Abstract

In recent years, the Internet and social media have provided many services to humans in a variety of areas, including information transmission, instant messaging, banking, video conferencing, etc. This makes information security an issue that requires high-security solutions to keep hackers away from these connections. Cryptography provides a secure method for transmitting information through insecure communication channels, converting plain text into ciphertext so that the ciphertext cannot be decrypted without knowledge of the corresponding key. Encryption algorithms are often integrated with other applications, some of these applications require faster execution time and others require high data security without paying attention to time and some require a limited execution environment, and this requires building a variety of encryption algorithms that meet this security need, and commensurate with these restrictions.

Cryptography schemes based on mathematical transformations are one of the types of symmetric cipher schemes that are encrypted in the form of blocks. These schemes depend on mathematical transformations in the encryption process and its inverse in the decryption process. The first cipher scheme of these schemes uses the Laplace transform, where the encryption process is as follows: the plaintext is encoded into decimal numbers, and these numbers are multiplied by the coefficients of the Taylor polynomial, then the Laplace transform is applied to the resulting polynomial, after that the resulting values are divided by a value (block length), where the remainder represents the encrypted value and the quotient represents the decryption key. This scheme has been proven to be insecure by Gupta and Mishra. Thereafter, several schemes based on other mathematical transformations were published in a manner similar to the previous one with some differences.

This thesis presented cryptanalysis of different types of these schemes and demonstrated that these schemes can be broken using different cryptographic attacks and identified weaknesses in these schemes. This thesis also presented a proposal to improve these schemes so that they have high-security against various cryptographic attacks. The improvement process is to hide the direct mathematical relationship between the plain text and the ciphertext, and it is done by adding an innovative substitution and permutation network in order to generate bit strings with enough randomness to create confusion and diffusion. In the innovative compensation process, the substitution box(S-box) consists of different values whose range depends on the range of values generated by the mathematical transformation, and these values are arranged in a random and secret manner. The resultant value of the substitution is located in the column and row whose number is equal to the remainder and quotient values respectively, resulting from previous schemes and that represented the ciphertext and the secret key. The innovative permutations process depends on the permutations group whose length depends on the length of the block, and its elements are arranged secretly and are also used as a secret key added to the ciphertext. The resulting encrypted values are returned as input to the next cycle, where the encryption process takes place in several cycles.

The improved algorithm was tested by several tests, including: statistical analyzes, such as Shannon entropy analysis, correlation analysis, etc., differential analyzes such

as NPCR and UACI analysis, randomization test (NIST), and execution speed. The results of security analyzes and randomness testing indicate that the proposed system provides a higher level of security against various cryptographic attacks, and the performance and execution time analysis shows that the improved algorithm offers high performance and improved security with low computational complexity.