A JOURNEY THROUGH CRYPTOGRAPHIC ALGORITHMS

JINI RAJU
M Tech Scholar
Department of Computer Science
Sree Buddha College of Engineering
Alappuzha,Kerala
jiniraju07@gmail.com

ARUN MADHU
Assistant Professor
Department of Computer Science
Sree Buddha College of Engineering
Alappuzha,Kerala
arunmadhu99@yahoo.com

Abstract— **Many cryptographic algorithms were evolved for the purpose of providing security to the data transmitted. All algorithms differ by the type of operations used for encryption, the number of keys used and the way in which the data is processed. In this paper, an extensive survey on the evolution of cryptographic algorithms is presented and this includes the traditional symmetric algorithms to the modern attribute based encryption algorithms. Symmetric cryptographic algorithms were the conventional encryption scheme in which same cryptographic key is used for both encryption and decryption. Unlike, Public key cryptographic systems use different keys for encryption and decryption. In some applications, traditional algorithms do not provide sufficient scalability. After the evolution of public key cryptography, a new trend evolves named as Identity based Encryption (IBE) that acts as an alternative to public key encryption and it avoids the need of a Public Key Infrastructure (PKI). Also, due to some drawbacks of IBE, Attribute Based encryption evolves and it is actually a realization of multiple IBEs. Thus the journey of cryptographic algorithms starts from symmetric key algorithm to attribute based algorithms. In this paper, most famous algorithms of each major category are also studied.**

Keywords—component; formatting; style; styling; insert (key words)

I. INTRODUCTION

The need for secure transmission and storage of data is increasing as more and more technology evolves. Humans are not the only one interesting in breaking the secrecy, even automated machine programs can interfere into the data transmission and may cause serious attacks. In this context, it is important to know about all the security attacks and the methods to prevent the attacks. Different types of cryptanalytic attacks can be done on an encrypted message such as includes Ciphertextonly attack, Known plaintext attack, Chosen plaintext attack, Chosen Ciphertext attack and Chosen text attack. Besides cryptanalytic attack, other attacks includes Denial of Service, masquerading, replaying, brute force attack, dictionary attack, password guessing attack and so on. Usually, the security can be assured by means of cryptographic algorithms. Cryptography dealt with secret coding and it is an effective method for the prevention of attacks. Major goals of cryptography include data confidentiality, integrity, authentication and access control.

The most primitive algorithms are symmetric and it is still used extensively. After the evolution of public key cryptography, the problem of key management solved. But the management of certificates and Public key infrastructures becomes a burden in some applications. In Identity Based encryption, any arbitrary string can take the role of a public key and it consists of a trusted Key Generation Centre (KGC) for the generation of private keys. In original IBE, some kind of error tolerance is accepted and is called as Fuzzy IBE. In IBE system, each user has a unique identity and this makes the IBE more secure. Unless the user reveals his identity and KGC remains secure, then there are no security breaches. Attribute Based Encryption (ABE) system is advancement in the area of cryptography and it is actually a realization of multiple IBEs. In ABE, multiple attributes are combined to form the private key of the user for decryption. Section II descibes the details of cryptography and discuss the trends in the secure data transmission. Section III deals with the standard symmetric algorithms and Section IV describes the standard asymmetric algorithms.

IJERT

II. TYPES OF CRYPTOGRAPHY

Cryptographic algorithm for encryption is mainly categorized into Private Key cryptography and Public key cryptography. Many modern trends are evolved now which can be used as an alternative to these includes Identity Based Cryptography and Attribute Based cryptography. These classes also contain a variety of algorithms for assuring the data confidentiality.

A. From Private Key Encryption to Public Key Encryption

Private Key Encryption is the only conventional encryption scheme before the development of Public Key Encryption. In Private Key Encryption, the main feature is the usage of same key for both encryption as well as decryption and hence the name symmetric encryption. Initially, these technique is used for protect the text by replacing a letter by digit or by another letter. Thus the techniques used in the early stages of symmetric cryptography include substitution and transposition ciphering. In substitution ciphering, plain text letters are replaced by any other letters or digits or symbols. The most famous one is the Caesar Cipher in which one letter is replaced by a letter standing three places down the alphabet. But it is very easy to recognize the plain text from a cipher text if the encryption and decryption algorithms are known. Transposition cipher makes some permutations to the plain text characters and then generates the cipher texts. The key has to be distributed from the sender to the recipients in a very secure manner. The use of key distribution centre (KDC) in this type of algorithms is actually a burden in the sense that the KDC knows all the secret keys and it questions the security of the keys. Diffie and Hellman addressed this problem and it leads to the development of Public Key

cryptography. In this scheme, the keys used for encryption and decryption are different and it is very difficult to determine the decryption key from the knowledge of encryption key and cryptographic algorithm. The use of different keys makes it termed as asymmetric algorithms. Public key encryption makes use of many mathematical concepts rather than substitutions and transpositions. Most popular Symmetric encryption standards include DES, IDEA, AES and Blowfish. Also, the famous classes of asymmetric encryption are RSA, Diffie-Hellman, Elliptic curve and DSA.

B. From Public Key encryption to Identity Based Encryption

Public key encryption, a message is encrypted under a public key e and the receiver is able to decrypt the message with a decryption key d. The keys are random strings that does not gives any idea about the identity of the users. Diffie Hellman key exchange can be used for the secure transmission of keys. But if the channe is not secure, then the ownership of a key cannot be ensured. This problem can be solved by using the usage of Public Key Infrastructure(PKI). A certification authority,CA, is used to sign the certificates to identify the sender of the message. One of the difficulties inherent in a PKI is the management of certificates and key-pairs. Thus Adi Shamir[10] introduces the identity based cryptography(IBE) in which the public keys are generated based on the identities of the user and it solves the difficulty in the certficate management.IBE is also a public key cryptography that includes the identities. A trusted authority named as Key Generation Center(KGC) is responsible for the generation of private keys. Private key is generated by combining the KGC's master secret key and the identities of users.In this, the identity associated with the private key matches exactly with the identity associated with the cipher text. Thus this IBE cannot be suitable in applications involving biometrics. The Certificate management can be greatly reduced but a major drawback of key escrow problem comes forward by the IBE.KGC knows all the private keys and it can decrypt the all the messages. Thus the security of IBE scheme is an open problem. Several schemes are introduced to solve the key escrow problem, but that solution spoils the advantage of IBE.

C. From Identity Based Encryption to Attribute Based Encryption

Because of the key escrow problem and the need of exact matching of the identity, IBE cannot be used in many secure applications. Fuzzy IBE[11] is introduced after the IBE that allows some error tolerance in the matching of identities. This Fuzzy IBE leads to the development of attribute based encryption(ABE). ABE is also a public key cryptographic system in which the encryption can be done based on the user attributes. The message can be read by all parties who has same attributes. ABE can be used to implement the fine grained access control. A user wants to encrypt a data based on the attribute set of the user. Thus, a file is encrypted for a group of user that have the same set of attributes and this reduces the encryption overhead present in public key cryptosystems using keys. The documents have to be stored on an untrusted server because the server can't decrypt the file. The encrypted file can be decrypted only by the users who possess the valid attribute set. Thus key escrow problem can be solved. Different classifications of ABE exist and it includes Key Policy ABE, Cipher Policy ABE, multi authority ABE and so on. ABE scheme is mainly used in log encryptions.

III. STANDARD SYMMETRIC ALGORITHMS

Symmetric key encryption algorithms are based on the Feistel structure. The digital data stream can be encrypted one bit at a time is the stream ciphering and the encryption of data by considering one block at a time is called as block ciphering. Most of the symmetric algorithms use the block ciphering principle.

A. Data Encryption Standard

In 1977, Data Encryption standard was adopted by the NIST and FIPS and is the most widely used symmetric encryption block cipher algorithm. It follows the Feistel structure and the data are encrypted in 64 bit blocks and it uses a 56 bit key, both acts as the inputs to the encryption algorithm. Sixteen identical rounds of operations are performed and the major techniques include the traditional substitution and transposition. After all rounds and inverse permutations, a 64 bit output is generated as the cipher text. But now, DES is not suitable for many applications because of its shorter key length and the symmetric key design. A DES key can be easily broken by Deep Crack and distributed.net in 22 hours and 15 minutes [1] in 1999. The DES encryption and Decryption can be viewed in Fig 2.Because of this vulnerability to brute force attack, the developers design a DES with multiple encryption and multiple keys. Double DES and Triple DES belong to this category. Triple DES is considered to be more secure because of the use of longer 168 bit key length. 3DES makes use of the original DES algorithm and apply the algorithm three times with different keys (K1, K2, K3). This algorithm is three times slow than DES in its software implementation is also sluggish in nature. Another variation is a two key triple DES that uses two keys in which K1 and K3 are the same. The key size is reduced to 112 bits and is less secure. Despite of all drawbacks, three key 3DES is now used in many Internet protocols.

B. International Data Encryption Algorithm

International Data Encryption Algorithm (IDEA)[2] is a block cipher algorithm first described in 1991. This algorithm is designed by Xuejia Lai and James L. Massey and it is a minor revision of an earlier cipher, PES (Proposed Encryption Standard IDEA was invented for the intention of replacing the DES and was originally called as Improved PES(IPES).IDEA was used in early versions of the Pretty Good Privacy cryptosystem. IDEA operates on 64 bit block sized plain text and cipher text and the key length is 128 bit. The standard consists of mainly two parts-key generation and encryption. Eight rounds of operations are present in this standard. 128 bit key is divided into fifty two 16 bit key sub-blocks cyclical sifting operations. The 64-bit plaintext block is divided into four 16-bit sub-blocks and all the operations used in the encryption process operate on 16-bit blocks. According to Daemon's report[3], large classes of weak keys have been found for the block cipher algorithm IDEA.

IJERT

C. Advanced Encryption Standard

In order to find a replacement to DES, NIST organized a call for new proposals in 1997 for a new Advanced Encryption standard which should have a better security and efficiency. 15 proposals were accepted in the first round and 5 were accepted for the second round. Finally, the algorithm selected was the Rijndael developed by Dr. Joan Daemen and Dr. Vincent Rijmen. 3DES was replaced by AES after a number of years. AES[4] is a symmetric block cipher algorithm in which key length can be 128,192 or 256 bits and a fixed block length of 128 bits is used and hence it is resistant to all known attacks. AES design includes the substitution and permutation techniques and there are 10 rounds for 128 bit key for both encryption and decryption and the input is the plain text of 128 bits. AES operates on a 4*4 column major order matrix and there are four different stages within each round except the last round. SubstituteBytes, ShiftRows, MixColumns and AddRoundKey are the different stages. For both encryption and decryption, the AddRoundKey is the first stage. The decryption algorithm is not similar to the encryption algorithm, but all the stages are reversible in nature. Square attack can be possible in AES and was proposed by the Rijndael itself. But according to NIST[4], "Assuming that one could build a machine that could recover a DES key in a second (i.e., try 255 keys per second), then it would take that machine approximately 149 thousand-billion (149 trillion) years to crack a 128-bit AES key." Thus AES is very secure against all attacks and is now replace the DES and 3 DES in almost every application.

D. Blowfish

Blowfish is designed in 1993 by Bruce Schneier[5]-[7] and it is a symmetric-key block cipher. No effective cryptanalysis of it has been found to date. Also, Blowfish is not patented and can be used as open source and thus it is still used in many countries. However, the Advanced Encryption Standard (AES) now receives more attention. It follows the Feistel network design and is a variable length key block cipher. The block size is fixed 64 bit and the key length varies from 32 bits to 448 bits. The algorithm consists of two parts: data encryption part and subkey generation part. The encryption has 16 rounds and each round consists of substitution and permutation methods. Permutation is dependent on the key and substitution is dependent on key and data. Key expansion converts a key of at most 448 bits into several subkey arrays totaling 4168 bytes. Data encryption occurs via a 16-round Feistel network. Additions and XORing are the main operations done on 32 bit words. Additional operation includes four indexed array data lookups per round. Twofish is a successor of Blowfish and was first published in 1998.It is a symmetric key block cipher algorithm using a block size of 128 bits. The key lengths may be 128,152 or 256 bit and all the operations are similar to Blowfish.

IV. STANDARD ASYMMETRIC ALGORITHMS

A. RSA

RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman and it was published[8] in 1978. It is the first practically available asymmetric algorithm based on the idea of Diffie Hellman and is used for the secure data transmission. The security of RSA relies on the factoring problem. RSA involves mainly three steps-key generation, encryption and decryption. RSA involves a public key-private key pair and the sender uses the public key for encryption and it is available to all the users in the system. The decryption of the data can be done only using the corresponding private key and it is known to the particular recipient only. The sender has to choose two random prime numbers, p and q and then calculates n=pq. The e can be calculated as gcd((p-1)(q-1))=1 and d can be calculated as de=1 (mod (p-1)(q-1)). Thus the public encryption key is (n,e) and the private decryption key is (p,q,d). The cipher text can be generated as

C=m^e mod n

The original message can be retrieved by

M=C^d mod n

The attacker gets only the n, e and C and it is practically infeasible to calculate the prime factors of a large number n; this increases the security of the data. Methods like this are commonly used for small amounts of data. When transmitting large amounts of data, RSA is very slow in computation. Thus, RSA algorithm is used to transfer a symmetric key for a faster encryption algorithm and the faster algorithm is used to encrypt and decrypt the data.

B. Diffie-Hellman Key exchange

It is a secure method[9] used for the exchange of keys and it is not a complete public key cryptosystem. Whitfield Diffie and Martin Hellman are the brains behind this idea and it was first published in 1976. The security relies on the difficulty in the computation of discrete logarithms. Fig 1 describes the algorithm and it is very secure. This algorithm is used in many of the public key algorithms for the key exchange. In the original proposal, authentication of sender or receiver is not included and it leads to the Man In The Middle attack. This vulnerability can be solved by using the digital signatures or certificates.

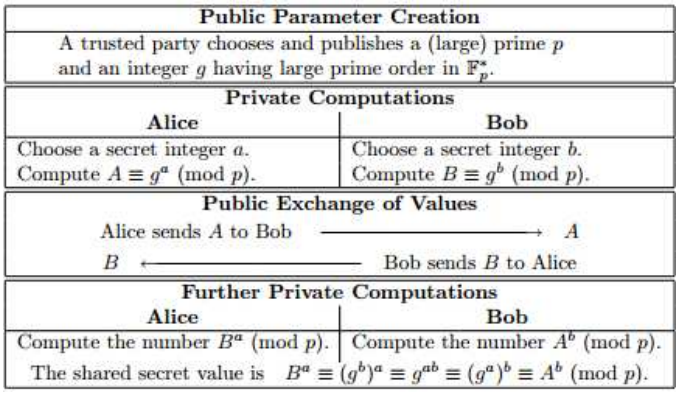

Fig 1: Diffie Hellman Key exchange protocol

REFERENCES

[1] Electronic Frontier Foundation, DES challenge III broken in record 22 hours, January 1999. (http://www.eff.org/Privacy/Crypto /Cryptomisc/ DESCracker/ HTML/19990119-deschallenge3.html).

[2] Ascom, IDEACrypt Coprocessor Data Sheet, 1999.(http:// www. ascom.ch/infosec/downloads/IDEACryptCoprocessor.pdf).

[3] J. Daemen, R. Govaerts, and J. Vandewalle, Weak keys for IDEA, Advances in Cryptology - Crypto '93, Springer-Verlag (1994), pp. 224-231.

[4] Joan Daemen and Vincent Rijmen, AES submission document on Rijndael, Version 2, September 1999. http://csrc.nist.gov/ CryptoToolkit/aes/rijndael/Rijndael.pdf

[5] B. Schneier, ”Description of a New Variable Length Key, 64-Bit Block Cipher (Blowfish)Fast Software Encryption”, CambridgeSecurity.

[6] Bruce Schneier, The Blowfish Encryption Algorithm Retrieved October 25, 2008.http://www.schneier.com/blowfish.html

[7] B. Schneier, ” Applied Cryptography”, John Wiley and Sons, New York, 1994.

[8] R.L. Rivest, A. Shamir, and L.‘Adleman. A method for obtaining digital signatures and public-key cryptosystems.Communications of the A.C.M., 21(2):120-126, February 1978.

[9] W. Diffie and M. Hellman. New directions in cryptography. IEEE Transactions on Information Theory, IT-22(6):644-654, 1976.

[10]A. Shamir,Identity based Cryptosystems and Signature Schemes,Proceedings of CRYPTO84 on Advances in cryptology, pages 47 -53. Springer,Verlag New York, 1985.

[11] A. Sahai and B. Waters,Fuzzy Identity Based Encryption,Advances in Cryptology Eurocrypt, volume 3494 of LNCS, pages 457 -473. Springer, 2005.

IJERT