Modern Cryptographic Technique – A Literature Review

Gunjan Sahni1 Gajendra Singh2
1M. Tech (IT) Student, 2H.O.D. (Comp. & IT Dept.)
1,2SSSIST, Sehore, India

Abstract--- In this paper, we are presenting a survey of some modern and popular cryptography techniques. The working of popular encryption and decryption methods is also discussed in brief. The advantages and drawbacks of some commonly used is also discussed in brief.

Keywords: AES, Blowfish, Cryptography, DES, RC4.

I. INTRODUCTION

Today information is one of the most valuable intangible assets. Due to this fact, information security had become an important issue. Cryptography is one of the methods used to protect data from unauthorized access and being stolen. There are two types of cryptosystem, which are symmetric cryptosystem and asymmetric cryptosystem. In Symmetric cryptosystem, the sender and recipient share the same key. It means the same key is used for encryption and decryption. In Asymmetric cryptosystem, different keys are used. A public key is used by sender to encrypt the message while the recipient used a private key to decrypt it. Both of these cryptosystem have their own pros and cons. For instance, Symmetric cryptosystem consume less computing power but it is less secure than Asymmetric cryptosystem. Currently, there are a few cryptosystem which are widely implemented such as Advanced Encryption Standard (AES), Blowfish, River Cipher 4 (RC4) and Data Encryption Standard (DES). However, these modern cryptosystem have their origins. The classical cipher such as Caesar Cipher, Hill Cipher, Vigenère Cipher act as the foundation of the cryptology’s world today.

Cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication. Cryptography is not the only means of providing information security, but rather one set of techniques.

A. Security Services:

The security services include:

1) Data Confidentiality
2) Data Integrity
3) Authentication
4) Non repudiation
5) Access Control

Cryptographic systems are generally classified along three independent dimensions:

1) Type of operations used for transforming plaintext to cipher text. All encryption algorithms are based on two general principles. Those are substitution, in which each element in the plain text is mapped into another element and transposition in which elements in the plaintext are rearranged. The fundamental requirement is that no information be lost. Most systems referred to as product systems, involved multiple stages of substitution and transposition.

2) The number of keys used: If sender and receiver use the same key, the system is referred to as symmetric, single key or secret key conventional encryption. If the sender and the receiver each uses a different key the system is referred to as asymmetric, two key, or public-key encryption.

3) The way in which the plaintext is processed: A block cipher processes the input on block of elements at a time, producing an output block for each input block. A stream cipher processes the input elements continuously, producing output one element at a time, as it goes along.

II. LITERATURE SURVEY

The ElGamal system [1] is a public-key cryptosystem based on the discrete logarithm problem. It consists of both encryption and signature algorithms. The encryption algorithm is similar in nature to the Diffie-Hellman key agreement protocol. The system parameters consist of a prime p and an integer g, whose powers modulo p generate a large number of elements, as in Diffie-Hellman. Alice has a private key a and a public key y, where y = ga (mod p). Suppose Bob wishes to send a message m to Alice. Bob first generates a random number k less than p. He then computes

y1 = gk (mod p) and y2 = m xor yk.

Where xor denotes the bit-wise exclusive-or. Bob sends (y1, y2) to Alice. Upon receiving the ciphertext, Alice computes m = (y1a mod p) xor y2.

The ElGamal signature algorithm is similar to the encryption algorithm in that the public key and private key have the same form; however, encryption is not the same as signature verification, nor is decryption the same as signature creation as in RSA. DSA is based in part on the ElGamal signature algorithm. Analysis based on the best available algorithms for both factoring and discrete logarithms shows that RSA and ElGamal have similar security for equivalent key lengths. The main disadvantage of ElGamal is the need for randomness, and its slower speed (especially for signing ). Another potential disadvantage of the ElGamal system is that message expansion by a factor of two takes place during encryption. However, such message expansion is negligible if the cryptosystem is used only for exchange of secret keys. The DES and 3DES are known to have worm holes in their...
security mechanism; the Blowfish and AES do not have any so far [6].
Authors [7] performed the performance comparison for variable sized text files as input. The analysis on computational running times results in significant difference among the methods. He believe in that the performance of DES is good especially in decryption method is very high than the alternatives.
Authors [9] have evaluated the performance of RC4 and AES encryption algorithms. Their performance metrics were encryption throughput and CPU work. The tradeoffs with security are not completely clear in [9].
The Comparative Analysis of AES and RC4 Algorithms for Better Utilization have designed by Nidhi Singhal in the year (2011). In the AES, CFB and CBC takes nearly similar time but ECB takes less time then both of these[10].
The Comparative Study of Two Symmetric Encryption Algorithms across Different Platforms designed by S.A.M Rizvi1 there is no significant difference in performance of CAST and AES. The BLOWFISH encrypts audio files at less speed for audio files [12].
The throughput analysis of selected algorithms are AES, 3DES, Blowfish and DES. The results presented show the numerous points. First of all it was concluded that Blowfish has better performance than other algorithms followed by AES in terms of throughput. Then secondly 3DES has least efficient of all the studied algorithms [15].
The experimental result [17] shown that RSA consume longest encryption time and memory usage is also very high but output byte is least in case of RSA algorithm [17].

III. PROBLEM IN ELGAMAL SYSTEM

- The main disadvantage of ElGamal is the need for randomness, and its slower speed (especially for signing).
- Another potential disadvantage of the ElGamal system is that message expansion by a factor of two takes place during encryption. However, such message expansion is negligible if the cryptosystem is used only for exchange of secret keys.
- Not secure against common modulus attack
- Not secure against known plaintext attack

IV. CONCLUSION

In this paper, we presented a literature survey of the popular cryptography algorithms. The working of each method is also discussed in brief. The merits and demerits of each method are also described in summarized way.

REFERENCES
[12] Dr. S.A.M Rizvi1 ,Dr. Syed Zeeshan Hussain2 and Neeta Wadhwa” A Comparative Study Of Two Symmetric Encryption Algorithms Across Different Platforms”,