AN OVERVIEW OF CRYPTANALYSIS ON AES

Km. Amrita[1],Neha Gupta[2],Rashmi Mishra[3]

[1]*Student, Department of Computer Science and Engineering, Buddha Institute of Technology, (India)*

[2]*Assistent Professor,Department of Computer Science and Engineering, Buddha Institute of Technology, (India)*

ABSTRACT

In this paper we give the overview of cryptanalysis.Cryptanalysis is the decryption and analysis of codes, ciphers or encrypted text. The field deals with the uncovering of encrypted messages without initial knowledge of the key used in the encryption process. It is use to break a single message, to recognize patterns in encrypted messages,to deduce the key, to find general weaknesses in an encryption algorithm. Advanced Encryption Standard (AES) (NITS FIPS-197) has been the subject of extensive cryptanalysis. This paper provides an overview of pre-existing and current cryptanalysis attacks on the AES cryptographic algorithm.Discussion is provided on the impact by each technique to the strength of the algorithm in national security applications.The paper is concluded with an attempt at a forecast of the usable life of AES in these applications.

Keywords-Advanced Encryption Standard; AES; Cryptanalysis; Side Channel Attacks.

I. INTRODUCTION

Cryptanalysis is the combination of two word cryptogram and analysis. Cryptogram means a communication in cipher (cypher) or code, a figure or representation having a hidden significance. And analysis means detailed examination of the elements.Advanced Encryption Standard (AES) is the current standard for secret key encryption.In 2003, the National Security Agency took the unprecedented step of approving a public-domain encryption algorithm, AES, for classified information processing. Prior to this milestone, all encryption algorithms approved by the NSA for classified processing were, themselves, classified. The strength of any good encryption algorithm is not enhanced by holding the design as secret. In fact, a public domain encryption standard is subject to continuous, vigilant, expert cryptanalysis. Any breakthroughs will very likely be available to users as well as their adversaries at the same time.

In consumer applications, this isn't as much of a problem, but in military communication applications it can be disastrous. Here, the adversary can have national intelligence agency level resources and can exploitVulnerabilities as soon as they are identified. If practical vulnerabilities are found, there will be a period of reduced confidence until a new algorithm can be installed.

I.I. Cryptanalysis

Cryptanalysis is the study of cipher text, ciphers and cryptosystems in order to study the hidden aspects of the systems.[1] Cryptanalysis is used to break cryptographic security systems and gain access to the contents of encrypted messages, even if the cryptographic key is known. Cryptanalysis is the decryption and analysis of codes, ciphers or encrypted text. A cipher (cypher) is an algorithm for performing encryption or decryption.

Cryptography is a technique of transforming and transmitting confidential data in an encoded way so that only authorized and intended users can obtain or work on it. It is a Greekorigin word in which "crypto" means hidden and “graphy” means writing [2], so cryptography means hidden or secret writing. It introduces triads like confidentiality, non-repudiation, integrity and authenticity within ongoing data communication.

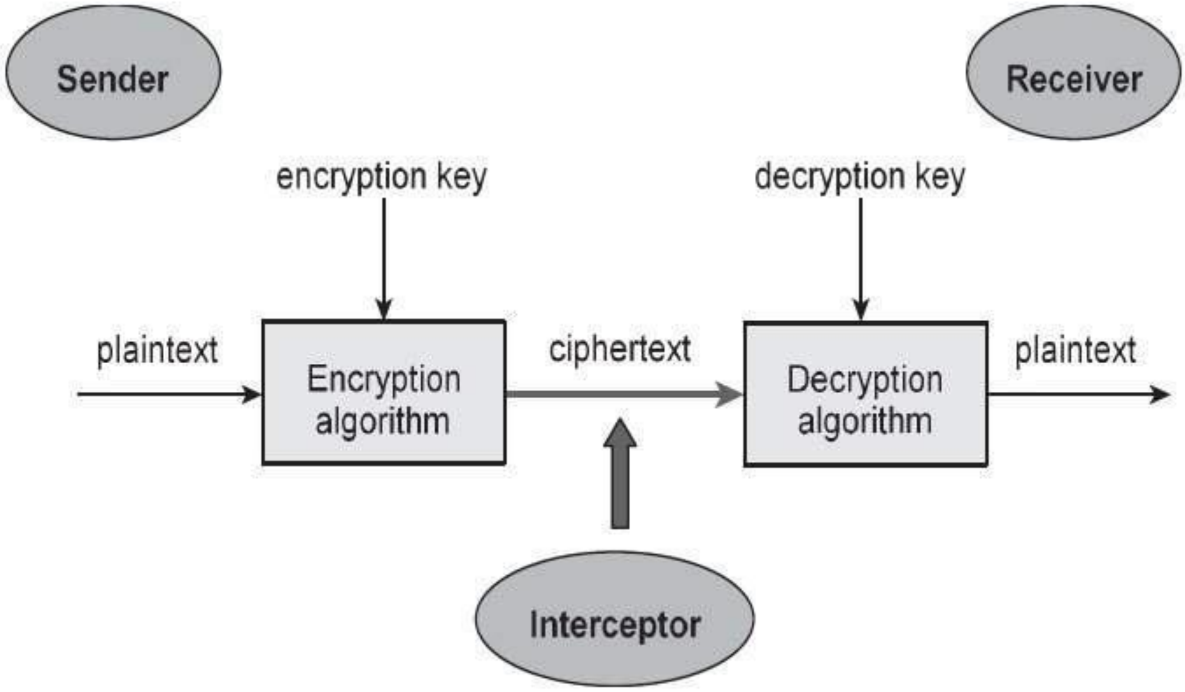

Fig 1:- Cryptographic System

Cryptanalysis is the opposite of cryptography. The field deals with the uncovering of encrypted messages without initial knowledge of the key used in the encryption process. It is the process of defeating the work of cryptography. Cryptanalyst inspect the security of crypto primitive.

I.II. Advanced Encryption Standard (AES)

On January 2, 1997 the National Institute of Standards and Technology (NIST) held a contest for a new encryption standard. The previous standard, DES, was no longer adequate for security. It had been the standard since November 23, 1976. Computing power had increased a lot since then and the algorithmwas no longer considered safe. In 1998 DES was cracked in less than three days by a specially made computer called the DES cracker.[29]Current alternatives to a new encryption standard were Triple DES (3DES) and International Data Encryption Algorithm (IDEA). The problem was IDEA and 3DES were too slow and IDEA was not free to implement due to patents. NIST wanted a free and easy to implement algorithm that would provide good security. Additionally they wanted the algorithm to be efficient and flexible.[30]

After holding the contest for three years, NIST chose an algorithm created by two Belgian cryptographers, Vincent Rijmen and Joan Daemen. The incorporated Information Processing Standard 197 used a standardized version of the algorithm called Rijndael for the Advanced Encryption Standard. The algorithm uses a combination of Exclusive-OR operations (XOR), octet substitution with an S-box, and a MixColumn,row and column rotations. It was successful because it was easy to implement and could run in areasonable amount of time on a regular computer.[30]

Before applying the algorithm to the data, the block and key sizes must be determined. AES allows for block sizes of 128, 168, 192, 224, and 256 bits. AES allows key sizes of 128, 192, and 256 bits.[30] The standard encryption uses AES-128 where both the block and key size are 128 bits. The block size is commonly denoted as N_b and the key size is commonly denoted as N_k. $N_b$refers to the number of columns in the block where each row in the column consists of four cells of 8 bytes each for AES-128[31].

II.CRYPTANALYSIS ATTACKS ON AES

II.I. Pre-existing Attacks

Two main pre-existing attacks on block cipher are linear and differential cryptanalysis attack.

This section briefly explains about these two attacks and other pre-existing attacks.

1. Linear Cryptanalysis Attack

Linear cryptanalysis was discovered by Mitsuru Matsui.Linear cryptanalysis is based on finding affine approximations to the action of a cipher.It tries to take advantage of high probability linear relationship that exist between inputs and outputs of a function block.In the case of a block cipher, linear combinations of plain text pattern and linear combinations of ciphertext patterns are compared to linear combinations of key bits.[4] the goal of linear cryptanalysis is to discover a relationship that is valid either significantly more or less than 50% of the time.[5]In many applications and scenarios it is reasonable to assume that the attacker has knowledge of a random set of plaintexts and the corresponding ciphertexts. Then apply plaintext patterns, retrieve the resulting cipher text patterns and linearly combine them (in a mod-2 sense) according to the approximation.The result of this operation will be, with some probability, a linear combination of key bits. The remaining key bits are found by exhaustive enumeration.

2. DifferentialCryptanalysis Attack

Differential cryptanalysis exploits relationships that exist between differences in the input and output of a function block.[5] In the case of an encryption algorithm, plaintext patterns with fixed differences are examined. The goal is to discover “characteristics”. Characteristics are specific differences in pairs of plaintext patterns that, for a given key, have a high probability of causing specific differences in the ciphertext pairs. A differential attack would consist of applying pairs of plaintext pairs and assigning probabilities to different candidate subkeys. The probabilities will be based on the cryptanalyst’s knowledge of the algorithm’s characteristics.Enough trails are run such that the correct key can be determined.

3. The Boomerang Attack

The boomerang attack introduced by Wagner[6] can be seenas an upgrade of classical differential cryptanalysis operating on quadruples of data instead of pairs with fixed difference. Quadruples of plaintexts are properly chosen, and observed together with corresponding quadruples of ciphertexts and intermediate states. Wagner showed how to apply this attack to some of the lesser known block cipher. In 2005, Biryukov[7] claimed that boomerang attacks on 5 and 6 rounds of AES are much faster than the exhaustive key search and twice as fast as original Square attack by the designers of the AES. We could not find any more recent work on boomerang attacks on AES.

4. Truncated Differentials, the Square Attack and Interpolation Attacks

Truncated differentials are a generalization of differential cryptanalysis where partially determined differentials are considered [8]. These partial differentials often cluster into pools of difference pairs. This property can yield statistics that significantly reduce the complexity for a successful attack. The Square attack is a generalization of an attack originally proposed against the Square Block Cipher [9]. For this attack, a “multiset” of plaintexts is carefully chosen to have certain properties. This multiset is applied to the algorithm and the propagation of these multisets is then examined through the various rounds. The persistence of these properties gives insight to the statistical behaviour of the algorithm which can be used to reveal bits of key. For interpolation attacks, the cipher is modeled using a high order polynomial [10]. Then the polynomial is solved for the key-dependent coefficients. The technique is very effective when a compact expression of low degree describing the cipher is possible.

4.1 Security Summary

The tenets of differential cryptanalysis, linear cryptanalysis, truncated differentials, the Square attack and interpolation attacks matured prior to the design of AES.In [11], the authors of AES establish the conditions that for a cipher to be secure against differential cryptanalysis that there are no differential trails with a predicted propagation ratio higher than 2^{1-n} and to be secure against linear cryptanalysis there are no linear trails with a correlation coefficient higher than $2^{n/2}$. They then proceed to show that AES meets these conditions with 8 rounds or greater and is, therefore, provably secure against both of these techniques. Further, AES is secure against truncated differentials with 6 rounds or more, is secure against the Square attack for 7 rounds or more and is secure, by design, against interpolation attacks.

III. CURRENT ATTACKS

1. Algebraic Attacks

Algebraic attacks were first introduced in 2002 in [12]. For these attacks, AES is expressed as a system of multivariate polynomial equations over a single Galois field. Efficiently solving this system of equations to recover the key variable is the objective of the attack. A very attractive feature of most algebraic attacks is that they require only a single, or a very small number of plaintext/ciphertext pairs, where encryption used the unknown key. This is in stark contrast to, say, classical linear attacks on DES, which perhaps are computationally manageable, but unfortunately they require a very unrealistic number of such pairs, namely about 240. On the other hand, the algebraic attack would be dangerous only if the set of equations defined by the cipher and unknown key is realistically solvable for sizes of several thousand variables and equations. There is no convincing evidence that such computations are feasible, while the difficulty of handling much smaller cases is notorious.

2. XL and XSL Attacks

In 1999, Kipnis and Shamir [13] were perhaps the first to attract attention of several researchers to the following general strategy: given a system of multivariate polynomials describing relationships between variables, i/o and keys of some cryptographic function, first try to express it as a single univariate polynomial of a special form over an extension field, and then use it to reduce the original cryptanalytic problem to a system of quadratic equations over the extension field. Such systems might be attacked using relinearizationmethods which are easier to handle, but require a larger number of variables.

This was extended in 2000 by Courtois, Klimov, Patarin and Shamir [14] to an approach potentially usable in the attacks on AES, which was called the XL (eXtended Linearization) algorithm. It is a method of solving systems of multivariate quadratic equations via linearization. This has been followed by an improvement of the XL algorithm called XSL (eXtended Sparse Linearization) by Courtois and Pieprzyk in 2002 [14]. The authors of XSL aimed at exploiting two properties of large systems of equations obtained from cryptanalysis: the systems are very sparse and they are overdefined. There were several further papers proposing more improvements to these algorithms, but also many papers and theses essentiallyimplying that these attacks, as intended, are unworkable.

3. Cube Attacks

Cube attacks rely on the ability to determine a low-order polynomial description of the output of the cipher. Then a clever iterative approach is used to solve the expression to find bits of key. This attack is most effective on stream ciphers with an LFSR structure [15]. AES and DES are believed to be immune to the attack primarily because an algebraic polynomial that could describe any good block cipher would be of too high a degree to allow this attack to be any more practical than a brute force search of the key space [16].

4. Side Channel Attacks

A side-channel attack exploits information leaked from a cryptosystem due to vulnerabilities in its physical 4 of 8 implementation rather than any cryptographic vulnerabilities of the algorithm. Information gained from observable parameters such as variations in timing, power consumption,electromagnetic radiation, thermal emanations or acoustic emanations can sometimes be used to determine sensitive data, such as bits of plaintext or a key variable.

Some examples of these methods are: timing attacks, differential power analysis attacks, simple power analysis attacks and fault injection based attacks. Timing analysis exploits relationships between the run-time of functions within a cryptographic device and sensitive data elements that are being processed. Changes in execution times of these functions are used together with a model of the system to determine bits of sensitive data. Although they are sometimes limited by the need for precise measurements, timing attacks can be particularly powerful because they are non-invasive and can be applied remotely [17]. Differential Power Analysis (DPA) enables the security of cryptographic devices to be compromised by analyzing their power consumption. Simple Power Analysis (SPA) is a simpler form of the attack that does not require statistical analysis [28] [29]. Fault injection based attacks exploit computational errors to find cryptographic keys [20] [21]. Computational errors are introduced into a cryptographic device by exposing the device to some physical effect such as electromagnetic radiation, excessive temperature or by applying inputs that exceed the device's specifications (clock rate, input levels, input timing, etc.). Miscomputed results, together with a fault model, are used to extract secret data. Some other examples of side-channel attacks include acoustic attacks and electromagnetic emanation analysis [22] [23].

5. Related-Key and Distinguishing Attacks

A related-key attack on a block cipher is a variant of a chosenplaintext differential attack. The attacker chooses multiple pairs of plaintexts, where the difference between the plaintextsin each pair is specified. Using the cipher as a black box oracle, the attacker encrypts each plaintext with two keys, where the difference between the keys is specified (but the keys themselves are unknown); these are the "related" keys forwhich the attack is named. From the information derived, the attacker recovers the unknown keys. Although related keys are unlikely when a block cipher is used for encryption, related keys are common when a block cipher is used as part of a cryptographic hash function. A successful related-key attack may then break the hash function.

In 2009, Biryukov et al. [24] published related-key attacks on full-strengthAES-192 and AES-256. The attacks recover the key with 2^{176} work for AES-192 and 2^{119}work for AES-256. Since these attacks take less time than brute force, AES-192 and AES-256 are theoretically broken; but the attacks take toolong to be practical. However, Biryukov et al. [25] also published related-key attacks on *reduced-round* variants of AES-256 that *are* practical -- 2^{39}work for 9-round AES-256, 245 work for 10-round AES-256. Ironically, these attacks donot succeed for AES-128, which with its shorter key is supposedly weaker than AES-192 and AES-256.

A distinguishing attack allows the attacker to detect non-randomness in the block cipher technically; the attacker can distinguish the block cipher's behaviour from that of an ideal random cipher. Since the security of cryptographic constructions, notably hash functions, built from block ciphers is typically proven assuming the block cipher is an ideal random cipher, a distinguishing attack on the block cipher calls into question the security of the construction.

Biryukov et al. [26], [27] have published a related-key distinguishing attack on AES-256 requiring 2^{120}time. They parlayed the distinguishing attack into a key recovery attack requiring 2^{65} memory and 2^{131} time. Like their previousattacks, this attack theoretically breaks full-strength AES-256 but is not practical. Gilbert and Peyrin [28] have published a known-key distinguishing attack on AES-128 reduced from 10 rounds to 8 rounds; the attack requires 2^{32} memory and 2^{48}time. This attack is practical and breaks a nearly-full-strengthvariant of AES.

IV.CONCLUSION

This paper presented the results of a study on the current progress of cryptanalysis research on the Advanced Encryption Standard (AES).

It was determined that cryptanalysis research is making progress against AES. Further, caution is recommended because that progress is happening in the public domain. Results show that AES is currently vulnerable to various side channel attacks. However, appropriate countermeasures are available which, when properly implemented, can eliminate these vulnerabilities at the equipment level. Other methods such as algebraic attacks, hybrid attacks, etc., are making steady progress, but no breakthroughs have been reported. With these, the trends indicate that AES won't have the life expectancy of the traditional algorithm suite approved for classified applications. This makes AES an inappropriate option for classified strategic applications. However, modern secure tactical communications equipment employs programmable cryptography. In the event of a public domain breakthrough, a new algorithm could be fielded relatively quickly. The period of vulnerability will be more defined by practical logistic issues rather than technical issues. Advance planning is required to prepare for this inevitable event.

REFERENCES

[1] **.**Cryptanalysis/Singles Analysis Nsa.gov.2009-01-15. Retrieved 2013-04-15.

[2]. Anjula Gupta and Navpreet Kaur Walia, “Cryptography Algorithms: A Review”, International Journal ofEngineering Development and Research, ISSN: 2321- 9939, Volume 2, Issue 2, pg.no-1667-1672.

[3]. M. Matsui, “Linear Cryptanalysis Method for DES Cipher”. EUROCRYPT, LNCS 765, pp.386-397, Springer, 1994.

[4]. Ben-Aroya, E. Biham, "Differential Cryptanalysis of Lucifer", CRYPTO. Journal of Cryptology, pp.187-199, Springer, 1994.

[5]. Ben-Aroya, E. Biham, "Differential Cryptanalysis of Lucifer", CRYPTO. Journal of Cryptology, pp.187-199, Springer, 1994.

[6]. D. Wagner, “The Boomerang Attack, Fast Software Encryption”, 6th International Workshop on Fast Software Encryption, LNCS 1636, Springer,1999.

[7]. A. Biryukov, “The Boomerang Attack on 5 and 6-Round Reduced AES”, LNCS 3373, pp.11-15, Springer, 2005.

[8] J. Daemen, L. Knudsen, V. Rijmen, "The Block Cipher Square", 4th International Workshop on Fast Software Encryption, LNCS 1267, pp. 149–165, Springer, 1997.

[9] T. Jakobsen, L. Knudsen "The Interpolation Attack on Block Ciphers", 4th International Workshop on Fast Software Encryption, LNCS 1267, pp.28–40,Springer, 1997.

[10]. J. Daemen, V. Rijmen, “AES Proposal: Rijndael, Version 2”, http://www.esat.kuleuven.ac.be/vijmen/rijndael, 1999.

[11]. J. Daemen, V. Rijmen, “AES Proposal: Rijndael, Version 2”,http://www.esat.kuleuven.ac.be/vijmen/rijndael, 1999.

[12]. N. Courtois, J. Pieprzyk, "Cryptanalysis of Block Ciphers with Overdefined Systems of Equations", ASIACRYPT, LNCS 2501, pp.267-287,Springer, 2002.

[13]. A. Kipnis, A. Shamir, "Cryptanalysis of the HFE Public Key. Cryptosystem by Relinearization", CRYPTO, LNCS 1666, pp.19-30, Springer, 1999.

[14]. N. Courtois, A. Klimov, J. Patarin, A. Shamir, "Efficient Algorithms for Solving Over defined Systems of Multivariate Polynomial Equations",EUROCRYPT, LNCS 1807, pp.392-407, Springer, 2000.

[15]. I. Dinur, A. Shamir, "Cube Attacks on Tweakable Black Box. Polynomials", EUROCRYPT, LNCS 5479, pp. 278-299, Springer, 2009.

[16]. B. Schneier, "Adi Shamir's Cube Attacks". http://www.schneier.com/blog/archives/2008/08/adi_shamirs_cub.html,

[17]. August 19, 2008. P. Kocher, "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems", CRYPTO, LNCS 1109, pp.104-113, Springer,1996.

[18]. P. Kocher, J. Jaffe, B. Jun, "Introduction to Differential Power Analysis and Related Attacks", Tech. Rep., Cryptography Research Inc, 1998.

[19]. P. Kocher, J. Jaffe, B. Jun, "Differential Power Analysis", CRYPTO,LNCS 1666, pp.388-397, Springer, 1999.

[20]. D. Boneh, R. A. DeMillo, R. J. Lipton, "On the Importance of Checking Computations", EUROCRYPT, LNCS 1233, pp.37-51, Springer, 1997.

[21]. E. Biham, A.Shamir, "Differential Fault Analysis of Secret Key Cryptosystems", CS 0910, CRYPTO, LNCS 1294, pp. 513 – 525, Springer,1997.

[22] D. Asonov, R. Agrawal, "Keyboard Acoustic Emanations", IEEE Symposium on Security and Privacy, Oakland, CA, pp.3-11, 2004.

[23] J.J. Quisquater, D. Samyde, "ElectroMagnetic Analysis (EMA): Measures and Counter-Measures for Smart Cards", Proceedings of the International Conference on Research in Smart Cards: Smart Card Programming and Security, pp.200–210, 2001.

[24] A. Biryukov, D. Khovratovich, "Related-key Cryptanalysis of the FullAES-192 and AES-256", ASIACRYPT, LNCS 5912, pp.1-18, Springer, 2009

[25] A. Biryukov, O. Dunkelman, N. Keller, D. Khovratovich, A. Shamir,"Key Recovery Attacks of Practical Complexity on AES Variants with up to10 Rounds", EUROCRYPT, Springer, 2010.https://www.cryptolux.org/mediawiki/uploads/3/38/Fast_attack_on_reduced_AES-256.pdf, 2009.

[26] A. Biryukov, D. Khovratovich, I. Nikolić, "Distinguisher and Related-Key Attack on the Full AES-256", CRYPTO, LNCS 5677, pp.231-249,Springer, 2009.

[27] A. Biryukov, D. Khovratovich, I. Nikolić, "Examples of DifferentialMulti-collisions for 13 and 14 Rounds of AES-256",https://www.cryptolux.org/mediawiki/uploads/f/f2/AES 256_nonrandomness_examples.pdf, 2009.

[28] H. Gilbert, T. Peyrin, "Super-Sbox Cryptanalysis, Improved Attacks for AES-like Permutations", Cryptology Print Archive Report 2009/531, November 2, 2009. http://eprint.iacr.org/2009/531.pdf.

[29] DES Encryption. Tropical Software. 2010. http://www.tropsoft.com/strongenc/des.htm (accessed March, 15, 2010).

[30] Kaufman, C., Perlman, R., and Speciner, M. *Network Security: Private Communication in a Public World*. 2nd ed. Upper Saddle River, N.J.: Prentice Hall PTR, 2002.

[31] Daemen, J., and Rijmen, V. *AES Proposal: Rijndael*. September 3, 1999. http://www.comms.scitech.sussex.ac.uk/fft/crypto/rijndael.pdf (accessed March, 15, 2010).