A Survey on Various Encryption Algorithms

[1]Supreetha Pai, [2]Arathi P
[1]Dept. of ISE, Dayananda Sagar Academy of Technology and Management, Bangalore, Karnataka, India
[2]Dept. of CSE, Dr. Ambedkar Institute of Technology, Bangalore, Karnataka, India

Abstract
This paper is a comprehensive survey on some common encryption algorithms. Robust encryption algorithms must minimize or even eradicate all the vulnerabilities associated with secure information transfer and management. Generally, encryption algorithms convert intelligible data into an unintelligible secure format.

Keywords
Encryption; Decryption; Cryptography; RSA; DES; AES

I. Introduction

Cryptography is the branch of cryptology dealing with the design of algorithms for encryption and decryption, intended to ensure the secrecy and/or authenticity of messages [1]. The two major types of cryptographic techniques are Symmetric Key Encryption and Asymmetric Key Encryption. The former performs encryption and decryption with a single key whereas the latter uses one key for encryption and another one for decryption. The core goals of cryptography are: Confidentiality, Integrity, Authentication, and Non-repudiation.

The various components of generic encryption algorithms are: Plaintext, Ciphertext, Secret Key, Encryption Algorithm and Decryption Algorithm.

A. Plaintext

The message in an intelligible (readable) form. This serves as the input to the encryption algorithm.

B. Ciphertext

The encrypted message which is in an unintelligible form. This is the output which the encryption algorithm generates using the plaintext as the input.

C. Secret Key

The secret key is one of the inputs to the encryption algorithm. It is used in the process of encrypting the plaintext.

D. Encryption Algorithm

This performs various functions and operations to convert the plaintext into the ciphertext. It takes the secret key and the plaintext as inputs and produces the ciphertext as the output (Fig 1).

E. Decryption Algorithm

This is the reverse of the encryption algorithm. Its operation is to convert the ciphertext back into the plaintext using the secret key and the ciphertext as inputs (Fig 2).

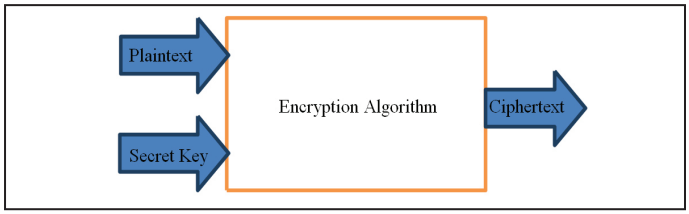

Fig. 1: Encryption

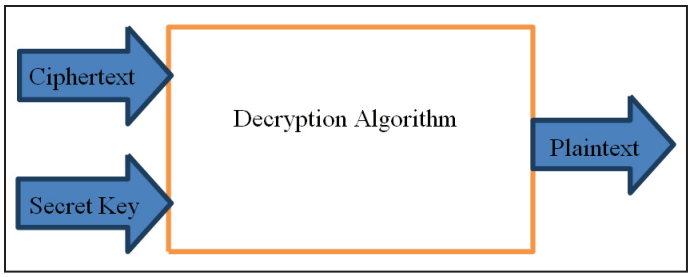

Fig. 2: Decryption

II. Overview of Algorithms

This section deals with some of the most commonly used Encryption algorithms. It includes three symmetric encryption algorithms (DES, AES, and Blowfish) and an asymmetric encryption algorithm (RSA).

A. Data Encryption Standard (DES)

It is the most popular symmetric and block cipher cryptography algorithm. DES [2] uses the Feistel cipher structure with 16 rounds of processing (Fig 3). It is a 64 bit block cipher algorithm. Each block of 64 bit plaintext is separately encrypted into a block of 64 bit ciphertext. DES uses a 56 bit key (actually 64 bits of the key is used, 8 bits are used as parity). The first round performs the initial permutation of 64 bits plaintext that is the independent of the key. Next, the plaintext block is divide the input into two equal (32 bits) parts left and right. The next 16 iterations (rounds) DES algorithm perform the same function but uses a different key. In 18th round the DES algorithm perform the switching of left and right parts. The last round performs the inverse permutation and generates the 64 bits ciphertext (that is also the independent of the key). The DES algorithm suffers from Simple Relations in its keys. The key schedule that DES uses is not one-way. This results in the attacker being able to recover most of the master-key by compromising the sub-keys of few rounds. The DES algorithm is vulnerable to linear cryptanalysis attacks as (Fig 3).

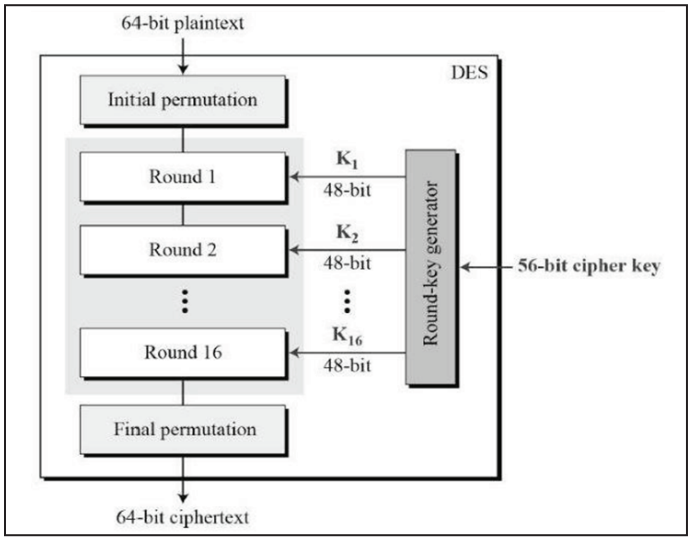

Fig. 3: Data Encryption Standard

B. Advanced Encryption Standard (AES)

Advanced Encryption Standard (AES) [3] is a symmetric key encryption algorithm. The algorithm was developed by two Belgian cryptographers Joan Daemen and Vincent Rijmen. AES is a block cipher deliberate to replace DES for commercial applications. AES was designed to be efficient in both hardware and software, and supports a block length of 128 bits and key lengths of 128, 192, and 256 bits. The basic difference between DES and AES is that in DES plaintext block is divided into two halves before the main algorithm starts whereas, in AES the entire block is processed to obtain the ciphertext as (Fig. 4).

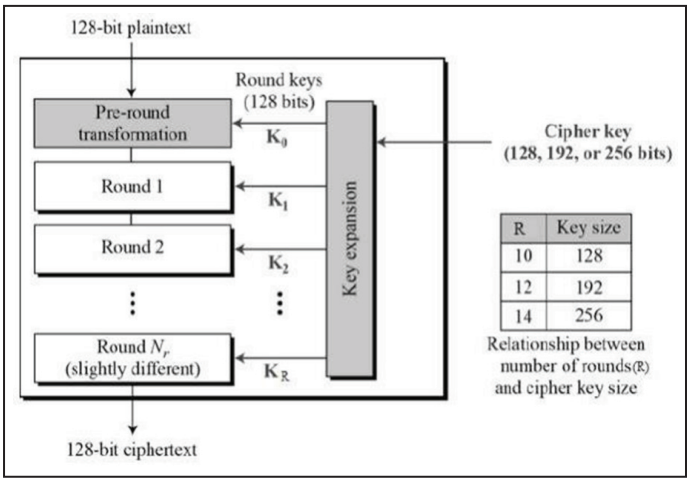

Fig. 4: Advanced Encryption Standard

C. Blowfish Algorithm

Blowfish [4] is a symmetric block cipher, designed by Bruce Schneier in 1993. The algorithm consists of two Parts: a key expansion part and a data encryption part. Blowfish has a 64-bit block size and a variable key length from 32 up to 448 bits. Key expansion converts a key of at most 448 bits into several sub-key arrays totaling 4168 bytes. Blowfish follows 16 rounds of Feistel Network. Bruce Schneier later created Twofish, which performs a similar function on 128-bit blocks. The Blowfish is designed to aim four criteria known as Fast, Compact, Simple and Variably Secure. Blowfish has some classes of weak keys. For these weak keys, separate rounds end up using the same round-keys. Keys belonging to these classes can be detected only in reduced-rounds versions of the algorithm and not on the full blowfish.

D. RSA Algorithm

RSA [5] algorithm is asymmetric cryptography algorithm. Asymmetric actually means that it works on two different keys i.e. Public Key and Private Key. As the name describes that the Public Key is given to everyone and Private Key is kept private.

The idea of RSA is based on the fact that it is difficult to factorize a large integer. The public key consists of two numbers where one number is multiplication of two large prime numbers. And private key is also derived from the same two prime numbers. So if somebody can factorize the large number, the private key is compromised. Therefore encryption strength totally lies on the key size and if we double or triple the key size, the strength of encryption increases exponentially. RSA keys can be typically 1024 or 2048 bits long, but experts believe that 1024 bit keys could be broken in the near future. But till now it seems to be an infeasible task.

III. Key Management

Key management techniques include Authenticated Key Exchange (AKE). Based on the number of involved parties, AKE protocols are classified into: 2 party AKE protocols [6], 3party AKE protocols [7] and N party AKE protocols [8].

Public key infrastructure (PKI) A public key infrastructure is a type of key management system that uses

hierarchical digital certificates to provide authentication, and public keys to provide encryption. PKIs are used in World Wide Web traffic, commonly in the form of SSL and TLS.

IV. Types of Authentication

Anonymity ensures that a user may use a resource or service without disclosing the user identity Completely. ID hiding usually means that a user may use a resource or service without disclosing the user identity during the protocol interaction, which is a kind of privacy protection partly. A pseudonym is an identifier of a subject other than one of the subject real names. ID hiding usually uses pseudonym to realize as the server may store the user identity. OTP (one-time password) usually means that the password can be used only once but the ID is plaintext during the protocol interaction, so there is no privacy protection. The above-mentioned terms related with authentication called anonymous authentication, hiding identity authentication and OTP authentication.

V. Conclusion

This survey paper summarizes various encryption algorithms and their approaches of encrypting text information. All of these techniques have their own advantages and disadvantages thus paving the way for newer encryption methods which might minimize the shortcomings of the existing algorithms without compromising on the existing functionality.

References

[1] William Stallings,"Cryptography and Network Security Principles and Practice", 5th Edition, Pearson Education, 2011.

[2] "Data Encryption Standard", Federal Information Processing Standards Publication 46-3, 1999.

[3] "Advanced Encryption Standard", Federal Information Processing Standards Publication 197(November 2001)

[4] B. Schneier,"Description of a New Variable Length Key, 64Bit Block Cipher (Blowfish), Fast Software Encryption", Cambridge Security Workshop Proceedings. Springer Verlagl, pp. 191-204, 1994.

[5] R. L. Rivest, A. Shamir, L. Adleman,"A Method for Obtaining Digital Signatures and Public-key Cryptosystems", Commun. ACM, Vol. 21, No. 2, pp. 120–126, 1978.

[6] Hongfeng Zhu, Yifeng Zhang, Yang Sun,"Provably Secure Multi-server Privacy-Protection System Based on Chebyshev Chaotic Maps without Using Symmetric Cryptograph", International Journal of Network Security, Vol. 18, No. 5, pp. 803-815, 2016.

[7] H. Li, C. K. Wu, J. Sun,"A general compiler for password-authenticated group key exchange protocol", Information Processing Letters, Vol. 110, No. 4, pp. 160–167, 2010.

[8] T. Y. Wu, Y. M. Tseng, T. T. Tsai,"A revocable ID-based authenticated group key exchange protocol with resistant to malicious participants", Computer Networks, Vol. 56, No. 12, pp. 2994–3006, 2012.

Supreetha Pai received her Bachelor of Engineering degree from Vivekananda College of Engineering and Technology, Puttur in 2008.She received her Master of Technology degree in Digital Electronics from East west Institute of Technology, Bangalore in 2013. She is the gold medalist in M.Tech Digital Electronics examinations from VTU. Currently, she is an assistant professor in Information Science Department in Dayananda Sagar Academy of Technology, Bangalore. Her research interests are in Data analytics and image processing, Internet of things.

Arathi P received her Bachelor of Engineering degree from JNNCE, Shimoga in 1999.She received her Master of Technology degree in AMC Engineering College in 2009. Currently, she is an assistant professor in Computer Science Department in Dr. Ambedkar Institute of Technology, Bangalore. Her research interests are in Artificial Intelligence computer Vision, and Data analytics.