Journal of Data Acquisition and Processing
ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.777631

A SURVEY ON SECURING DATA IN CRYPTOGRAPHY

Dr. Rupesh Sendre

(Dept. of International Institute of Professional Studies, Devi Ahilya University, Indore, M.P., India)

Abstract:
The Internet and mobile revolution have had a profound impact on human life, bringing about significant transformations. These technological advancements have provided individuals with a wide range of devices for swift information exchange, catering to various needs. One crucial aspect of any information system is the assurance of secure information exchange from its source to its destination, accomplished through the implementation of cryptography. Cryptanalysis, as a vital process, assesses the strength and vulnerabilities of these systems, while also conducting security audits. Whenever a novel cryptographic method emerges, comprehensive analysis becomes indispensable, encompassing perspectives from hackers, cryptanalysts, and users, alongside performance evaluations. With a focus on computational methods for cryptanalysis, researchers continue to develop new techniques and algorithms. This paper presents an extensive survey of these advancements, comparing them to state-of-the-art approaches and discussing future prospects and directions in the realm of cryptic mining.

Keywords: *Cryptography, Cryptanalysis, Hacker, AI-Genetic Algorithm, Swarm Intelligence cipher, Neural Network.*

1. Introduction:

The continuous evolution and rapid progress in the field of cryptography have paved the way for learning-based cryptic algorithms in hybrid mobile applications, aimed at preventing various smart cryptographic attacks. As the race between attackers and security experts intensifies, the advanced study of cryptanalysis based on learning techniques plays a crucial role in enhancing cryptosystems and fortifying prevention mechanisms against such attacks. Over the past few decades, significant work has been undertaken in this domain, with disciplines like machine learning, artificial neural networks (ANN), genetic algorithms, and others contributing to the design of effective and efficient cryptosystems. This paper conducts a comprehensive survey, focusing on the following criteria:

1. Applied Techniques: ANN, KNN, SVM, Decision Tree, GA, And Fuzzy Logic.
2. Used Algorithms: AES, DES, Blowfish, and the Vigenere cipher.
3. Nature of Key: Symmetric Key (Private Key), Asymmetric Key (Public Key).
4. Mathematical Operations: Interpolation (Polynomial, Fuzzy), Mean Square Error Method, Tree Parity Machine, Key-based Multiple Huffman Tables.

By analyzing these criteria and utilizing associated research tools, valuable insights are gained and presented in the subsequent sections of this paper.

2. Work done on Cryptography:

The following section provides a brief overview of the literature reviewed by various authors. Bagnall, A. J. et al., (1997) [1] has described method of deciphering messages encrypted with

rotor machine using genetic algorithm. It searches the keyspace in encrypted text. This method didn't work with a two rotor problem in times comparable to those obtained using the iterative technique. In Diffie, W. & Hellman, M. E., (1979) [16] have presented a tutorial introduction to contemporary cryptography. The authors provided a comprehensive overview of classical and modern cryptographic systems, discussing their fundamental aspects, theoretical properties, and computational characteristics. Additionally, they conducted a thorough cryptanalytic analysis of significant systems and explored the practical application of cryptography in safeguarding timesharing systems and computer networks. Their work also includes a valuable reference to the extensive cryptographic literature. Winterhof, A., (2001) [17] has extended the most of the results on the interpolation of the discrete logarithm in the finite prime field F_p by polynomials modulo p and modulo $p-1$ given by Coppersmith and Shparlinski to arbitrary $F_{pr.}$ Dileep. A. D. & Sekhar, C. C., (2006) [18] have used support vector machine approach for identification of encryption for block ciphers. They considered this task as document categorization task and for this purpose they have used common dictionary based method and the class specific dictionary based method.

According to Thomas, B., (2008) [19] block ciphers probably figure in the list of the most important cryptographic primitives. Although they are used for many different purposes, their essential goal is to ensure confidentiality. This thesis focuses on the quantitative security aspects of cryptographic systems, specifically emphasizing measurable attributes that determine their effectiveness in ensuring confidentiality. The authors extensively discuss distinguishing attacks and key-recovery attacks targeting block ciphers, while also presenting strategies to transform the former into the latter. Klein, E. et al., (2004) [2] the novel phenomenon "Two neural networks that are trained on their mutual output synchronize to an identical time dependant weight vector" can be used for creation of a secure cryptographic secret-key using a public channel. They have proposed several models for this cryptographic system, and tested for their security under different sophisticated attack strategies. In Laskari, E. C., (2007) [3] proposes the short survey on applications of computational intelligence to cryptographic problems and stated that computational intelligence methods can constitute a first measure of the cryptosystems security. The performance of artificial neural network in solving cryptographic problems depends on the problem formulation and data representations. In a study conducted by Alallayah, K. in 2010 [20], the issue of cryptanalysis was characterized as an unknown entity, and it was suggested that neural networks serve as effective tools for identifying black box systems. To address this, the researchers developed a mathematical black-box model and integrated system identification techniques with adaptive system methods to create the Neuro-Identifier. The authors opted to utilize the LM algorithm of neural networks to train the NID, as it demonstrated favorable approximation capabilities, faster convergence, a more stable performance surface, and the ability to achieve precise accuracy by adjusting the degrees of freedom in the hidden layer. Sharaf, M. S., (2009) [6] proposed the theory of quantum cryptography can contribute to the network security and inviolability of the laws of quantum mechanics will be the base for security of network communications. He summarized the current state of quantum cryptography, and the real-world application implementation of this technology. In Francisco, L. & Iglesias, S. (2012) [5] have suggested general probabilistic attacks for neural cryptography. These make use of mathematical tools usually from the field of statistical mechanics to calculate some underlying probability distributions like the secret

keys generated by the cryptographic protocol take this or that shape. Alallayah, K., (2012) [4] have developed a mathematical black-box model and have combined system identification techniques with adaptive system techniques to construct the neuro-identifier. It is constructed of target cipher system to determine the key from given plaintext-ciphertext pair.

According to Nuhn, M. & Knight, K., (2014) [21] automation of decryption of various types of ciphers makes it possible to sift through the large number of encrypted messages found in libraries and archives, and to focus human effort only on a small but potentially interesting subset of them. It will reduce human effort as well as error in decryption. A classifier can be trained to predict which encipherment method has been used to generate a given ciphertext. In Jogdand, R. M. & Bisalpur, S. S., (2011) [7] suggest that neural network can be used to generate common secret key. Neural cryptography involves a scenario where two communicating networks are provided with the same input vector, and subsequently generate an output bit. The training process of these networks is then based on the outcome of the generated output bit. The generated secret key over a public channel is used for encryption and decryption of information. Mishra, S. & Bhattacharya, A., (2013) [13] stated as cryptanalysis can be performed by applying combined approach. This combined approach uses various algorithms simultaneously to transform uses various algorithms simultaneously to transform cipher-text into information. This algorithms can be block length/stream detection, entropy/recurrence analysis, dictionary and decision tree based approach etc.

3. Cryptography at a Glance:

By analyzing Cryptography is the field dedicated to the practice and study of concealing information, aiming to ensure its secrecy and safety. It combines elements of mathematics, computer science, and electrical engineering. Cryptography plays a vital role in various aspects of daily life, including ATM cards, computer passwords, and online shopping. When employing cryptography to transmit a message, the content is transformed, or encrypted, before being sent. This process is achieved through a "code" or, more precisely, a "cipher." The transformed text is referred to as "ciphertext," which makes the message difficult to decipher [14]. To decrypt the message and make it readable again, the recipient must possess the secret method for reversing the encryption, known only to the sender and receiver. The practice of deciphering the ciphertext to unveil the secret is called "cryptanalysis," "cracking," or sometimes "code-breaking." Different cryptographic techniques can offer varying levels of ease of use and effectiveness in hiding the secret message. Ciphers utilize a "key," which is a secret element that conceals the encrypted message. The cryptographic method itself does not need to be kept secret. Multiple individuals can employ the same method but different keys, ensuring that they cannot read each other's messages. For example, the Caesar cipher, which has as many keys as there are letters in the alphabet, can be easily deciphered by trying all the possible keys. However, more complex methods are required to crack ciphers with billions of potential keys [2-4].

In Symmetric cryptography, the sender and receiver share the same key. The sender utilizes the key in a specific manner to encrypt the message, while the receiver uses the same key in the opposite way to decrypt and reveal the message. Most cryptographic systems are symmetric, with the Advanced Encryption Standard (AES) being a widely used example.

Asymmetric cryptography is harder to use. Each participant employing asymmetric cryptography possesses a secret key and a distinct "public key" that can be shared with others.

When someone wishes to send a message to a recipient, they use the public key to encrypt the message. The message can only be decrypted by the receiver using their secret or "private key." This way, the secret key does not need to be disclosed to anyone else. Asymmetric cryptography is often used for computer signatures, ensuring that a file is verified as originating from a specific sender. For instance, software companies use it to sign updates, proving their authenticity and protecting against malicious alterations. Asymmetric ciphers are also utilized by computers to exchange keys for symmetric ciphers. While symmetric cryptography is more practical for message transmission, asymmetric cryptography serves crucial roles in digital signatures and secures key exchange.

There are two widely utilized encryption standards are AES (Advanced Encryption Standard) and DES (Data Encryption Standard). AES is based on a design principle known as a substitution-permutation network, combination of both substitution and hardware. Unlike DES, AES does not employ a Feistel network. AES is a variant of Rijndael, with a fixed block size of 128 bits and a key size of 128, 192, or 256 bits. In contrast, the Rijndael specification allows block and key sizes to be any multiple of 32 bits, ranging from a minimum of 128 to a maximum of 256 bits. On the other hand, DES is a symmetric block cipher that utilizes a shared secret key with a length of 56 bits. It was published as the Federal Information Processing Standards (FIPS) 46 standard in 1977 and officially withdrawn in 2005. DES is now considered insecure for many applications due to its small key size. In 1999, distributed.net and the Electronic Frontier Foundation collaborated to publicly break a DES key in just 22 hours and 15 minutes, highlighting its vulnerability. Although there are theoretical weaknesses in the cipher, practical exploitation is infeasible. Triple DES, which applies the DES algorithm three times, is believed to be secure in practice, despite the existence of theoretical attacks. In recent years, AES has replaced DES as the preferred encryption standard. Additionally, the National Institute of Standards and Technology has withdrawn DES as a standard [4, 9, 13 & 15].

4. Work Analysis on Cryptography:

Some research papers published over the last two decades. The survey is conducted based on specific keywords, and the papers have been classified accordingly. The keywords considered for classification include artificial neural network, K nearest neighbor, support vector machine, AES, DES, Blowfish, decision tree, data mining, genetic algorithm, public key, fuzzy classification, mean square error method, symmetric key encryption, polynomial interpolation, Vignere cipher, quantum cryptography, key-based multiple Huffman tables, and tree parity machine, among others. The classification of papers based on these keywords aims to analyze the extent of work carried out using different techniques and algorithms in the field of cryptanalysis.

The study reveals that the study of cryptanalysis using neural networks experienced a decline before the last two decades. However, the survey demonstrates a recent growth in this field, suggesting the presence of a research gap and opportunities for further exploration. The referenced papers provide a comprehensive range of future scope that can be explored through additional research. The study serves as a foundation for further investigation, considering the referenced papers included in the survey [15].

5. Future Scope on Cryptography:

In conclusion, evolutionary computation (EC) methods, along with computational intelligence (CI) methods in general, can serve as practical tools for assessing the efficiency and

effectiveness of proposed cryptographic systems. Cryptography extends its scope to include the cryptanalysis of substitution-permutation systems and potential variations of the rotor machine. The framework employed in this study can handle not only binary and categorical attributes but also continuous quantitative attributes. A promising approach involves making the sender's keying information public, thereby eliminating the need for a secure key distribution channel. The exploration of chaotic maps for transforming synchronized network states into chaotic encryption keys shows potential with remarkably low tolerance for decryption errors. Further experiments are necessary to complete the results and ensure the safety of the cryptographic procedure. Advanced synchronization algorithms involving different types of chaotic synchronization appear to offer enhanced security. Utilizing the Data Encryption Standard (DES) alongside sophisticated cryptosystems like public key encryption and exploring efficient algorithms to reduce the search space for keys and employing neural networks to obtain the correct keys are viable approaches. The key distribution center plays a vital role in generating and securely distributing the secret key using various methods. The success of majority attacks highlights the need to explore algorithms where the attackers' overlap develops faster than their overlap with other parties. This can potentially be achieved by employing larger K values or making other modifications. These models are currently under consideration and ongoing investigation.

6. Conclusion:

Considering the above survey and analysis, one can easily identify the work done in cryptanalysis using various techniques and algorithms. Further the reader can identify the scope in which studies can be carried out to enhance the analysis being done in that particular field. This paper just not merely list the number of research paper that have been published since decades. But also depicts the summary of those research papers. The representation of statistics is self explanatory to draw the conclusions regarding the work done in various fields of cryptanalysis. This paper will be a supplement to boost the research work in cryptanalysis.

References

[1] Bagnall, A. J. et al. (2000). Cryptanalysis of a three rotor machine using a genetic algorithm.

[2] Klein, E. et al. (2004). Synchronization of neural networks by mutual learning and its application to cryptography. Advances in Neural Information Processing Systems 17 (NIPS 2004).

[3] Laskari, E. C. et al. (2007). Cryptography and Cryptanalysis through computational intelligence. Springer - Computational Intelligence in Information Assurance and Security, pp. 1-49.

[4] Alallayah, K. et al. (2012). Applying neural networks for simplified data encryption standard cipher system cryptanalysis. IAJIT, Vol.09, No. 02, pp. 163-169.

[5] Francisco, L. & Iglesias, S. (2012). Probabilistic attacks on neural cryptography.

[6] Sharaf, M. S. (2009). Quantum cryptography: A new generation of information technology security system. IEEE computer society, Sixth International Conference on Information Technology: New Generation, pp. 1644-1648.

[7] Jogdand, R. M. & Bisalapur, S. S. (2011). Design of an efficient neural key generation. IJRAIA, Vol. 02, No. 01, pp. 60-69.

[8] Mislovaty, R. et al. (2004). Security of neural cryptography. Proceedings of the 2004 11th IEEE International Conference.
[9] Lawrence, S. et al. (1997). Lessons in neural network training over fitting may be harder than expected. Proceedings of the Fourteenth National Conference on Artificial Intelligence (AAAI-97), pp. 540-545.
[10] Chakraborty, S. et al. (2015). Neural synchronization based secret key exchange over public channels: A survey.
[11] Jin, W. (2004). Fuzzy classification based on fuzzy association rule mining.
[12] Diffie, W. & Hellman, M. E. (1976). Multiuser cryptographic techniques. AFIPS 76.
[13] Mishra, S. & Bhattacharya, A. (2013). Pattern analysis of cipher text a combined approach. Proceeding of the IEEE conference on ICRTIT, pp. 393-398.
[14] Abood, O. G. & Guirguis, S. K. (2018). A survey on cryptography algorithms. IJSRP, Vol. 08, Issue 07, pp. 495-516.
[15] Kaur, J. & Ramkumar, K. R. (2022). The recent trends in cyber security: A review. IKSUCIS, Vol. 34, pp. 5766-5781.
[16] Diffie, W. & Hellman, M. E. (1979). Privacy and authentication: An introduction to cryptography. Proceedings of the IEEE, Vol. 67, Issue 03, pp. 397-427.
[17] Winterhof, A. (2002). Popynomial interpolation of the discrete logarithm. Design, Dodes and Cryptography, Vol. 25, pp. 67-72.
[18] Dileep, A. D. & Sekhar, C. C. (2006). Identification of block cipher using support vector machines. Proceedings of the IEEE International Joint Conference on Neural Network.
[19] Thomas, B. (2008).Quantum security of block ciphers: Design and cryptanalysis tools.
[20] Alallayah, K. et al. (2012). Attack and construction of simulator for some of cipher system using Neuro-Identifier. IAJIT, Vol.07, No.02, pp. 365-372.
[21] Nuhn, M. & Knight, K. (2014). Cipher type detection. Proceedings of the 2014 EMNLP, pp. 1769-1773.