A walkthrough on various methods of Public Key Cryptosystems

Miss. Mayuri Rajas
Department of CSE
PRMIT&R, Badnera-Amravati

Prof. M. A. Pund
Department of CSE
PRMIT&R, Badnera-Amravati

Abstract - *To make secure data transmission over networks cryptography is used. The algorithm selected for cryptography should fulfill the conditions of integrity protection, conventional message authentication and digital signatures. Key exchange algorithms, hash functions, PN numbers are used for encryption and decryption of data. This encryption can be applied on data in stream format or in blocks. Moreover the length of key is the biggest constraint in encryption. Here in our paper we have studied present algorithms currently used for encryption.*

***Key Words*: Public Key Algorithm, Symmetric Key Algorithm, Hash Function, Cipher Text, Key Length**

1. INTRODUCTION

Cryptography is the practice of secure data communication in the presence of third party. Cryptography encrypt the data at the transmitter end to protect it from stolen and from errors. More generally, it is about constructing and analyzing protocols that overcome the influence of adversaries and which are related to various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation. It deals with mathematics, computer science and electrical engineering. Cryptography comes from the Greek words for ''secret writing.'' It has a long and colorful history going back thousands of years. Professionals make a distinction between ciphers and codes. A cipher is a character-for-character or bit-for-bit transformation, without regard to the linguistic structure of the message. In contrast, a code replaces one word with another word or symbol. Codes are not used any more, although they have a glorious history [1][2].

The messages to be encrypted, known as the plaintext, are transformed by a function that is parameterized by a key. The output of the encryption process, known as the cipher text, is then transmitted, often by messenger or radio. We assume that the enemy, or intruder, hears and accurately copies down the complete cipher text. However, unlike the intended recipient, he does not know what the decryption key is and so cannot decrypt the cipher text easily. Sometimes the intruder can not only listen to the communication channel (passive intruder) but can also record messages and play them back later, inject his own messages, or modify legitimate messages before they get to the receiver (active intruder). The art of breaking ciphers, called cryptanalysis, and the art devising them (cryptography) is collectively known as cryptology. Beyond that the security of conventional encryption depends on the secrecy of the key not the secrecy of the algorithm. We do not need to keep the algorithm secret; we need to keep only the secret key.

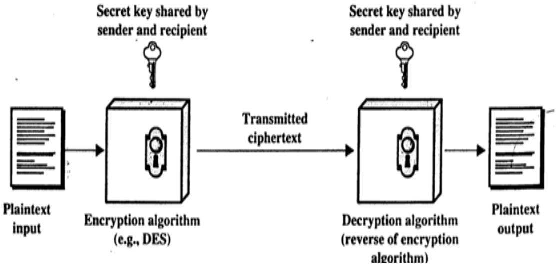

Secret key shared by sender and recipient
Secret key shared by sender and recipient
Transmitted ciphertext
Plaintext input
Encryption algorithm (e.g., DES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

Figure1: Simplified Model of Convolutional Algorithm

2. Cryptography Terminology

The modern field of cryptography can be divided into several areas of study.

2.1 SECRETE CRYPTOGRAPHY

With secret key cryptography, a single key is used for both encryption and decryption. As shown in Figure 2, the sender uses the key (or some set of rules) to encrypt the plaintext and sends the cipher text to the receiver. The receiver applies the same key (or rule set) to decrypt the message and recover the plaintext. Because a single key is used for both functions, secret key cryptography is also called symmetric encryption.

plaintext
ciphertext
plaintext

Figure 2: Secret key Cryptography. SKC uses same secret key for both encryption and decryption

Secret key cryptography schemes are generally categorized as being either stream ciphers or block ciphers. Stream ciphers operate on a single bit (byte or computer word) at a time and implement some form of feedback mechanism so that the key is constantly changing. A block cipher is so-called because the scheme encrypts one block of data at a time using the same key on each block. In general, the same plaintext block will always encrypt to the same cipher text when using the same key in a block cipher whereas the same plaintext will encrypt to different cipher text in a stream cipher [3].

Stream ciphers are of many types but two are worth mentioning here. Self-synchronizing stream ciphers calculate each bit in the key stream as a function of the previous n bits in the key stream. It is termed "self-synchronizing" because the decryption process can stay synchronized with the encryption process merely by knowing how far into the n-bit key stream it is. One problem is error propagation; a garbled bit in transmission will result in n garbled bits at the receiving side. Synchronous stream ciphers generate the key stream in a fashion independent of the message stream but by using the same key stream generation function at sender and receiver. While stream ciphers do not propagate transmission errors, they are, by their nature, periodic so that the key stream will eventually repeat.

Block ciphers can operate in one of several modes; the following four are the most important:

- Electronic Codebook (ECB) mode is the simplest, most obvious application: the secret key is used to encrypt the plaintext block to form a cipher text block. Two identical plaintext blocks, then, will always generate the same cipher text block. Although this is the most common mode of block ciphers, it is susceptible to a variety of brute-force attacks.

- Cipher Block Chaining (CBC) mode adds a feedback mechanism to the encryption scheme. In CBC, the plaintext is exclusively-ORed (XORed) with the previous cipher text block prior to encryption. In this mode, two identical blocks of plaintext never encrypt to the same cipher text.

- Cipher Feedback (CFB) mode is a block cipher implementation as a self-synchronizing stream cipher. CFB mode allows data to be encrypted in units smaller than the block size, which might be useful in some applications such as encrypting interactive terminal input. If we were using 1-byte CFB mode, for example, each incoming character is placed into a shift register the same size as the block, encrypted, and the block transmitted. At the receiving side, the cipher text is decrypted and the extra bits in the block (i.e., everything above and beyond the one byte) are discarded.

2.2 PUBLIC KEY CRYPTOGRAPHY

Symmetric-key cryptosystems use the same key for encryption and decryption of a message, though a message or group of messages may have a different key than others. A significant disadvantage of symmetric ciphers is the key management necessary to use them securely. Each distinct pair of communicating parties must, ideally, share a different key, and perhaps each cipher text exchanged as well [4][5]. The number of keys required increases as the square of the number of network members, which very quickly requires complex key management schemes to keep them all straight and secret. The difficulty of securely establishing a secret key between two communicating parties, when a secure channel does not already exist between them, also presents a chicken-and-egg problem which is a considerable practical obstacle for cryptography users in the real world.

plaintext
ciphertext
plaintext

Figure 3: Public Cryptography with Different Key.

In public cryptography two different keys- public and private are generated. These two keys are different but interdependent on each other. In public-key cryptosystems, the public key may be freely distributed, while its paired private key must remain secret. In a public-key encryption system, the public key is used for encryption, while the private or secret key is used for decryption. Public-key cryptography can also be used for implementing digital signature schemes. A digital signature is reminiscent of an ordinary signature; they both have the characteristic of being easy for a user to produce, but difficult for anyone else to forge. Digital signatures can also be permanently tied to the content of the message being signed; they cannot then be 'moved' from one document to another, for any attempt will be detectable.

Public-key cryptography algorithms that are in use today for key exchange or digital signatures include:

- RSA: The first, and still most common, PKC implementation, named for the three MIT mathematicians who developed it — Ronald Rivest, Adi Shamir, and Leonard Adleman. RSA today is used in hundreds of software products and can be used for key exchange, digital signatures, or encryption of small blocks of data. RSA uses a variable size encryption block and a variable size key. The key-pair is derived from a very large number, n, that is the product of two prime numbers chosen according to special rules; these primes may be 100 or more digits in length each, yielding an n with roughly twice as many digits as the prime factors [6]. Nevertheless, if a large number is created from two prime factors that are roughly the same size, there is no known factorization algorithm that will solve the problem in a reasonable amount of time. Regardless, one presumed protection of RSA is that users can easily increase the key size to always stay ahead of the computer processing curve. As an aside, the patent for RSA expired in September 2000 which does not appear to have affected RSA's popularity one way or the other.

- Diffie-Hellman: After the RSA algorithm was published, Diffie and Hellman came up with their own algorithm. D-H is used for secret-key key exchange only, and not for authentication or digital signatures.

- Digital Signature Algorithm (DSA): The algorithm specified in NIST's Digital Signature Standard (DSS), provides digital signature capability for the authentication of messages.

- Cramer-Shoup: A public-key cryptosystem proposed by R. Cramer and V. Shoup of IBM in 1998.

- Key Exchange Algorithm (KEA): A variation on Diffie-Hellman; proposed as the key exchange method for Capstone.

- LUC: A public-key cryptosystem designed by P.J. Smith and based on Lucas sequences. Can be used for encryption and signatures, using integer factoring.

HASH FUNCTION

Hash functions, also called message digests and one- way encryption, and are algorithms that, in some sense, use no key (Figure 4). Instead, a fixed-length hash value is computed based upon the plaintext that makes it impossible for either the contents or length of the plaintext to be recovered. Hash algorithms are typically used to provide a digital fingerprint of a file's contents, often used to ensure that the file has not been altered by an intruder or virus[8]. Hash functions are also commonly employed by many operating systems to encrypt passwords. Hash functions, then, provide a measure of the integrity of a file.

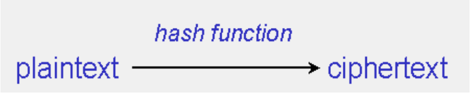


Figure4: Hash Function Encryption

Hash algorithms that are in common use today include:

- Message Digest (MD) algorithms: A series of byte-oriented algorithms that produce a 128-bit hash value from an arbitrary-length message.
  - MD2 (RFC 1319): Designed for systems with limited memory, such as smart cards. (MD2 has been relegated to historical status, per RFC 6149.)[7]
  - MD4 (RFC 1320): Developed by Rivest, similar to MD2 but designed specifically for fast processing in software. (MD4 has been relegated to historical status, per RFC 6150.)
  - MD5 (RFC 1321): Also developed by Rivest after potential weaknesses were reported in MD4; this scheme is similar to MD4 but is slower because more manipulation is made to the original data. MD5 has been implemented in a large number of products .
- Secure Hash Algorithm (SHA): Algorithm for NIST's Secure Hash Standard (SHS). SHA-1 produces a 160-bit hash value and was originally published as FIPS 180-1 and RFC 3174. FIPS 180-2 (aka SHA-2) describes five algorithms in the SHS: SHA-1 plus SHA-224, SHA-256, SHA-384,

and SHA-512 which can produce hash values that are 224, 256, 384, or 512 bits in length, respectively.

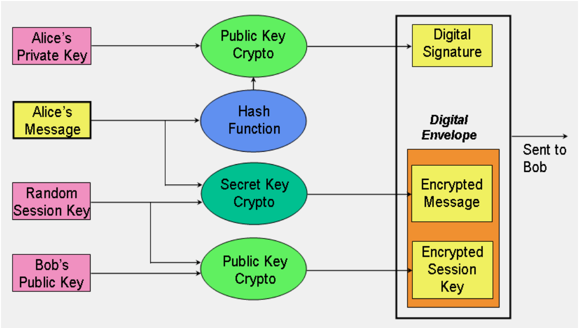


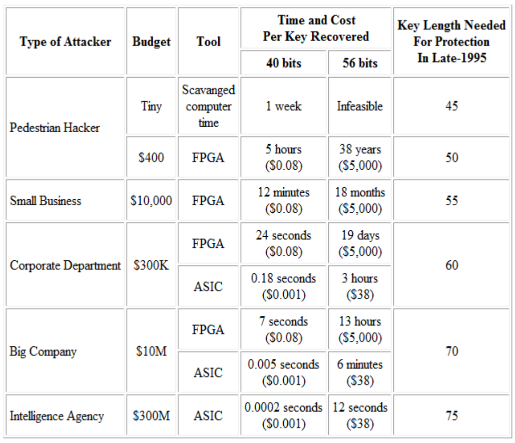
Figure5: Sample Application of three cryptographic Techniques

3. SIGNIFICANCES OF KEY LENGTH

The table below shows what DES key sizes are needed to protect data from attackers with different time and financial resources. This information is not merely academic; one of the basic tenets of any security system is to have an idea of what you are protecting and from whom you are protecting it! The table clearly shows that a 40-bit key is essentially worthless today against even the most unsophisticated attacker. On the other hand,

56-bit keys are fairly strong unless you might be subject to some pretty serious corporate or government espionage. But note that even 56-bit keys are declining in their value and that the times in the table are worst cases [9] [10].

TABLE 1. Minimum Key Lengths for Symmetric Ciphers.



Type of Attacker	Budget	Tool	Time and Cost Per Key Recovered		Key Length Needed For Protection In Late-1995
			40 bits	56 bits	
Pedestrian Hacker	Tiny	Scavanged computer time	1 week	Infeasible	45
	$400	FPGA	5 hours ($0.08)	38 years ($5,000)	50
Small Business	$10,000	FPGA	12 minutes ($0.08)	18 months ($5,000)	55
Corporate Department	$300K	FPGA	24 seconds ($0.08)	19 days ($5,000)	60
		ASIC	0.18 seconds ($0.001)	3 hours ($38)	
Big Company	$10M	FPGA	7 seconds ($0.08)	13 hours ($5,000)	70
		ASIC	0.005 seconds ($0.001)	6 minutes ($38)	
Intelligence Agency	$300M	ASIC	0.0002 seconds ($0.001)	12 seconds ($38)	75

4. CONCLUSIONS

Cryptography has been emerged as essential tool for data transmission. Various algorithms of cryptography has been studied, If advantages of all these algorithms are combined in one algorithm then performance of cryptography can be increased along with the length of key. In public key algorithm for generation of private key CDMA approach of communication can be used. Each user is provided a Different unique number called PN number and no other user is having that number. For each user this unique number is generated randomly and at the receiver end same PN number can be used to decrypt the message.

REFERENCES

[1] P. Rogaway, T. Shrimpton, Cryptographic Hash- Function Basics:Definitions, Implications, and Separations for Preimage Resistance, Second-Preimage Resistance, and Collision Resistance (FSE 2004)

[2] Jim Alves-Foss, An Eficient Secure Authenticated Group Key Exchange Algorithm for Large and Dynamic Groups

[3] J. Black, P. Rogaway, and T. Shrimpton. Black-box analysis of the block-cipher-based hashfunction constructions from PGV. In Advances in Cryptology – CRYPTO '02, volume 2442 of Lecture Notes in Computer Science. Springer-Verlag, 2002.

[4] Mao, W. (2004). Modern Cryptography: Theory & Practice. Upper Saddle River, NJ: Prentice Hall Professional Technical Reference.

[5] Vishwa gupta, Gajendra Singh, Ravindra Gupta, Advance cryptography algorithm for improving data security,IJARCSSE vol 2Issue 1, Jan2012

[6] Symmetric key cryptography using random key generator, A.Nath, S.Ghosh, M.A.Mallik, Proceedings of International conference on SAM-2010 held at Las Vegas(USA) 12-15 July,2010, Vol-2,P-239-244.

[7] Data Hiding and Retrieval, A.Nath, S.Das, A.Chakrabarti, Proceedings of IEEE International conference on Computer Intelligence and Computer Network held at Bhopal from 26-28 Nov, 2010.

[8] Md. Nazrul Islam, Md. Monir Hossain Mia, Muhammad F. I. Chowdhury, M.A. Matin ―Effect of Security Increment to Symmetric Data Encryption through AES Methodology, Ninth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing 978-0-7695-3263-9/08 DOI 10.1109/SNPD.2008.101 IEEE 2008.

[9] Dripto Chatterjee, Joyshree Nath, Suvadeep Dasgupta, Asoke Nath ―A new Symmetric key Cryptography Algorithm using extended MSA method: DJSA symmetric key algorithm published in 2011 International Conference on Communication Systems and Network Technologies, 978-0-7695-4437-3/11 $26.00 © 2011 IEEE.

[10] [Rijn99] Joan Daemen and Vincent Rijmen, AES submission document on Rijndael, Version 2, September 1999.