International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 5 | Issue 4 | ISSN : 2456-3307
DOI : https://doi.org/10.32628/CSEIT195412

A Brief Review on Methodology of Cryptanalysis

K V Srinivasa Rao[1], Prof. M M Naidu[2], Prof. R. Satya Prasad[3]
[1]Research Scholar, Acharya Nagarjuna University, Andhra Pradesh, India
[2]Professor (Retired), S.V University College of Engineering, Andhra Pradesh, India
[3]Professor & HOD, Acharya Nagarjuna University, Andhra Pradesh, India

ABSTRACT

Cryptanalysis comes into deferent forms in order to support that rigorous analysis of the structure cryptographic primitive to evaluate and verify its claimed security margins. This analysis will follow the attack models represented previously in order to exploit possible weakness in the primitive. Thus, achieving the associated attack goals which will vary from a distinguishing attack to a total break that is defined based on the security margins or claims of the primitive under study. For example, for a hash function, total break constitutes finding a collision or obtaining the message from the hash value. While in block ciphers it revolves around recovering the secret key. When it comes to the claimed security margins, the design approaches will follow certain security models as in provable security or practical security or a mixture of both. The role of cryptanalyst is to subject these primitives to different existing categories of cryptanalysis approaches and tailor new ones that will push the design's security margins. This paper will introduce the prominent methods of cryptanalysis that utilize certain behavior in the cipher structure. Such behavior disturbs the assumed randomness of the output or the cipher text. This Paper will also explore the basic definitions of prominent cryptanalysis methods that targets the specific structure of a cipher namely differential and linear cryptanalysis and their different variants. It will also discuss other potential crytpanalytic methods that are usually used in symmetric-key ciphers analysis especially block ciphers.

Keywords: Cryptanalysis, Block Ciphers, Linear Cryptanalysis

I. INTRODUCTION

Computer data often travels from one computer to another, leaving the safety of its protected physical surroundings. Once the data is out of hand, people with bad intention could modify or forge your data, either for amusement or for their own benefit. Cryptography can reformat and transform our data, making it safer on its trip between computers. The technology is based on the essentials of secret codes, augmented by modern mathematics that protects our data in powerful ways.

- Computer Security – generic name for the collection of tools designed to protect data and to thwart hackers.
- Network Security - measures to protect data during their transmission
- Internet Security - measures to protect data during their transmission over a collection of interconnected networks Security Attacks, Services and Mechanisms.

To assess the security needs of an organization effectively, the manager responsible for security needs some systematic way of defining the requirements for security and characterization of approaches to satisfy those requirements. One approach is to consider three aspects of information.

security: Security attack – Any action that compromises the security of information owned by an organization.

Security mechanism – A mechanism that is designed to detect, prevent or recover from a security attack. Security service – A service that enhances the security of the data processing systems and the information transfers of an organization. The services are intended to counter security attacks and they make use of one or more security mechanisms to provide the service. Basic Concepts of Cryptography, the art or science encompassing the principles and methods of transforming an intelligible message into one that is unintelligible, and then retransforming that message back to its original form Plaintext. An algorithm for transforming an intelligible message into one that is unintelligible by transposition and/or substitution methods with Key is encryption algorithm. The transformed unintelligible text is cipher. Some critical information used by the cipher is known only to the sender & receiver. Encipher (encode) The process of converting plaintext to cipher text using a key. Decipher (decode) the process of converting cipher text back into plaintext using a cipher and a key. Using the study of principles and methods of transforming an unintelligible message back into an intelligible message without knowledge of the key is called code breaking or cryptanalysis. In both cryptography and cryptanalysis Code, An algorithm for transforming an intelligible message into an unintelligible one using a code-book can be designed. Cryptography, Cryptographic systems are generally classified along 3 independent dimensions: Type of operations used for transforming plain text to cipher text. All the encryption algorithms are based on two general principles: substitution, in which each element in the plaintext is mapped into another element, and transposition, in which elements in the plaintext are rearranged. The number of keys used If the sender and receiver uses same key then it is said to be symmetric key (or) single key (or) conventional encryption. If the sender and receiver use different keys then it is said to be public key encryption. The way in which the plain text is processed A block cipher processes the input and block of elements at a time, producing output block for each input block. A stream cipher processes the input elements continuously, producing output element one at a time, as it goes along.

Cryptanalysis, The process of attempting to discover X(plain text) or K(key) or both is known as cryptanalysis. The strategy used by the cryptanalysis depends on the nature of the encryption scheme and the information available to the cryptanalyst. There are various types of cryptanalytic attacks based on the amount of information known to the cryptanalyst. Cipher text only – A copy of cipher text alone is known to the cryptanalyst. Known plaintext – The cryptanalyst has a copy of the cipher text and the corresponding plaintext. Chosen plaintext – The cryptanalysts gains temporary access to the encryption machine that uses it to decrypt several string of symbols, and tries to use the results to deduce the key. They cannot open it to find the key. However; they can encrypt a large number of suitably chosen plaintexts and try to use the resulting cipher texts to deduce the key.

II. EXISTING METHODOLOGY

Estimating Differential Probability

This difference in the differential property is usually achieved through an XOR, since it is the common operation for the key mixing layer. In addition to other modular group operations as in modular addition as mentioned earlier. The difference operation is chosen to eliminate the effect of the key used in the system when applying differential relation to undergo the attack. For example, if we have two ciphertexts/plaintext pairs (c1,m1) and (c2,m2) produced by $c1 = f(m1) = m1 \oplus k$ where the key is k and f is the encryption process. We will obtain $c1 = m1 \oplus k$ and $c2 = m2 \oplus k$. Applying the difference relation we will obtain $c2 \oplus c1 = m2 \oplus m1 \oplus k \oplus k = m2 \oplus m1$. Similarly if we considered modular addition over certain integer values, the same concept will hold, yet the additive inverse of an element over the group (or ring of integers) should be considered when the difference is applied. In this sense, c2*c1−1 = (m2*m1−1)* (k−1)* k = m2*m1−1 given that c1 = m1*k and c2 = m2*k where * denotes multiplication. It should be noted that the non-linear layer in cryptographic primitive or specifically block ciphers as in S-box layer or modular addition is the main target to reflect the probability of holding such difference. Since the input difference will yield a certain output difference with specific probability when passing this layer. This is not the case for the linear layer which does not affect the difference operation. This indicates that the probability of this difference after passing the linear layer, is 1. This is not the case for the non-linear layer. The differences will propagate through this layer with certain probability. A difference distribution table for an S-box can be constructed where all probabilities of all possible input/output differences are stated. Similarly to Definition , For an S-box S : Fn 2 →Fm 2 the difference over the S is defined as DP(α,β)=2−n#{x ∈Fn 2|(S(x⊕α)= S(x)⊕β)} If f is parametrized by a key K of size k, then the differential probability DP(α,β;K) can be defined for random variable K uniformly distributed over the key space of size 2k where K ∈ κ. This will motivate the computation of the average differential probability over the full key space. This term is referred to as Expected Differential Probability (EDP) which can be defined as the following: EDP(α,β)=PK∈κ DP(α,β;K) 2k.

Differential Characteristic

In practice symmetric-key primitives in general and block ciphers in specific are built from compositions of a single transformation or round function (encryption of decryption). This concept is what is referred to as iterated cipher. For iterated block ciphers, an encryption is defined by a composition of a function (i.e rounds) EK = R(r) kr ◦R and similarly decryption is defined by a composition of a function (i.e rounds) EK = R^{-1}(r) kr ◦R^{-1} . Differential properties (similar to linear properties) are examined on a scale of one round and then extended on the rest of the rounds. This concept is referred to as Differential Characteristic in differential cryptanalysis.

Definition. A differential characteristic DC is a sequence of intermediate differences through the different steps of encryptions at each round of the composition of rounds under study. 40 → R1 →41 … → .. →4r−1 → Rr →4r The sequence is indicated by an input difference and a collection of output differences of each step.

or alternatively DP(DC)= #{x ∈Fn 2|(Rr ◦Rr−1.......◦R1)(x⊕40)=(Rr ◦Rr−1.......◦R1)(x)⊕4r} 2n Assuming these characteristics are independent, the probability of accumulating characteristics that will take an input difference to output difference over multiple applications of R and intermediate differences is the product of these characteristics. This is because of ciphers that follow Definition ref. of Markov and form a homogeneous Markov chain, such that sequence of differences in the chain of differences where every intermediate consecutive differences are independent of each other, and the probability distribution for all consecutive differences is the same. It is worth noting that the differential probability of a differential characteristic indicates the fraction number of right pairs that will satisfy given input/output difference.

When the differential probability of a r-round differential characteristic is too small to be used directly, the cryptanalyst uses α = 40 r−rounds −−−−−→ β = 4r where differences in between the rounds are not considered. Only input and output difference will be taken into consideration. This is usually referred to as r-round differential which are a collection of several r-round differential characteristics that starts and end with the same input/output difference. They can be also referred to as differential paths or trails. The probability of such differentials is DP(α,β)= Pr(4r = β|40 = α)= X DC∈(α,β) DP where a differential would have an input α = 40 and output β = 4r of the difference approximation (α,β). This can be viewed as having many trails between α → β where each r-round differential characteristic with the specific intermediate differences is a single differential trail or differential path of α → β. This differential probability of the various differential relations over R can be expressed in a matrix that is referred to as difference transition probability matrix (M) [9]. This matrix will be constructed for n-bit Markov cipher with dimensions of (2n−1)(2n−1).

Each entry will constitute the probability of the differential the differential characteristic with corresponding input/output differences to a matrix row and column respectively. For r-round differential between the input/output differences, the entries in mr will reflect their probabilities.

In the application of differential cryptanalysis, cryptanalyst aims to obtain the best or highest possible differential probability given that it obtains reasonable attack complexity. This can be also referred to Maximum Differential Probability (MDP) MDP(R)= MAXα6=0,β(DPR(α,β)) where the maximum is taken over all possible differential probabilities over all possible input/output difference except zero input differences. The same concept can be applied to obtain the maximum differential r-round characteristic probability under the assumption of rounds independence as follows.

This can be utilized in evaluating the security of a cryptographic primitive, in this context SPN-based block ciphers or Feistel ciphers with SP components, against differential cryptanalysis. Deciding the minimum number of active S-boxes or a lower bound on this number is a practical approach of this evaluation. This can be achieved through approximating an upper bound on maximum differential characteristic probability. As for ARX structures, bit-level deferential analysis is carried out which indicates that finding differential paths might be complex [4], [3]. This form of differential analysis contains analysis on the probability distribution of for integer addition with carry, differential probability for modular addition, and differential probability of XOR for differences that use modular addition where an algorithm using matrix multiplication is utilized [4], [8].

Key Recovery and Data Complexity

Considering the target of the cryptanalysis is block cipher with an input block of size n, a secret key of size k, and iterating on r number of rounds. The cryptanalyst will aim to construct an effective (r −1)-round differential (α,β) or (r −1)-round differential characteristic (α,β) for a reduced number of rounds usually r−1. The attack complexity achieved by this differential characteristic or differential should be considerably less than the full codebook 2n to be deemed usable in less than exhaustive search terms.

The attacker's goal of key recovery is to use the filtered plaintext/ciphertext pairs, and the established differential relation (α,β) to (partially or fully) guess the last round r key kr. Using the guessed key kr for a partial decryption for the given ciphertext pair (cr,c0 r) which obtains β = 4r−1. This indicates that the guessed key is a candidate key. This will be achieved for each key in 2|kr| where |kr| is the size of the round key and every pair of the filtered set. The candidates keys with the highest number of matches for the differential characteristic on the set of filtered pairs will be the right key. The time complexity for the guessing phase is less than 2|kr|. In principal values of input differences, intermediate differences, output differences, and the keys will affect the differential probability of a certain (r −1)-round characteristic. The attacker will have to evaluate probability of a differential or a characteristic in correspondence to the all possible key values obtained and pairs of plaintexts. Since this is not practical scenario as most of the pairs of plaintext/ciphertext obtained using some fixed key. Stochastic key equivalence is established under the assumption that round keys behave independently and most of the secret keys will behave similarly. It states that the differential probability of obtaining a certain output difference after r−1 rounds given a certain input difference is approximately the same to the differential probability of obtaining the same output difference after r−1 rounds given the same input difference and the associated rounds keys. This is not true for all ciphers as in IDEA [5] , [1].

Further estimates on the success probability and data complexity are provided. There are several extensions and variations of differential cryptanalysis that were introduced to target different cryptographic primitives or specifically block ciphers based on their accurate structure and differential behaviour. This includes truncated differential cryptanalysis, impossible differential cryptanalysis and higher-order differential cryptanalysis. Although they might be restricted to certain differential behaviour or structure, yet when performed they yield relatively better results than classical differential cryptanalysis in terms of data complexity and number of rounds attacked.

Truncated Differential Cryptanalysis

Introduced by Knudsen in [10], truncated differential cryptanalysis is an extension to differential cryptanalysis. It tends to be used on ciphers that appear to be resistant to classical differential cryptanalysis.

The basic idea is to construct a partially known input/output differences where after certain number of rounds only a part of the output difference is known. It shows that to construct differential property it is not necessary to know the full n-bit difference as few bits will be enough. It is achieved by applying a truncation for the differential property that represents the bits as known bits value as(0)which indicates same value in the same bit location. In addition to (∗) where it denotes an unknown or free value that could be 1 or 0 so values at the indicated position can be similar or different. This can be also applied to bytes where non-zero byte differences will be grouped together. Truncated differential characteristic can be viewed as set of characteristics which resembles the case of differential. Considering bits that are the same in value and in the same location in the output differences will obtain higher probability than classical scenario of focusing only one output difference. Truncated differential approach might not be practical for certain designs as they tend to achieve best results for ciphers with slow diffusion layers as truncated differentials tend to spread the differential properties to the whole state faster than differentials. They tend to provide better results in comparison to classical differentials when applied as they might provide better differential probability, lower data complexity or an increment to the number of rounds attacks [6].

Linear Characteristic and Linear Hulls

As in differential characteristic, these approximations are traced within the cipher structure to form a linear characteristic.

Definition :A linear characteristic is a sequence of linear approximations or relations for a given number of rounds. Each element in this list will determine the linear bias or the correlation of the respective linear characteristic. These approximations can be expressed as ΓI0,...,ΓIr where the list of input/output/intermediate values are stated as the following I0 = P,.....,Ir = C. As in the relation between 0differentials and differential characteristics, the set of linear characteristics with input/output masks (α = ΓI0 = α0,β = ΓIr = αr) respectively is referred to as a linear hull of the approximation (α0,αr). In this respect as with differential trails, each r-round characteristic with the following sequence (α0,. ,αr) is a trail between the starting input/output masks where there can be more than one trail between these two masks.

Linear Probability Estimations

As we have discussed in the previous section, the linear layer (i.e permutation layer) will preserve the linear property with probability 1, while the non-linear layer (i.e S-box or Modular addition) will propagate it with certain probability.

The combined probability for these linear approximations is calculated using the pilingup lemma introduced by Matsui in [2].

To go through this deduction certain notations shall be introduced [6]. First, starting with Fourier transfer on a boolean function which can be defined as f : Fn 2 →F2 ˆ f(a)= X x∈Fn 2 f(x)(−1)ha,xi where a ∈Fn 2 In this case, ha, xi is the dot product between the two values. Applying this Fourier transform on the sign function fx = (−1)f = 1−2f is going to obtain the difference between the number of times the function f and ha, xi are equal and differ from each other. This is referred to as Walsh Transform of f ˆ fx(a)= X x∈Fn 2 (−1)f(x)⊕ha,xi To denote the probability that f(x) =hα, xi which is Peq = Pr(f(x) =hα,xi).

These correlation and bias calculations are usually used to construct a linear approximation table on the the non-linear function in the cipher which is usually the S-box in SPN structures of block ciphers. The linear approximation table will represent all possible linear input/output masks and their associated probabilities. For example, if S : Fn 2 →Fm 2 for small integers m and n with input/output masks (α,β) then S(α,β) =#{X ∈Fn 2such thathβ,S(X)i=hX,αi} The probability and correlation of the linear input/output masks (α,β) can be expressed as the following [2,76]: In [7], An estimation of linear trails correlation was stated stated for key alternating ciphers which is a subclass of Markov ciphers that will alternate the use of number of keys (XORing or adding the keys to the rounds) with a key independent instances of round functions . It was noted that when considering linear trails it should be noted that they are key dependent where only the sign of the correlation depends on the key. The correlation of the linear hull will be the sum of these trails' correlations.

Key Recovery in Complexity Data

Matsui proposed two algorithms for recovering key information using linear cryptanalysis. The first algorithm which is referred to in the literature as Matsui's Algorithm 1 which is considered a distinguishing attack since it aims to find one bit of the key based on the obtained linear probability or correlation of the linear approximation (α,β). While Matsui Algorithm 2 will find part of the last round key based on the obtained linear probability or correlation of the linear approximation of the r rounds given a large number of plaintext and cipher text pairs.

The data complexity and the success probability of linear cryptanalysis over exhaustive search is dicussed in [8]. Assuming that the presented linear approximation probability will not reveal anything for the wrong key (Pr = 1 2), and will be independent for each candidate key. The success probability PS with respect to at least a-bit advantage is measured with respect to the needed N plaintexts/ciphertexts where a and N are large is as follows:

Linear Cryptanalysis based on chosen plaintexts was proposed on DES to reduce the data complexity of the original attack [3]. There are various extensions to classical linear cryptanalysis that aims as well to reduce the complexity or improve the attack by recovering more key bits. One example is using multiple linear approximations to obtain more information about the key bits [11], [9], [2], [10], [4]. These results were improved in multidimensional linear attacks because they involve many key, several key bits of K can be derived at the same time [1], [10]. Thus, the data complexity will be reduced to the capacity based on the bias of all biases of different approximations Cap =qP2 i. However, due to the simultaneous processing of multiple approximations the time complexity of the approximation analysis has been increased.

Other Variants

Cryptographic attacks goes beyond what has been discussed so far in this chapter. As there are many variants that target certain components as in key scheduling, or the structure of the cipher as integral attacks. There attacks which targets the behavior of the cipher in the implementation environment as in hardware attacks (i.e Deferential Power Analysis, timing attacks, etc). The following sections will briefly describe integral and cube attacks.

Cube Attacks

A variant of higher order differentials is cube attack. The attack was proposed by Dinur and Shamir in [8]. The aim of the attack is to get a linear function of the secret key bits by summing over different inputs even under the assumption that attacker does not know specifics of the cipher design. If a single output bit can be expressed in a low degree polynomial then algebraic attacks have a better chance of success. It should be noted that the attack will have a higher complexity with a bigger size of index set I, so getting the appropriate max. Term will be challenging for long max. terms yet easier for short ones. When looking for an appropriate max. terms, I is set randomly then it will be updated with indices until the super poly is a constant value (linear relation) then the search for another max. Term will do all over. Linearity tests on various max. Terms is applied to get a linear super poly, this is referred to as cube testers [2]. Cube attacks work well for polynomials of low degrees. However, most block ciphers have relatively high algebraic degree. To be utilized for output bits might have low degree, The can be used on the outputs of NLFSR of stream ciphers. These attacks were applied on reduced round Trivium [6].

Integral Cryptanalysis

Integral attacks were first introduced by Knudsen in their application on SQUARE in [7] and later on was applied and generalized under different references as in multiset attacks and saturation attacks on Twofish [10]. The attack relies on constructing sets of or multisets of chosen plaintexts that either sum to a constant or differs in certain parts of the set. Thus exploiting relations between various encryptions. The main goal of the attack is to follow the preservable nature of certain properties of the sets. For example, in integral attacks, the set I of internal states are constructed such that they differ in only one byte d0 which covers all 28possibilities. It is noted that this property will hold after an application of an S-box layer (or a bijective transformation) to the state I. While the diffusion layer will make the rest of the bytes active.

An n-bit value multiset can be defined as unordered tuple where values might recur. The multiset might have certain properties that can be utilized as a distinguishing factor in an attack. For instance, if all values in the multiset are the same then this multiset will have the property C that refers to a constant. If all values are different then the multiset is referred to as A or all. S refers to the fact that the sum of the values can be predicated while? Refers to the fact that it cannot be predicted. There are other properties as well that are utilized in integral or multiset attacks. If each value in the mutliset occurs zero or even number of times, then this multiset is even or E. In addition to that a multiset is a permutation or P if it holds only once every 2m possibilities. Finally, a multiset has a property Balanced B if the XOR of all values is zero this is closer to the S property. Any multiset which is a permutation or even multiset is called dual or D multiset which is also balanced [8].

As stated throughout this paper, resistance to cryptanalytic methods depends on the selected designs parameters by the designers which take into consideration the implementation environment as well. The goal of the designers is to establish an infeasible attack margins through pushing the probabilities of the characteristics presented to be small. In addition to raising the data complexity of the potential attacks. An example of such design strategies that presents certain bounds on the probabilities of differential and linear characteristics for certain design structure and given number of rounds is the wide-trail strategy which is used in AES [5]. It shows that the composite choice of nonlinear layer, linear layer and key mixing layer can control the differential and linear bounds of the attack. As important it is to select an S-box (non-linear layer) which achieves the smallest potential differential and linear probabilities, it is crucial to choose the appropriate linear layer. In common terms such linear layer shall provide a good diffusion property where the number of active S-boxes is maximized in the next round over certain number of rounds. Hence, affecting the propagation of linear and differential properties to be minimal.

III. CONCLUSION

In this paper we discussed various types of cryptanalysis techniques. If we know about various types of attacks then it is very useful to improve the cryptographic algorithm or encryption techniques. The knowledge of various type of attacking techniques helps to make our system safe from any cryptographic attack. The overall observation tells that various cryptosystem in this paper reviewed is having its weak and strong points. Therefore according to our requirement we can choose the appropriate cryptosystem and analyse that cryptosystem so as to get enhanced performance in a more better way.

Cryptanalysis is most commonly practiced in two arenas. The first use is Cryptographers employ cryptanalytic techniques during the creation of new cryptographic algorithms.

If cryptanalytic techniques uncover vulnerabilities in a cryptosystem, then the cryptosystem would require modifications which eliminate these vulnerabilities before it should be used. The second major use of cryptanalysis is for espionage. This application of cryptanalysis can take many forms, from warring nations attempting to decrypt each other's military communications, and for rival industries attempting to uncover each other's fabrication.

This analysis will follow the attack models represented previously in order to exploit possible weakness in the primitive. Thus, achieving the associated attack goals which will vary from a distinguishing attack to a total break that is defined based on the security margins or claims of the primitive under study.

IV. REFERENCES

[1]. Akshima, D. Chang, M. Ghosh, A. Goel, and S. K. Sanadhya. Improved Meet-inthe-Middle Attacks on 7 and 8-Round ARIA-192 and ARIA-256. In A. Biryukov and V. Goyal, editors, Progress in Cryptology – INDOCRYPT 2015: 16th International Conference on Cryptology in India, Bangalore, India, December 6-9, 2015, Proceedings, pages 198–217. Springer International Publishing, 2015. ISBN 978-3-319-26617-6.

[2]. Akshima, D. Chang, M. Ghosh, A. Goel, and S. K. Sanadhya. Single Key Recovery Attacks on 9-Round Kalyna-128/256 and Kalyna-256/512. In S. Kwon and A. Yun, editors, Information Security and Cryptology - ICISC 2015: 18th International Conference, Seoul, South Korea, November 25-27, 2015, Revised Selected Papers, pages 119–135. Springer International Publishing, 2016. ISBN 978-3-319-30840-1.

[3]. R. AlTawy, O. Duman, and A. M. Youssef. Fault Analysis of Kuznyechik. IACR Cryptology ePrint Archive, 2015/347, 2015. https://eprint.iacr.org/2015/347. pdf.

[4]. R. AlTawy and A. M. Youssef. A Meet in the Middle Attack on Reduced Round Kuznyechik. IEICE Transactions, 98-A(10):2194–2198, 2015.

[5]. R. Ankele, S. Banik, A. Chakraborti, E. List, F. Mendel, S. M. Sim, and G. Wang. Related-Key Impossible-Differential Attack on Reduced-Round SKINNY. Cryptology ePrint Archive, Report 2016/1127, 2016. http://eprint.iacr.org/2016/1127.

[6]. K. Aoki and Y. Sasaki. Meet-in-the-Middle Preimage Attacks Against Reduced SHA-0 and SHA-1. In S. Halevi, editor, CRYPTO, volume 5677 of Lecture Notes in Computer Science, pages 70–89. Springer Berlin Heidelberg, 2009.

[7]. S. Azimi, Z. Ahmadian, J. Mohajeri, and M. Aref. Impossible differential cryptanalysis of Piccolo lightweight block cipher. In Information Security and Cryptology (ISCISC), 11th International ISC Conference on, pages 89–94, Sept 2014.

[8]. S. Banik, A. Bogdanov, T. Isobe, K. Shibutani, H. Hiwatari, T. Akishita, and F. Regazzoni. Midori: A Block Cipher for Low Energy. In T. Iwata and J. Cheon, editors, Advances in Cryptology ASIACRYPT 2015, volume 9453 of Lecture Notes in Computer Science, pages 411–436. Springer Berlin Heidelberg, 2015. ISBN 978-3-662-48799-0.

[9]. A. BANNIER, N. BODIN, and E. FILIOL. Automatic Search for a Maximum Probability Differential Characteristic in a Substitution-Permutation Network. Cryptology ePrint Archive, Report 2016/652, 2016. http://eprint.iacr.org/2016/652.

[10]. A. Bar-On and N. Keller. A 270 Attack on the Full MISTY1. In M. Robshaw and J. Katz, editors, Advances in Cryptology – CRYPTO 2016: 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part I, pages 435–456. Springer Berlin Heidelberg, Berlin, Heidelberg, 2016. ISBN 978-3-662-53018-4.

[11]. R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks, and L. Wingers. The SIMON and SPECK Families of Lightweight Block Ciphers. Cryptology ePrint Archive, Report 2013/404, 2013. http://eprint.iacr.org/2013/404.

[12]. R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks, and L. Wingers. SIMON and SPECK: Block Ciphers for the Internet of Things. Cryptology ePrint Archive, Report 2015/585, 2015. http://eprint.iacr.org/2015/585.

Cite this article as :

K V Srinivasa Rao, Prof. M M Naidu, Prof. R. Satya Prasad, "A Brief Review on Methodology of Cryptanalysis ", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 5 Issue 4, pp. 85-93, July-August 2019. Available at doi : https://doi.org/10.32628/CSEIT195412
Journal URL : http://ijsrcseit.com/CSEIT195412