A Survey Report on Various Cryptanalysis Techniques

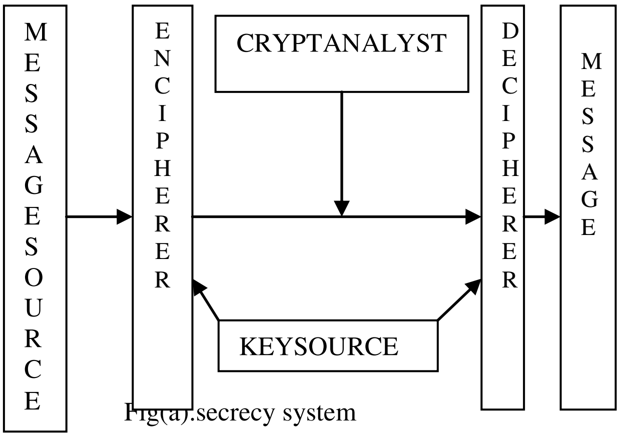
Ashish Kumar Kendhe, Himani Agrawal

Abstract*— *This paper mainly focuses on various types of attacks on symmetric cipher & asymmetric cipher .In this paper we tried to describe the existing cryptanalytic attacks on various ciphers and countermeasures to these attacks have been suggested on the basis of information available to attacker ,computational time requirements and memory requirements etc . In order to develop a new secure cipher, it is very necessary that these attacks should be taken into consideration during development and countermeasures of these attacks should be applied in the design, so that the new design is not vulnerable to these attacks. It will also facilitate the security analysis of the existing ciphers and provide an opportunity to understand the requirements for developing a secure and efficient cipher design. This paper surveys about various cryptanalysis techniques for image encryption schemes ,public key cryptosystems ,various encryption standards such as AES ,DES,RSA etc and then tries to suggest some points to improve the level of security .

Keywords - cipher, cryptanalysis, cryptanalyst, cryptography.

I. INTRODUCTION

Cryptology [15] -[45] is an art and science of hidden or secret writing. It has two main areas: cryptography and cryptanalysis [4]-[45]. Cryptography is basically related with converting data to make them secure and immune to attacks where cryptanalysis is related with breaking of codes [2].The figure(a) below shows the secrecy system used for cryptanalysis.



Fig(a).secrecy system

There are two categories of cryptography.

A. Symmetric key cryptography
B. Asymmetric key cryptography

In symmetric key, there is only single key which is used by sender for encryption and receiver for decryption. In this type the key is shared between both the parties [4].

In asymmetric key, there are two keys: a private key and a public key. Private key is kept by receiver for decryption and public key is announced to public and used for encrypt the data [3]. Now various new techniques are developing for encryption of data as well as various techniques are also evolving in order to hack that data. This paper holds various methods of cryptanalysis which are used in these days.

II. CLASSIFICATION OF ATTACKS

The main goal of a cryptanalyst is to obtain maximum information about the plaintext (original data).Classification of attacks can be done on following basis [4]:

A. Amount of Information Available to Attacker

The main objective of attacking is to access the encryption key in place of simply decrypt the data. Attacks can be classified on the basis of information available to attacker.

□ Cipher text Only: In this type of attack an attacker can access only cipher text or decrypted data but cannot access plain text. This type of attack is done on simple cipher like caesar cipher where frequency analysis can be used to break the code.

□ Known Plain text: In this type a cryptanalyst have plaintext and their corresponding cipher text . Attacker tries to find out the relation between these two.

□ Chosen Cipher text: The attacker obtain the various plaintext corresponding to an arbitrary set of cipher text.

□ Chosen Plain text: The attacker obtain the various cipher text corresponding to an arbitrary set of plain text.

□ Adaptive Chosen Plain text: This is similar with the Chosen Plaintext, except in this attacker chooses subsequent set of plaintext which is based on the information obtain from previous encryption methods.

□ Adaptive Chosen Cipher text: This is similar with the Chosen Cipher text, except in this attacker chooses subsequent set of cipher text which is based on the information obtain from previous encryption methods.

□ Related Key Attack: Like the chosen plaintext, attack in which attacker can obtain only cipher text encrypted with the help of two keys. These keys are unknown but the relationship between these keys is known. Example two keys differ by a single bit.

B. Computational Resources Required

Attacks can also be classified on the basis of resources they require. Those resources are:

□ Time: the number of computation steps (like encryption) that must be performed.

□ Memory: the amount of memory required to perform the task.

□ Data : the amount of plain text or cipher text required.

Actually it is very difficult to find out all these resources very

Manuscript received on May, 2013.

Ashish Kumar Kendhe, Dept of Electronics & Telecommunication, Csvtu/ Sscet/ Sscet, Bhilai, India.
Himani Agrawal, Dept of Electronics & Telecommunication, Csvtu/ Sscet/ Sscet, Bhilai, India.

precisely, specially when the attack isn't practical to actually implement for testing. But academic cryptanalyst tend to provide at least estimated order of magnitude of their attacks difficulty.

III. CRYPTANALYSIS OF SYMMETRIC CIPHER

There are various types of attacks done on symmetric cipher. The explaination is given below:

A. Boomerang Attack

This is a method of cryptanalysis of block cipher based on differential cryptanalysis.This attack provide various avenues of attack on various cipher which are deemed safe from differential cryptanalysis. Example of Boomerang attack in differential cryptanalysis, an attacker exploits how difference in the input to a cipher can affect the resultant change in the cipher. A high probability "differential" is needed that covers all or nearly all of the cipher. This attack allows differentials to used which covers only part of cipher. This attack is used to generate so called "quartet" at the point halfway through the cipher. For this purpose an encryption action E is split into its two consecutive stages E0 and E1 so that E (M) = E1 (E0 (M)), where M is plaintext message.

B. Brute Force Attack

Brute force attack or exhaustive key search is a type of strategy which can be applied on any type of encrypted data. In this type of attack all possible keys are tried systematically until correct key is found. This method is used when any other weakness is not useful. The key length used in the encryption process specifies the practical feasibility of brute force attack, with longer keys exponential more difficult to crack as compared to smaller keys [1].One of the measure strength of the encryption system depends on theoretically how much time is taken to mount a successful brute force attack .The resources required for brute force attack grow exponentially with increase in key size, not linearly.

C. Davies' Attack

This attack is dedicated statistical cryptanalysis method for attacking Data Encryption Standard (DES).This attack was originally created by Donald Davies in 1987.It is a Known Plain Text Attack which is based on non uniform distribution of output of pairs of adjacent S-boxes [3].It works by collecting various plaintext/ cipher text pairs and calculating empirical distribution of its characterstics. Various bits of keys are find out from plain texts, leaving remaining bits to be find out through brute force attack. There is trade off between number of plaintext, keys found and probability of success.

D. Differential Cryptanalysis

This attack is a chosen plaintext attack in which relationship is find out between the cipher text produced by two related plaintext. It focuses on the statistical analysis of two inputs and two outputs of cryptographic algorithm [4].This scheme can successfully crack DES with an effort on the order of 247 chosen plaintext. In the method, the difference can be specified in several ways but eX-clusive-OR (XOR) operation is mostly used. The cryptanalyst then encrypts plaintext and its XORed pairs using all possible sub keys, and it seeks the signs of non- randomness in each pair of intermediate cipher text pairs.

E. Integral cryptanalysis

This attack is applicable on block cipher based on substitution-permutation networks. Unlike differential cryptanalysis, it uses sets or even multiset's of chosen plaintext of which part is held constant and other part varies with all possibilities It is commonly known as Square attack [1].

F. Linear Cryptanalysis

This is a known plaintext attack that require access to large amount of plaintext and cipher text pairs which are encrypted with unknown keys .It focuses on statistical analysis against one round of decryption on large number of cipher text.the attacker decrypts each cipher text using all possible sub keys for one round of encryption and studies the resulting intermediate cipher text to seek the least random result. A subkey which generate the least random intermediate cipher for all cipher texts becomes a candidate key (most likely sub key) [2].

G. Man-in-the-Middle Attack

This type of attack can be used in those cases in which multiple keys are used for encryption[4].This attack is known plain text attack, the attacker has access to both the plaintext and resulting cipher text. Example is attack versus Double DES. To improve the strength of 56-bit DES, Double DES (two rounds of DES encryption using two different keys, of total key length of 112 bits) was suggested. The attacker wants to recover two keys (key1 and key2) used for encryption. The attacker first apply brute force attack on key1 using all 256 different single keys to encrypt the plaintext and saves each keys and cipher text ant analyst again brute force for key2 by using 256.The brute force attack is complete when both keys are known to attacker. The attack takes 256 plus atmost 256 attack, or maximum 257 total attempts. This is far easier than 2112 attempts.

IV. CRYPTANALYSIS OF ASYMMETRIC CIPHER

Asymmetric cryptography is a type which relies on two keys, one private key for decryption and one public key for encryption. Such kind of cipher rely on the "hard" mathematical problem for their security. So the main point of attack is to develop methods to solve such problems. The security of two key cryptography depends on mathematical questions in a way that one key cryptography doesn't, conversely links to wider area of mathematical research in a new way. Asymmetric techniques are designed around of solving various mathematical problems. In case any improved algorithm is found to solve the problem then system is weakened. For example the security of Diffie-Hellman key exchange depends on calculating the discrete logarithm [2].RSA's security depends on difficulty of integer factorization-a breakthrough in factoring would impact security of RSA. Another main feature of asymmetric over symmetric cipher is that cryptanalyst has an opportunity to make use of knowledge obtained from public key [3].

V. SIDE CHANNEL ATTACK

The side channel attacks basically based on some additional information based on some physical implementation of cryptographic algorithm including the hardware used to encrypt or decrypt the data. All cryptographic attacks above described assume that attacker has access plaintext or cipher text pairs or cryptographic algorithm.

A side channel attack basically used additional information like CPU cycle used, memory used, time consumed to perform calculation, voltage used etc [4].There are many practical example of side channel attack. One example of side channel attack is network based.

VI. LITERATURE REVIEW

A. Cryptanalysis of Public Key Cryptosystem Using Generalized inverse of Matrices ,2001.

Hung-Min Sun[5] in this paper proposed a methodology based on the theory of inverse of matrices over a finite field and is mainly motivated for the breaking of public key cryptosystem ,In this the cryptosystem can be broken by representing the cipher text as a linear combination of rows according to the public key .

B. Side Channel Cryptanalysis,2002.

In this paper J-J. Quisquater et.al[6] concluded that the side channel cryptanalysis is a powerful tool and can defeat some implementations of very robust and well suited algorithms.perhaps in the future, other side channels will be discovered but the real cost of these attacks is increasing. In order to be immunated to a high number of cryptanalysis ,implementations must now integrate a very high level of expertise.

C. Cryptanalysis of Security Enhancement For The Timestamp-Based Password Authentication Scheme Using Smart Cards, 2004.

Chou-Chen Yang et.al[7]here proposed the cryptanalysis of security enhancement for the time stamp based password authentication scheme using smart cards and concludes that shen et.al's scheme is vulnerable to the forgery attack.

D.Cryptanalysis of Some Multimedia Encryption Schemes,2005.

Chengqing Li[8] in this paper mainly focuses on the cryptanalysis of some encryption schemes protecting multimedia data, especially the capacity to withstand the known/chosen-plaintext attack. This paper also describes the weakness of scheme, against the known/chosen- plaintext attack.

E.Breaking A Chaos-Noise-Based Secure Communication Scheme,2005.

Shujun Li et.al[9] in this paper concluded that the key space of the studied scheme can be drastically reduced, and that the decryption is insensitive to the mismatch of the secret Key, which means that the scheme can be easily broken.

F.Refined Analysis of Bounds Related to Linear and Differential Cryptanalysis for the AES, 2005.

Liam Keliher [10] in this paper carefully analyzed bounds related to linear and differential cryptanalysis for the AES. This paper presents nontrivial lower bounds on the 2-round maximum expected linear probability (MELP) and maximum expected differential probability (MEDP), trapping each value in a small interval. It then prove that the best upper bounds on the 2-round MELP and MEDP are not tight. Finally, shows how a modified version of the KMT2 / KMT2-DC algorithm can potentially improve existing upper bounds on the MELP / MEDP for any SPN, and we use the modified KMT2 algorithm to tighten the upper bound on the AES MELP to 1.778 × 2^−107, for $T \geq 8$.

G. A Framework for Describing Block Cipher Cryptanalysis,2006.

Raphel C.W Phan [11] in this paper provides a general framework to describe the block cipher cryptanalysis, with the additional capabilities of allowing specification of the technical details of each type of attack and comparison of their respective strengths. In this, comparison of different distinguishers allows us to see the natural generalizations. Using this framework we can easily compare different distinguishers used on basis of their strengths.

H.Cryptanalysis of Simplified Data Encryption Standard via Optimization heuristics, 2006.

Nalini N and G.R Rao[12] in this paper demonstrated the applicability of two optimization heuristics ,simulated annealing (SA) and tabu search for the cryptanalysis of simplified data encryption standard (SDES).On cryptanalysis of SDES using Matlab version 7.1 on p4 system it is concluded that tabu search is more efficient than simulated annealing .

I.Cryptanalysis of Two Password Authenticated Key Exchange Protocols Based on RSA,2006

Tianjie Cao et.al [13] in this paper concluded that the RSA based password authenticated key exchange protocol is insecure against an active off-line dictionary attack.

J.Chaotic Cryptosystems: Cryptanalysis And Identifiability, 2006.

Floriane Anstett et.al[14] provides a general framework based on the identifiability concept for the cryptanalysis of a large class of chaotic cryptosystems is proposed More precisely. It is provided a systematic methodology to test, a priori, during the design stage, whether the parameters of a chaotic cryptosystem may play the role of the secret key or not.

K.Cryptanalysis of a Hash Function Proposed at ICISC, 2006.

Willi Geiselmann et.al[15] Proposed a simple method for constructing collisions for Shpilrain's polynomial-based hash function from ICISC 2006 is presented here. In this from the discussion and demonstration through a specific collision, the hash function proposed in Shp06 does not offer strong collision resistance. Consequently, for applications that rely on collision resistance, the use of this hash function does not seem to be advisable.

L.Cryptanalysis of Mir-1: A T-Function-Based Stream Cipher, 2007.

Yukiyasu Tsunoo et.al[16] in this paper describes the cryptanalysis of mir-1,a new T Function based stream cipher and concludes that the theoretical amount of data required for the attack is no more than about 2^10 words .The attack method in this makes good use of the T-function properties .This is an effective way to attack a T-function based stream cipher.

M.On the vulnerability of Simplified AES Algorithm Against Linear Cryptanalysis, 2007.

S. Davod Mansoori et.al[17] in this paper improves work on first round and develop it for full round linear attack.It shows that this algorithm is vulnerable against linear attack. Undoubtly, one of the important results of this cryptanalysis is that, it will be possible to propose proper linear attack on Rijndael.The linear attack was developed on full rounds SAES in this paper. Using this linear cryptanalysis results, shown the first and second round SAES is breakable with linear calculations. So,this algorithm is vulnerable against linear attack.This,as a consequence, can be led to design a better cryptanalytic attack on real AES.

N.New Results on Impossible Differential Cryptanalysis of Reduced AES,2007.

Wentao Zhang et.al[18] in this paper presented some new results on impossible differential cryptanalysis of reduced AES, which update the best known impossible differential attacks on reduced AES. Firstly it shows, some new attacks on 6-round AES (for all the three key length). Secondly, it extend to 7-round AES, also for all the three key variants. This paper, improved the best known impossible differential attacks on AES. For AES-128, we can reach up to 7 rounds while the previous attacks can only reach up to 6 rounds. For AES-256, we can reach up to 8 rounds while the previous attacks can only reach up to 7 rounds. Furthermore,it presents an improvement of the attack on 7-round AES-192 , which makes the time complexity reduced greatly.

O.Differential Cryptanalysis of T-Function Based Stream Cipher TSC-4,2007.

Haina Zhang et.al[19] in this paper introduces a differential method to analyze TSC-4. Attack is based on the vulnerable differential characteristics in the state initialization of TSC-4, and for the chosen IV pairs, the differential probability is up to2^−15.40 in the case of weak keys. Here developed a differential attack on TSC-4. Utilizing the structure of T-function in TSC-4, we constructed a special differential characteristic with high probability which incurs about 2^72 weak keys. 2^40.53 chosen IV pairs can be used to identify a weak key and recover 8 bits of the weak key. Hence we can recover the other 72 key bits by exhaustive search.

P.Cryptanalysis of Reduced Versions of the HIGHT Block Cipher from CHES 2006,2008.

Jiqiang Lu[20] in this paper presented an impossible differential attack on 25-round HIGHT ,a related-key rectangle attack on 26- round HIGHT, and finally a related-key impossible differential attack on 28-round HIGHT.HIGHT is a 32-round block cipher with a 64-bit block size and a 128-bit user key, which was proposed at CHES -06 for low-resource applications like RFID. Like most cryptanalytic attacks on block ciphers, the presented attacks are theoretical, but they suggest that the reduced versions of HIGHT are less secure.

Q.Cryptanalysis of An Image Encryption Scheme Based On The Hill Cipher,2008.

Chengqing Li et.al[21] in this paper proposed a method for the security and performance of an image encryption scheme based on the Hill cipher .It has been found that the scheme can be broken with only one known/chosen plain-image.There is a simple necessary and sufficient condition that makes a number of secret keys invalid. In addition, the scheme is insensitive to the change of the secret key/plain-image. In conclusion, the encryption scheme under study actually has much weaker security than the original Hill cipher, therefore is not recommended for applications.

R.Cryptanalysis of A Computer Cryptography Scheme Based On A Filter Bank, 2008.

David Arroyo et.al [22] in this paper analyzed the security of a recently-proposed signal encryption scheme based on a filter bank. It has been shown that there exist's a great number of weak keys derived from the fact that the logistic map is not always chaotic. In this it is concluded that the cryptosystem is very weak against a known-plaintext attack in the sense that the secret key can be totally recovered using a very short plain text.

S.Cryptanalysis of A Image Encryption Algorithm,2008.

Nikhil Balaji[23] here presented several weaknesses of the method based on standard cryptanalytic attacks. In this the author perform a side-channel attack & observed the execution time of the encryption algorithm and successfully reduced the key space by a factor of 104 for a key length of 16 digits.

T.Cryptanalysis of An Image Encryption Scheme Based On A New Total Shuffling Algorithm,2008.

David Arroyo et.al[24] in this paper proposed two new image encryption schemes where the encryption process involves a permutation operation and an XOR-like transformation of the shuffled pixels, which are controlled by three chaotic systems. This paper discusses some defects of the schemes and how to break them with a chosen-plaintext attack.

U.Probabilistic Versus Deterministic Algebraic Cryptanalysis—A Performance Comparison,2009.

Enes Pasalic[25] in this paper presented the performance of probabilistic algebraic attacks is compared with classical (fast) algebraic attacks in the context of their application to certain linear feedback shift register (LFSR)-based stream ciphers.Under a reasonable assumption that a good cryptographic function is sufficiently close to a randomly generated function, it has been shown that classical (fast) algebraic attacks outperform probabilistic ones.

V.Breaking A Chaotic Cryptographic Scheme Based On Composition Maps,2009.

Chengqing Li et.al[26] in this paper studied the security of the scheme and reports the following findings:

1) The scheme can be broken by a differential attack with 6 +log L[(MN)] chosen-plaintext, where MN is the size of plaintext and L is the number of different elements in plain-text.
2) The scheme is not sensitive to the changes of plain text .
3) The two composition maps do not work well as a secure and efficient random number source.

W.Cryptanalysis of A Generalized Ring Signature Scheme,2009.

H Wang et.al[27] in this paper proposed an attack on Ren-Harn's generalized ring signature scheme based on elgamal Signature & found that the original scheme cannot satisfy the convertibility. This means that the scheme is broken easily.

X.Cryptanalysis of simplified –DES Using Genetic algorithm,2009.

Vimalathithan.R et.al[28] in this paper presented an approach for cryptanalysis of SDES using genetic algorithm.In this,the time complexity of the proposed approach has been reduced drastically when compared to brute force attack .Though SDES is a simple encryption algorithm ,this is one of the promising methods and can be used to handle other complex block ciphers like DES and AES .

Y.Cryptanalysis of 7-Round AES-128, 2009.

Hadi Soleimany et.al.[29] proposed a new related key impossible Differential attack on 7 round AES-128 which is the first attempt using this technique.In this an attack on 7-round AES-128 with the time complexity of 2^105 , the fastest attack of all the previous ones from time and pre-computation complexities points of view. A key point to construct such attack is using a special property of Mix Column operation of AES. so it is concluded that Attack on 7-round AES-128 with 32 bit structure leads to a better attack than the previous ones from time and pre-computation complexity perspective.

Z.Related-key Cryptanalysis of the Full AES-192 and AES-256,2009 .

Alex Biryukov et.al[30] in this paper presented two related-key attacks on the full AES. For AES-256 He shows the first key recovery attack that works for all the keys and has complexity 2^119, while the recent attack by Biryukov-Khovratovich-Nikoli c works for a weak key class and has higher complexity.The second attack is the first cryptanalysis of the full AES-192. Both attacks are boomerang attacks, which are based on the recent idea of finding local collisions in block ciphers and enhanced with the boomerang switching techniques to gain free rounds in the middle.

AA.Improved Cryptanalysis of the Reduced Grost1 Compression Function, ECHO Permutation and AES Block Cipher,2009.

Florian Mendel et.al[31] in this paper proposed two new ways to mount attacks on the SHA-3 candidates Grost1, and ECHO,and apply these attacks also to the AES.Here results improve upon and extend the rebound attack.Using the new techniques, we are able to extend the number of rounds in which available degrees of freedom can be used. As a result, here presented the first attack on 7 rounds for the Grost1-256 output transformation and improve the semi-free-start collision attack on 6 rounds. Further, it presents an improved known-key distinguisher for 7 rounds of the AES block cipher and the internal permutation used in ECHO.

BB.Breaking A Modified Substitution-Diffusion Image Cipher Based on Chaotic Standard And Logistic Maps,2009.

Chengqing Li, et.al [32] here pointed out that the modified scheme Substitution-Diffusion Image Cipher Based On Chaotic Standard And Logistic Maps is still insecure against the same known/chosen-plaintext attack.

CC.Cryptanalysis And Enhancements of Three-Party Authenticated Key Exchange Protocol Using ECC ,2011.

Shuhua Wu et.al[33] in this paper demonstrated that Yang et.al*'*s three-party authenticated protocol is potentially vulnerable to an unknown key-share attack and impersonation attack.

DD.Cryptanalysis of DES using computational Intelligence,2011.

Vimalathithan. R et.al [34] in this paper proposed to cryptanalyze DES by combining the genetic algorithm and particle swarm optimization. In this paper a known plaintext is used and varieties of optimum keys are computed .Through this approach,the optimum key can be found faster without searching the entire key space .This method satisfactorily perform the cryptanalysis of DES using Matlab version 7.5 in an intel core (2.4ghz) system.

EE.Cryptanalysis of an Efficient Threshold Self-Healing Key Distribution Scheme, 2011.

Huaqun Wang et.al[35] proposed in this paper an attack method against this Self-Healing Key Distribution Scheme ,this key distribution scheme's presents a forward security. Furthermore, this attack method can also be applied to this scheme's backward security. Thus, the original threshold self-healing key distribution scheme is insecure.

FF.Robust Secure Scan Design Against Scan-Based Differential Cryptanalysis, 2012.

Youhua Shi et.al[36] in this paper presented a robust secure design against Scan based differential cryptanalysis ,Scan technology carries the potential risk of being misused as a "side channel" to leak out the secrets of crypto cores.

GG.Cryptanalysis of Two Identity-Based Authenticated Key Agreement Protocols,2012.

Kyung-Ah Shim[37] in this paper presented two identity-based authenticated key agreement protocols proposed by H'olbl and Welzer which are completely broken easily .

HH.Heuristic Search Procedures for Cryptanalysis and Development of Enhanced Cryptographic Techniques, 2012.

Rajashekarappa et.al [38] in this paper proposed an approach for the heuristic search procedures for cryptanalysis and development of enhanced cryptographic techniques.To implement the proposed Tabu search, Genetic, and Simulated Annealing algorithms firstly by utilising cipher text as well as some plain text and secondly by using only the cipher text to retrieve the original data. The goal of this paper is to comparison between Tabu Search, Genetic Algorithm and simulated annealing were made in order to investigate the performance for the cryptanalysis on SDES. The time complexity of the proposed approach has been reduced drastically when compared to the Genetic Algorithm, and Simulated Annealing Algorithm. Result indicates that Tabu search is extremely powerful technique for attacking SDES.

II.AES Security Enhancement By Using Double S-Box, 2012.

Amish Kumar et.al[39] in this paper concluded that the result of this Process is the high bit independent criteria so the avalanche effect also increases and improved the security of AES by improving the avalanche criteria.

JJ.An Analysis of the Attack on RSA Cryptosystem Through Formal Methods, 2012.

Sachin Upadhyay et.al [40] in this paper analyzed the results given by Wiener's, who says that if the private exponent d used in RSA cryptosystem is less than n^0.292 than the system is insecure. We will focus on the result given by Weiner's and try to increase the range of private exponent d up to n^0.5. As n is the product of p & q (which are the relative prime numbers). This paper also aims at considering the different factors that affects the performance of encryption algorithms so as to make our information more secure over the network.

KK.Super-Sbox Cryptanalysis: Improved Attacks For AES-Like Permutations,2012.

Henri Gilbert et.al[41] in this paper introduced the Super-S box cryptanalysis, which very often improves upon the classical rebound or start-from-the-middle attacks both in terms of efficiency and simplicity. This technique leads to improved cryptanalytic results for both Grost -l and ECHO, two SHA-3 candidates, and to the best known-key distinguisher so far for the AES-128 block cipher.

LL.A Review of Various Techniques of Cryptanalysis,2012.

Mr. Vinod Saroha et.al [42],[45] proposed a paper which mainly focuses on various types of attacks which are mainly in use, in particular attacks on symmetric cipher, asymmetric cipher, Hash system.Also on classification of attacks and side channel attacks. It Aim a brief description of all available types of cryptanalysis techniques. In this it is concluded that if we know about all type of attacks then it is very useful to improve the cryptographic algorithm or encryption techniques. The knowledge of all type of attacking techniques helps to make our system safe from any cryptographic attack.

MM.Cryptanalysis of RCES/RSES Image Encryption Scheme, 2012.

Shujun Li, et.al[43] in this paper analyzed the security of RCES (random control encryption system), and points out that it is insecure against the known / chosen-plaintext attacks: the number of required known / chosen plain-images is only one or two. In addition, the security of RCES against the brute-force attack was over estimated. Both theoretical and experimental analyses are given to show the performance of the suggested known/chosen-plaintext attacks.

NN.Cryptanalysis of An Image Scrambling Scheme Without Bandwidth Expansion,2012.

Shujun Li, et.al[44] in this paper presented a comprehensive cryptanalysis on this image scrambling scheme, showing that it is not sufficiently secure against various cryptographical attacks including cipher text-only attack, known /chosen plaintext attack,and chosen-ciphertext attack. In this paper, Based on the cryptanalytic results, concluded that the image scrambling scheme can only be used to realize (lossless or lossy) perceptual encryption, instead of providing a full protection on all visual information in the plain-image.

VI. 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.

On the basis of study of all the above mentioned research papers, the following conclusions can be drawn:-

1) On cryptanalysis of S-DES via optimization heuristics, genetic algorithm ,and computational intelligence in matlab we found that the time complexity for breaking any cipher is reduced and optimum key can be found without searching entire key space when compaired to brute force attack.
2) Cryptanalysis of image encryption scheme based on hill cipher tells that the encryption scheme used is weaker and cannot be recommended for applications.
3) Cryptanalysis of image encryption scheme based on shuffling algorithm shows the defects of scheme used and how to break them with choosen plain text .
4) On Cryptanalysis of AES it is concluded that the aes is a modern block cipher which supports three key lengths 128,192 &256 bits which provides excellent long term security against brute force attacks.
5) Using double s-box method security of AES can also be increased .
6) RSA based password authenticated key exchange protocol is insecure against the offline dictionary attack.
7) Secure communication scheme based on chaos can be easily broken by reducing the key space drastically.
8) On cryptanalysis of image scrambling without bandwidth expansion it is concluded that the scheme is not sufficiently secure against various attacks such as cipher text only attack,known/choosen plain text attack,and choosen ciphertext attack .

ACKNOWLEDGEMENT

The author would like to thank the anonymous reviewers for their valuable comments and suggestions.

REFERENCES

[1] William Stalling "Network Security Essentials (Applications and Standards)", Pearson Education, 2004.

[2] Atul Kahate (2009) ," Cryptography and Network Security", 2nd edition, McGraw-Hill.

[3] Stallings (1999), "Cryptography and Network Security", 2nd edition, Prentice Hall.

[4] William Stallings (2003), "Cryptography and Network Security", 3rd edition, Pearson Education.

[5] Hung-Min Sun, "Cryptanalysis of public key cryptosystem using generalized inverse of matrices ", IEEE communication letters, vol. 5, no.2, 2001.

[6] J-J. Quisquater and D.Samyde ,"Side Channel Cryptanalysis ",SEC publication 2002.

[7] Chou-Chen Yang,Hung-Wen Yang and Ren-Chiun Wang,"Cryptanalysis of Security Enhancement For The Timestamp-Based Password Authentication Scheme Using Smart Cards", IEEE Transactions on Consumer Electronics, vol 50,no.2,2004.

[8] Chengqing Li ,"Cryptanalysis of Some Multimedia Encryption Schemes",IEEE transactions on multimedia ,vol.10,no.3,2008.

[9] Shujun Li ,Gonzalo Alwarez,guanrong chen,and xuanqin mou, "Breaking A Chaos-Noise-Based Secure Communication Scheme" ,2005.

[10] Liam Keliher ,"Refined Analysis of Bounds Related to Linear and Differential Cryptanalysis for the AES"published in International Association for Cryptologic Research, 2005.

[11] Raphel C.W Phan and m umar siddiqui ,"A Framework for Describing Block Cipher cryptanalysis " , IEEE transactions on computers ,vol.55,no.11,2006.

[12] Nalini N and G Raghevendra Rao,"Cryptanalysis of simplified data encryption standard via optimization heuristics", IJCSNS, vol.6,no.1b,2006.

[13] Tianjie Cao and Dongdai Lin "Cryptanalysis of Two Password Authenticated Key Exchange Protocols Based on RSA",IEEE communication letters,vol.10,no.8.2006.

[14] Floriane Anstett, Gilles Millerioux, and Gérard Bloch, "Chaotic Cryptosystems: Cryptanalysis and Identifiability",IEEE Transactions on circuits and systems-1,regular papers ,vol.53,no.12,2006.

[15] Willi Geiselmann and Rainer Steinwandt, "Cryptanalysis of a Hash Function Proposed at ICISC 2006" ICISC ,2007.

[16] Yukiyasu Tsunoo,Teruo saito,Hiroyasu kubo and Tomayasu suzaki, "Cryptanalysis Of Mir-1: A T-Function-Based Stream Cipher", IEEE, 2007.

[17] S. Davod. Mansoori and H. Khaleghei Bizaki, "On the vulnerability of Simplified AES Algorithm Against Linear Cryptanalysis", IJCSNS International Journal of Computer Science and Network Security, vol.7,no.7, 2007.

[18] Wentao Zhang et.al, "New Results on Impossible Differential Cryptanalysis of Reduced AES", SPRINGER , 2007.

[19] Haina Zhang and Xiaoyun Wang,"Differential Cryptanalysis of T-Function Based Stream Cipher TSC-4",SPRINGER,2007.

[20] Jiqiang Lu, "Cryptanalysis of Reduced Versions of the HIGHT Block Cipher from CHES 2006", SPRINGER ,2007.

[21] Chengqing Li ,Dan Zhang , and Guanrong Chen ,"Cryptanalysis of an image encryption scheme based on the Hill cipher" Preprint submitted to Zhejiang University SCIENCE,2008.

[22] David Arroyo,Chengqing Li,Shujun Li and Gonzalo Alvarez, **"**Cryptanalysis Of A Computer Cryptography Scheme Based On A Filter Bank", ELSIVER publication, 2008.

[23] Nikhil Balaji **,"**Cryptanalysis Of A Image Encryption Algorithm", ELSIVER publication, 2008.

[24] David Arroyo,Chengqing Li, Shujun Li, Gonzalo Alvarez, and Wolfgang A. Halang **"**Cryptanalysis Of An Image Encryption Scheme Based On A New Total Shuffling Algorithm", ELSIVER publication ,2008.

[25] Enes Pasalic **,"**Probabilistic Versus Deterministic Algebraic Cryptanalysis—A Performance Comparison", IEEE Transactions on information theory ,vol.55,no.11,2009.

[26] Chengqing Li, David Arroyo2 and Kwok-Tung Lo, **"**Breaking A Chaotic Cryptographic Scheme Based On Composition Maps", ELSIVER publication 2009.

[27] Huaqun Wang, Futai Zhang, and Yanfei Sun, "Cryptanalysis of a Generalized Ring Signature Scheme" IEEE Transactions on dependable and secure computing ,vol.6,no.2,2009.

[28] Vimalathithan and Dr.M.L.Valarmathi**,"**Cryptanalysis of simplified –DES Using Genetic algorithm", International Journal of Recent Trends in Engineering,vol.2,no.4,2009.

[29] Hadi Soleimany , Alireza Sharifi, Behnam Bahrak and Mohammadreza Aref**, "** Cryptanalysis of 7-Round AES-128",7th Iranian community conference,2009.

[30] Alex Biryukov and Dmitry Khovratovich," Related-key Cryptanalysis of the Full AES-192 and AES-256", SPRINGER publication,2009.

[31] Florian Mendel,Thomas Peyrin,Christian Rechberger, and Martin Schlaffer, "Improved Cryptanalysis of the Reduced Grostl Compression Function, ECHO Permutation and AES Block Cipher", SPRINGER publication ,2009.

[32] Chengqing Li,Shujun Li,and Kwok-Tung Lo. **"**Breaking A Modified Substitution-Diffusion Image Cipher Based On Chaotic Standard And Logistic Maps", Preprint submitted to Communications in Nonlinear Science and Numerical Simulation, 2009.

[33] Shuhua Wu et.al, "Cryptanalysis And Enhancements Of Three-Party Authenticated Key Exchange Protocol Using ECC" SPRINGER publication ,2011.

[34] Vimalathithan. R and M.L.Valarmathi,"Cryptanalysis of DES Using Computational Intelligence ",WSEAS Transactions on computers,Issue.7,vol.10,2011.

[35] Huaqun Wang and Yuqing Zhang,"Cryptanalysis of an Efficient Threshold Self-Healing Key Distribution Scheme", IEEE Transactions on wireless communications ,vol.10,no.1,2011.

[36] Youhua Shi,Nozomu Togawa,Masao Yanagisawa and Tatsuo Ohtsuki,**"**Robust Secure Scan Design Against Scan-Based Differential Cryptanalysis",IEEE vol.10,2012.

[37] Kyung-Ah Shim, **"**Cryptanalysis Of Two Identity-Based Authenticated Key Agreement Protocols", IEEE communication letters ,vol.16,no.4,2012.

[38] Rajashekharappa and Dr,K M S Soyjaudah," Heuristic Search Procedures for Cryptanalysis and Development of enhanced Cryptographic Techniques", IJMER vol.2,Issue.3,2012.

[39] Amish Kumar et.al **,"**Security Enhancement By Using Double S-Box",2012

[40] Sachin upadhyay,yashpal singh and Amit kumar jain," An analysis of the Attack on RSA Cryptosystem Through Formal Methods", IJSCE,vol.2,Issue.2,2012.

[41] Henri Gilbert and Thomas Peyrin,"Super-Sbox Cryptanalysis: Improved Attacks For AES-Like Permutations",IJRCSSE,2012.

[42] Vinod Saroha ,Suman Mor and Jyoti Mallik, "A review of various techniques of cryptanalysis", IJRCSE ,vol.2,Issue.10,2012.

[43] Shujun Li, Chengqing Li, Guanrong Chen and Kwok-Tung Lo, **"**Cryptanalysis Of RCES/RSES Image Encryption Scheme" ,IJSCE, 2012.

[44] Shujun Li, Chengqing Li, Kowk-Tung Lo, " Cryptanalysis of an Image Scrambling Scheme without Bandwidth Expansion" IEEE ,2012.

[45] Christopher Swenson," Modern Cryptanalysis Techniques For Advanced Code Breaking", wiley publication Inc.2008.

Ashish Kumar Kendhe, Persuing Master Of Engineering In Digital Communication From Sscet,Bhilai,Chhattisgarh , India.

Himani Agrawal, Woking As An Associate Professor In Electronics & Tele- Communication Department, Sscet, Bhilai,Chhattisgarh,India