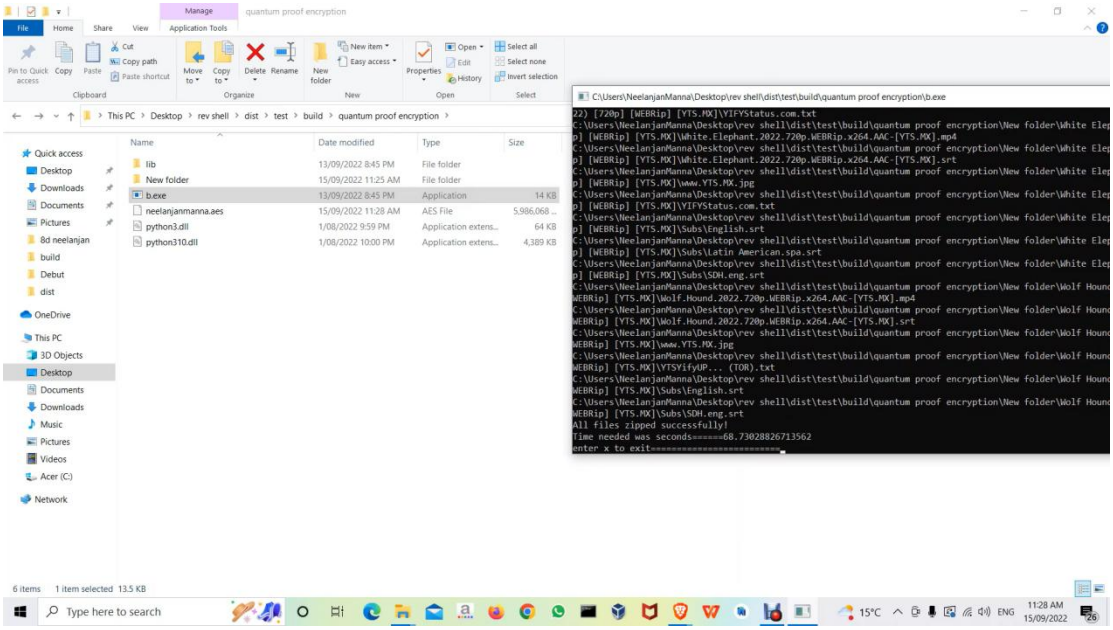












Synopsis : A folder of over 5 gigabytes is encrypted with a 1 megabyte application file based on the world famous Nist standard Advanced Encryption standard cipher . The encryption is completed in 66 seconds approximately and decryption in 36 seconds approximately

Conclusion

Post-quantum cryptography is a term used in the field of cryptography to describe cryptographic algorithms (typically public-key algorithms) that are thought to be secure against a cryptanalytic attack by a quantum computer. It is also referred to as quantum-proof, quantum-safe, or quantum-resistant. The issue with existing common algorithms is that their security depends on one of three challenging mathematical problems: the discrete logarithm problem, the discrete logarithm problem with elliptic curves, or the integer factorization problem. On a quantum computer running Shor's algorithm and with appropriate power, all of these issues may be readily resolved. It can be aptly said that a modified way generating the key for the aes cipher is sufficient to secure your data than relying more on carbon footprint intensive encryption solutions.