Literature Survey of Recent Papers on Cryptography in Cyber Security

Cryptanalysis of the Simple Substitution Cipher with Word Divisions

Task: The paper aimed to analyze the vulnerability of the simple substitution cipher, specifically when word divisions were added, to cryptanalysis.

Approach: The authors conducted a thorough cryptanalysis of the modified simple substitution cipher, utilizing word divisions, and demonstrated that it was susceptible to frequency analysis, pattern recognition, and dictionary attacks. Their approach involved assessing the impact of word divisions on the cipher's security.

Observation: The paper observed that the addition of word divisions to the simple substitution cipher did not significantly enhance its security. The authors found that frequency analysis and pattern recognition techniques were still effective in breaking the cipher, emphasizing its vulnerability.

Improvement: To improve the security of this cipher, the authors suggested incorporating multiple substitution alphabets, thereby increasing the complexity of the encryption process. This enhancement would make cryptanalysis techniques like frequency analysis and pattern recognition less effective, providing stronger data protection.

Cryptanalysis of the Hill Cipher Using Genetic Algorithms

Task: The paper aimed to analyze the security of the Hill cipher against cryptanalysis techniques, specifically using genetic algorithms for key recovery.

Approach: The authors employed genetic algorithms to perform a cryptanalysis of the Hill cipher. They focused on key recovery, emphasizing the application of genetic algorithms to search for the cipher's encryption key efficiently.

Observation: The paper observed that the Hill cipher was susceptible to key recovery attacks using genetic algorithms. The authors demonstrated that, with the right approach, the key could be successfully retrieved, highlighting the need for stronger key management in the Hill cipher.

Improvement: To enhance the security of the Hill cipher, the paper suggested implementing additional key management techniques, such as key diversification, and considering larger key sizes. These improvements would make key recovery attacks using genetic algorithms significantly more challenging.

A Survey of Modern Encryption Techniques in Network Communication

Task: The paper aimed to provide an overview of modern encryption techniques employed in network communication.

Approach: The authors conducted a survey that encompassed various modern encryption techniques used in network communication. They reviewed the strengths and weaknesses of techniques such as symmetric and asymmetric encryption, blockchain-based encryption, and quantum cryptography.

Observation: The paper observed that modern encryption techniques have evolved significantly, with an emphasis on stronger key management, adaptability to emerging technologies, and resistance to quantum attacks. Asymmetric encryption and quantum cryptography were noted for their potential to provide robust security.

Improvement: The paper highlighted the importance of continuously improving encryption techniques to meet the challenges of evolving threats. It recommended integrating quantum-resistant algorithms and enhancing key distribution mechanisms to ensure long-term security in network communication.

Modification of Playfair Algorithm using Genetic Algorithm

Task: This paper aimed to enhance the Playfair Algorithm's security and overcome its limitations by applying genetic algorithms.

Approach: The authors introduced a dual encryption method for the Playfair Algorithm and employed genetic algorithms for key modification. They presented a modified 9x9 matrix to accommodate lowercase, uppercase, numbers, and special symbols, addressing Playfair's limitations.

Observation: The paper observed that the Playfair Algorithm, though historically strong, had limitations such as susceptibility to brute force attacks and the exclusion of lowercase letters, numerals, and special symbols.

Improvement: To improve the Playfair Algorithm's security, the paper suggested applying genetic algorithms for key modification and using a larger matrix. The dual encryption approach and the inclusion of additional characters strengthened the algorithm's resistance to attacks.

Enhancing Playfair Cipher using Seed Based Color Substitution

Task: This paper aimed to improve the Playfair Cipher's security by introducing color substitution based on hexadecimal colors and integrating the middle square method.

Approach: The authors presented a modified Playfair Cipher that used color substitution, providing nearly 18 decillion colors. They integrated the middle square method for generating random numbers, making it challenging for cryptanalysis techniques to decipher the information.

Observation: The paper observed that the integration of color substitution and the middle square method significantly enhanced the Playfair Cipher's security, making it resistant to cryptanalytic and brute force attacks.

Improvement: To further improve the Playfair Cipher's security, the paper suggested exploring pixelated or color spectrum representations and standardizing cipher size to enhance encryption strength. This approach would offer both security and aesthetic benefits in data protection.

In summary, these papers address various cryptographic techniques and their vulnerabilities, offering insights and recommendations for improving data security through encryption.