Analysis In Symmetric And Asymmetric Cryptology Algorithm

Harsh Mathur[1], Prof.Zahid Alam[2]

[1]Scholar in Mtech in LNCT, RGPV University,
Bhopal, M.P. INDIA

[2]Associate professor in LNCT, RGPV University
Bhopal, M.P. INDIA

Abstract

This paper will present a peer analysis in the field of encryption algorithms, in concentrating on private key block ciphers which are generally used for bulk data and link encryption. we have initially survey some of the more popular and efficient algorithms currently in use. This paper focuses mainly on the different kinds of encryption techniques that are existing, and comparative study all the techniques together as a literature survey. Aim an extensive experimental study of implementations of various available encryption techniques. Also focuses on image encryption techniques, information encryption techniques. This study extends to the performance parameters used in encryption processes and analyzing on their security issues

Keywords:-encryption, block cipher, analyzing.

1. INTRODUCTION

1.1 Cryptography

Cryptography is the science that studies the mathematical techniques for keeping message secure and free from attacks [1] .Cryptography system can be classified into two parts first is Symmetric key Cryptography and second is public key cryptography.

Symmetric key cryptography:

In symmetric key cryptography system sender and receiver share a single key which is used to encrypt and decrypt a message. It is also called secret key cryptography. The algorithms used for symmetric key cryptography is called symmetric- key algorithms.

There are two types of symmetric algorithms such as stream cipher and block cipher. Stream ciphers encrypt the bits of information one at a time and Block ciphers encrypt the information by breaking down into blocks. [1]

List of Symmetric Algorithms

1. Data Encryption Standard(DES)
2. Advanced Encryption Standard (AES)
3. Blowfish Encryption Algorithm
4. International Data Encryption Algorithm
5. Triple Data Encryption Standard etc.

Public key cryptography:

In public key cryptography there is pair of keys one is secret key and other is public key. In which one is used for encrypting the plain text, and the other is used for decrypting the cipher text [1].

List of public key algorithms

1. Diffie-Hellman
2. RSA
3. DSA etc.

The Goal of Cryptography is about concealing the content of the message. At the same time encrypted data package is itself evidence of the existence of valuable information. [3] This paper holds some of those recent existing encryption techniques and their security issues. The performance of all those encryption techniques are studied in chapters of the paper.

2. International Data Encryption algorithm (IDEA).

International Data Encryption algorithm (IDEA) is a block cipher algorithm designed by Xuejia Lai and James L. Massey of ETH-Zürich and was first described in 1991.The original algorithm went through few modifications and finally named as International Data Encryption Algorithm (IDEA). The mentioned algorithm works on 64-bit plain text and cipher text block (at one time). Forencryption, the 64-bit plain text is divided into four 16 bits sub-blocks. In our discussion, we denote these four blocks as P1 (16 bits), P2 (16 bits), P3 (16 bits) and P4 (16 bits). Each of these blocks goes through 8 rounds and one output transformation phase. In each of these Eight rounds, some (arithmetic and logical) operations are performed. Throughout the eight rounds, the same sequences of operations are repeated. In the last phase, i.e., the output transformation phase, we perform only arithmetic operations. At the beginning of the encryption process, the 64 bit plain text is divided in four equal size blocks and ready for round1 input. The output of round1 is the input of round2. Similarly, the output of round2 is the input of round3, and so on. Finally, the output of round8 is the input for output transformation, whose output is the resultant 64 bit cipher text (assumed as C1 (16bits), C2 (16 bits), C3 (16 bits) and C4 (16 bits)). As the IDEA is a symmetric key algorithm, it uses the same key for encryption and for decryption. The decryption process is the same as the encryption process except that the sub keys are derived using a different algorithm [6]. The size of the cipher key is 128bits. In the entire encryption process we use total 52 keys (round1 to round8 and output transformation phase); generated from a 128 bit cipher key. In each round (round1 to round8) we use six sub keys. Each sub-key consists of 16bits. And the output transformation uses 4 sub-keys.

3. Observations on RSA Algorithm

The RSA encryption/decryption algorithms are a type of public key cryptography namedfor Ron Rivest, Adi Shamir and Leonard Adleman, who first presented the algorithmin 1977. Encryption and decryption are both very simple: If Alice is sending a secretmessage m to Bob, he tells her his public key, which consists of two values, e and n. Alicethen sends to Bob the ciphertext message $c = m^e$ mod n. He decodes it using his privatekey, d, computing $m = c^d$ mod n to get Alice's original message back. The eavesdropperEve cannot decode it because she does not have Bob's private key. However, she couldfigure out d if she could factor n, so the algorithm's security relies on generating verylarge prime numbers that are difficult to factor. We now show why Bob's decryption procedure reveals the message m. If $c = m^e$ mod n

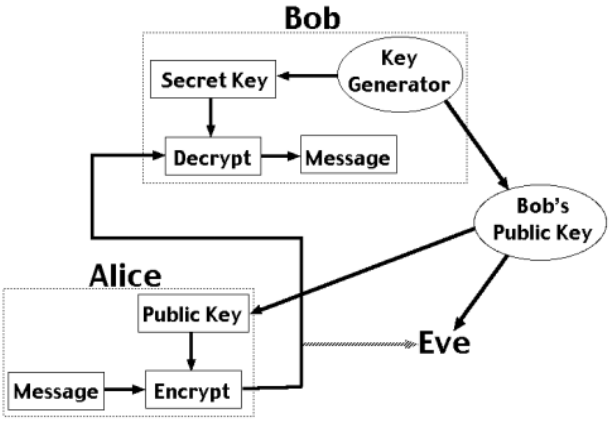
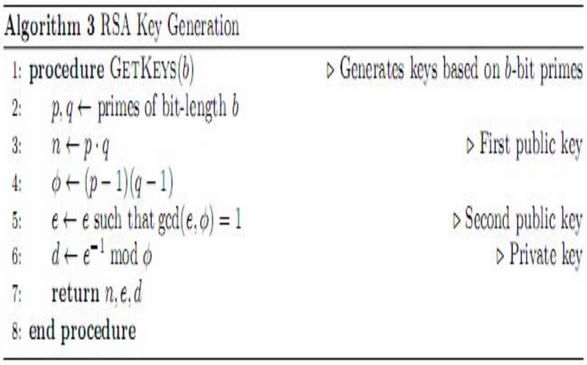


figure : An overview of RSA


Algorithm 3 RSA Key Generation

```
procedure GetKeys(b)                          ▷ Generates keys based on b-bit primes
    $p, q \leftarrow$ primes of bit-length $b$
    $n \leftarrow p \cdot q$                  ▷ First public key
    $\phi \leftarrow (p-1)(q-1)$
    $e \leftarrow e$ such that $\gcd(e, \phi) = 1$    ▷ Second public key
    $d \leftarrow e^{-1} \bmod \phi$           ▷ Private key
    return $n, e, d$
end procedure
```

An Analysis of RSA

After surveying the previous four types of cryptographic algorithms, we decided to focus on one algorithm in particular: RSA. We began by analyzing its algorithmic complexity, which we express using Big-O notation. Big-O notation is used to classify algorithm runtimes by their dominant parts. Coefficients and polynomial terms of lesser degree are often dropped when using Big-O notation. For example, if an algorithm executes a loop of length *n* three times, instead of describing it as having a runtime of length *3n*, we would say it runs in *O(n)* time, or linear time. If an algorithm can be described as having a runtime of n^3 + *2n2*, we would say it runs in *O(n3)* or cubic time. The two main groups of algorithm runtimesare polynomial and exponential. Exponential-time algorithms are considered impractical, since they run extremely slowly on largeinputs, while polynomial-time algorithms scale better.

4. Advanced Encryption Standard (AES) / Rijndael

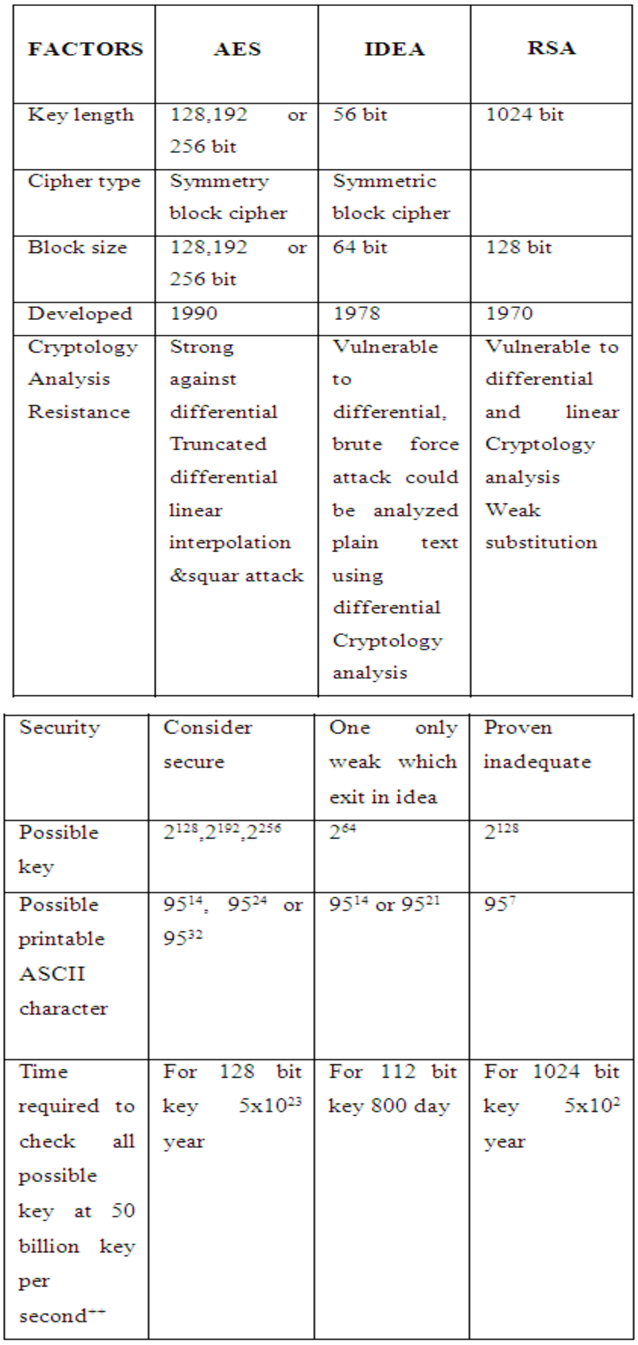
The Rijndael (pronounced "rhine-doll") algorithm, destined to become the new Advanced Encryption Standard. Rijndael mixes up the SPN model by including Galios field operations in each round. Quit similar to RSA modulo arithmetic operations, the Galios field operations produce apparent gibberish, but can be mathematically inverted.AES have Security is not an absolute; it's a relation between time and cost. Any question about the security of encryption should be posed in terms of how long time, and how high cost will it take an attacker to find a key? The AES algorithm is an repetitive private key symmetric block cipher that can process data block of 128-bits through the use of cipher keys with key length 128,192 and 256 bits. Optimized and synthesizable VHDL code is developed for implementation of all AES-128/192/256 bit key encryption. Thus it can reduce the space by enclosing different encryption standards in a single architecture and the power consumption can also be reduced which makes it usable in battery operated network devices having Bluetooth and wireless communication devices like software radio

5. Comparison Between AES, RSA AND IDEA.

Advance Encryption Standard (AES), RAS and IDEA are commonly used block ciphers. Whether you choose AES, RSA or IDEA depend on your needs. In this paperwee would like to focus their differences in terms of security and performance IDEA was developed in 1977 and it was designed to work better . IDEA performs lots of bit manipulation in each of 16 rounds. Even though it seems large but according to resent computing power it is not sufficient and appropriate to handel force attack. Therefore, IDEA could not good enough with advancement in technology and it is not in used for security. Because IDEA was widely used inpreviouscryptology , the quick solution was to introduce RSA is widely used in electronic online money transfer industry. RSA takes thrice much CPU power than comparing with its predecessor which is significant performance hit. AES outperforms IDEA both in software and in hardware [12], [13].

- Security
- Software & Hardware performance
- Suitability in restricted-space environments
- Resistance to power analysis and other
- Implementation attacks.

The experimental results of many papers showedthat AES has better performance and efficiency than all other block ciphers. The next technique that is widely used toprotect our information is AES. I have read many papers on Cryptography that mainly used AES algorithm for information security. AES is the most secure & widely used by researchers. AES can be used with many techniques like AES& DES, RSA &AES, RSA & Diffie Hellman, RSA & IDEA , AES& Blowfish, RSA & Two fish by combining cryptography algorithms to improve security. I have studied many papers on cryptography. Some papers were very good and effective and can be used for future work . This paper provides beginners to work in this field. If the beginners read this paper, then they have not to read the all papers completely. They just go to read this review paper and may get many ideas for their work. Of course other tools provide a best information security but its importance can't be ignored



FACTORS	AES	IDEA	RSA
Key length	128,192 or 256 bit	56 bit	1024 bit
Cipher type	Symmetry block cipher	Symmetric block cipher	
Block size	128,192 or 256 bit	64 bit	128 bit
Developed	1990	1978	1970
Cryptology Analysis Resistance	Strong against differential Truncated differential linear interpolation &squar attack	Vulnerable to differential, brute force attack could be analyzed plain text using differential Cryptology analysis	Vulnerable to differential and linear Cryptology analysis Weak substitution
Security	Consider secure	One only weak which exit in idea	Proven inadequate
Possible key	2^{128},2^{192},2^{256}	2^{64}	2^{128}
Possible printable ASCII character	95^{14}, 95^{24} or 95^{32}	95^{14} or 95^{21}	95^{7}
Time required to check all possible key at 50 billion key per second^{++}	For 128 bit key 5x10^{23} year	For 112 bit key 800 day	For 1024 bit key 5x10^{2} year

6.CONCLUSION

Comparative study between IDEA, RSA and AES are carried out in to nine factors, Which are key length, cipher type, block size, developed, Cryptology analysis resistance, security, possibility key, possible ACSII printable character keys, time required to check all possible key at 50 billion second, these factors's proved the AES is better than IDEA and RSA. an important application-oriented problem concerning the data security, has been presented. The author hopes that this work may have some influence on the future standardization policy in encryption and decryption.

References

[1] A. Bonnaccorsi, "On the Relationship between Firm Size and Export Intensity," Journal of International Business Studies, XXIII (4), pp. 605-635, 1992. (journal style)

[2] R. Caves, Multinational Enterprise and Economic Analysis, Cambridge University Press, Cambridge, 1982. (book style)M. Clerc, "The Swarm and the Queen: Towards a Deterministic and Adaptive Particle Swarm Optimization," In Proceedings of the IEEE Congress on

[3] Evolutionary Computation (CEC), pp. 1951-1957, 1999. (conference style)

[4] H.H. Crokell, "Specialization and International Competitiveness," in Managing the Multinational Subsidiary, H. Etemad and L. S, Sulude (eds.), Croom-Helm, London, 1986. (book chapter style)

[5] K. Deb, S. Agrawal, A. Pratab, T. Meyarivan,"A Fast Elitist Non-dominated Sorting Genetic Algorithms for Multiobjective Optimization: NSGA II," KanGAL report 200001, Indian Institute of Technology, Kanpur, India, 2000. (technical report style)

[6] J. Geralds, "Sega EndsProduction of Dreamcast," vnunet.com, para. 2, Jan. 31, 2001. [Online]. Available: http://nl1.vnunet.com/news/1116995. [Accessed: Sept. 12, 2004].(General Internet site)