

General Conclusion

Over the past 2,500 years, cryptography has developed numerous types of systems to hide messages and subsequently a rich vocabulary in which to describe them. The focus of this work was stationed in the field of Symmetric Key Encryption. The improved AES algorithm that use 512 bit of key and data block provides high level of security, because of the use of a key size larger than the original 128-bit AES key. However, it has a deficiency in performance, the encryption process become heavy when it comes to the modern communicating world that depends on the resource-limited systems and real-time operations.

The main objective of this work was designing an alternative algorithm that keeps the level of security that the 512-bit AES provides, and minimizes the cost of memory space used and encryption time that it takes.

We started our work with a general introduction that speak about security of the transmission over the internet in general.

The first chapter talks about the technical and applicative aspects of cryptology with its two branches: cryptography and cryptanalysis.

In the second chapter, we talk about Mathematical preliminaries required in encryption and decryption methods, and a detailed study of a new variation of the original 128-bit AES algorithm called 512 bit AES that was appeared to provide more security.

The third chapter explain in detail the proposed algorithm that is given as an alternative to the one that called "512-bit AES" for improving the performance level, explaining its transformations methods including the general architecture and key expansion.

The fourth chapter talks about the environment of the implementation that we have done to make the comparison between algorithms, and the tests that we have done including the results that prove the amelioration of the performance level.

The experimental results on several data (text, image, sound, video) show that the used memory space is reduced to quarter, and the encryption time is reduced almost to the half. Therefore, the adopted method is very effective for encryption of multimedia data.