A NOVEL APPROACH TO SECURE AUDIO TRANSMISSION USING STEGANOGRAPHY AND QUANTUM KEY DISTRIBUTION PROTOCOL.

RESEARCH ARTICLE

Md. Mizanur Rahman[1], Md. Raisul Islam Rifat[2], Md. Abdul Kader Nayon[2], and M.R.C. Mahdy[3, *]

[1]Department of CSE, RUET
[2]Department of EEE, CUET
[3]Department of Electrical and Computer Engineering, North South University, Bashundhara, Dhaka

ABSTRACT

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

Keywords Lorem ipsum, Placeholder text, Text generation, Typography, LaTeX formatting, Document design, Content management, Semantic analysis, Latin text, Formatting templates, Filler content, Automated writing, Document structure

1 Introduction

The most simplest, as well as the most important, form of exchange for human beings is verbal communications. The invention of the Telephone by Alexander Graham Bell in 1876 transformed the verbal communication demography - making the transmission of human voice, which are essentially audio signals, over long distances possible. In the subsequent centuries, technological improvements has broadened the scope of audio transmission. With the rise of the Internet, the amount of information exchanged through audio signals increased rapidly. This increase number audio transmission resulted in the development of different encryption techniques and cryptographic algorithms. The most popular among these algorithms are the symmetric AES and the asymmetric RSA encryption schemes. AES [1] is a block cipher scheme that utilizes multiple matrix operation to encrypt and decrypt data using the same key. Without any knowledge of the cipher key, it is computationally infeasible to reverse the orations performed during encryption. RSA [2], on the other hand, utilizes prime number factorization to generate public-private key-pairs for each user that are used to encrypt and decrypt data. The security of the RSA scheme relies on the insane amount of computational power required to obtain the private key from a public through prime number factoring.

However, with the advent of Quantum Computers with increasing number of functional qubits, these classical cryptography and encryption schemes face an imposing threat [3]. In 1996, Lov K. Grover proposed an algorithm to search an unordered database of size N using $\sqrt{N}$ quantum queries [4]. Using Grover's algorithm, the number of trials required to brute-force a key of length k reduces from 2^k to $2^{k/2}$. This reduction in number of brute-force

* Corresponding author. *E-mail address*: mahdy.chowdhury@northsouth.edu (M.R.C. Mahdy).

trials effectively reduces the security level of symmetric encryption schemes such as AES [5]. For example, the AES-128 encryption scheme with a pre-quantum security level of 128 reduces to a post-quantum security level of 64, which is much easier to brute-force. In 1994, P.W. Shor presented a quantum algorithm that can quickly find the prime factorization of any positive integer N [6]. As the security of the RSA algorithm relies on the arduousness of prime number factorization to derive private key from public key, it is currently facing an existential threat due to the exponential speed of Shor's algorithm. It is estimated that the time complexity for Shor' algorithm is $\mathcal{O}(72(log(N))^3)$, as opposed to $\mathcal{O}(N^3)$ for classical computers.

To address these arising challenges, new research is being done on the field of quantum augmented communication systems. These systems exploits the principles of quantum mechanics to attain secure data transmission. One of the most promising area of research in the field of quantum communications is Quantum Key Distribution (QKD). QKD protocols works by establishing a secure cryptographic key between two users over an insecure channel [7]. QKD employ properties unique to quantum mechanics, such as the no-cloning theorem [8] and the uncertainty principle [9], that ensures the detection of any eavesdropping attempts and thereby guarantees the security of the key. However, QKD itself does not provide security on its own, rather it facilitates the establishment and secure exchange of secret keys that are subsequently used by other cryptographic algorithms and encryption techniques to secure the transmitted information.

2 Related Works

3 Methodology

4 Experiments and Results

5 Findings and Discussion

6 Conclusion and Future Work

References

[1] V. Rijmen and J. Daemen, "Advanced encryption standard," *Proceedings of federal information processing standards publications, national institute of standards and technology*, vol. 19, p. 22, 2001.

[2] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[3] D. J. Bernstein and T. Lange, "Post-quantum cryptography," *Nature*, vol. 549, no. 7671, pp. 188–194, 2017.

[4] L. K. Grover, "A fast quantum mechanical algorithm for database search," in *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, pp. 212–219, 1996.

[5] J. Daemen and V. Rijmen, *The Design of Rijndael*. Springer Berlin Heidelberg, 2002.

[6] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Journal on Computing*, vol. 26, p. 14841509, Oct. 1997.

[7] R. Alléaume, C. Branciard, J. Bouda, T. Debuisschert, M. Dianati, N. Gisin, M. Godfrey, P. Grangier, T. Länger, N. Lütkenhaus, *et al.*, "Using quantum key distribution for cryptographic purposes: a survey," *Theoretical Computer Science*, vol. 560, pp. 62–81, 2014.

[8] V. Bužek and M. Hillery, "Quantum copying: Beyond the no-cloning theorem," *Physical Review A*, vol. 54, no. 3, p. 1844, 1996.

[9] D. Sen, "The uncertainty relations in quantum mechanics," *Current Science*, pp. 203–218, 2014.