International Journal of Computer Applications Technology and Research
Volume 3– Issue 2, 130 - 135, 2014

Analysis of Cryptographic Algorithms for Network Security

Kritika Acharya
DIT University
Dehradun, India

Manisha Sajwan
DIT University
Dehradun, India

Sanjay Bhargava
DIT University
Dehradun, India

Abstract: Cryptography plays a major role in securing data. It is used to ensure that the contents of a message are confidentially transmitted and would not be altered. Network security is most vital component in information security as it refers to all hardware and software function, characteristics, features, operational procedures, accountability, access control, and administrative and management policy. Cryptography is central to IT security challenges, since it underpins privacy, confidentiality and identity, which together provide the fundamentals for trusted e-commerce and secure communication. There is a broad range of cryptographic algorithms that are used for securing networks and presently continuous researches on the new cryptographic algorithms are going on for evolving more advanced techniques for secures communication.

Keywords: Cryptography, plain text, cipher text, encryption, decryption, network security.

1. INTRODUCTION

The building blocks of computer security are cryptographically-based mechanism. Cryptography can be applied anywhere in the TCP/IP stack, though it is not common at physical layer. Cryptography is also used in complicated protocols that help to achieve different security services, thus called security protocols. The main feature of the encryption/decryption program implementation is the generation of the encryption key [1].

1.1 Basic Terms Used in Cryptography

1.1.1 Plain Text

The original message that the person wishes to communicate with the other is defined as Plain the original message that the person wishes to communicate with the other is defined as Plain Text. In cryptography the actual message that has to be send to the other end is given a special name as Plain Text. For example, Alice is a person wishes to send "Hello Friend how are you" message to the person Bob. Here "Hello Friend how are you" is a plain text message.

1.1.2 Cipher Text

The message that cannot be understood by anyone or meaningless message is what we call as Cipher Text. In Cryptography the original message is transformed into non readable message before the transmission of actual message. For example, "Ajd672#@91ukl8*^5%" is a Cipher Text produced for "Hello Friend how are you".

1.1.3 Key

A specific string of data that is used to encrypt and decrypt messages, documents or other types of electronic data.. Keys have varying levels of strength. Keys having higher numbers of bits are theoretically tougher to break because there are more possible permutations of data bits. (Since bits are binary, the number of possible permutations for a key of x bits is 2x.) The specific way a key is used depends on whether it's used with asymmetric or symmetric cryptography.

1.1.4 Encryption

A process of converting Plain Text into Cipher Text is called as Encryption. Cryptography uses the encryption technique to send confidential messages through an insecure channel. The process of encryption requires two things- an encryption algorithm and a key. An encryption algorithm means the technique that has been used in encryption. Encryption takes place at the sender side.

1.1.5 Decryption

A reverse process of encryption is called as Decryption. It is a process of converting Cipher Text into Plain Text. Cryptography uses the decryption technique at the receiver side to obtain the original message from non-readable message (Cipher Text). The process of decryption requires two things- a Decryption algorithm and a key. A Decryption algorithm means the technique that has been used in Decryption. Generally the encryption and decryption algorithm are same.

Now a day, cryptography has many commercial applications. If we are protecting confidential information then cryptography is provide high level of privacy of individuals and groups. However, the main purpose of the cryptography is used not only to provide confidentiality, but also to provide solutions for other problems like: data integrity, authentication, non-repudiation. Cryptography is the methods that allow information to be sent in a secure from in such a way that the only receiver able to retrieve this information. Cryptography not only protects data from theft or alteration, but can also be used for user authentication. It is necessary to apply effective encryption/decryption methods to enhance data security. Cryptography provides a number of security goals to ensure the privacy of data, non-alteration of data etc[2].

1.2 Goals of Cryptography

1.2.1 Confidentiality

Ensures that no one can read the message except the intended receiver.

1.2.2 Authentication

Mechanism to realize authentic communication i.e. the process of proving one's identity.

1.2.3 Integrity

Assuming the receiver that the received message has not been altered in any way from the original.

1.2.4 Non-Repudiation

Ensures that neither the sender nor the receiver of message should be able to deny the transmission.

1.2.5 Access Control

Only the authorized parties are able to access the given information.

Network security involves the authorization of access to data in a network, which is controlled by the network administrator. The initial encrypted data is referred to as plain text. It is encrypted into cipher text, which will in turn be decrypted into usable plain text. Cryptographic algorithms are categorized based on the number of key that are employed for encryption and decryption[4].

1.3 Three Cryptographic Schemes

1.3.1 Secret Key Cryptography Or Symmetric Cryptography

Uses a single key for both encryption and decryption.

1.3.2 Public Key Cryptography Or Asymmetric Cryptography

Uses one key for encryption and another for decryption[2].

1.3.3 Hash Function

Uses a mathematical transformation to irreversibly "encrypt" information[14].

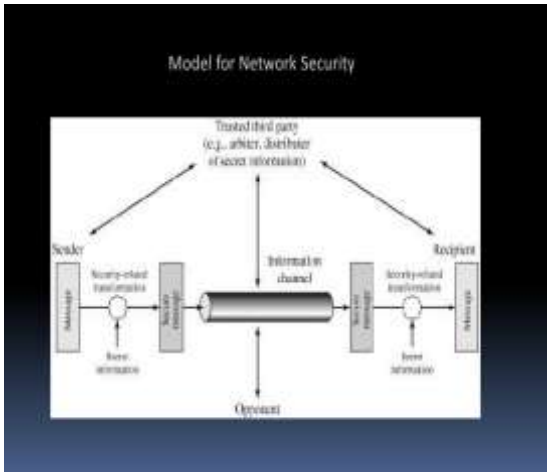

Figure 1. Model For network security

2. METHODOLOGY

Before implementing an encryption algorithm, we need to understand the principle behind the encryption i.e. to secure data held within a message or file and to ensure that the data is unreadable to others. The most important type of the encryption type is the symmetric key encryption. In the symmetric key encryption both for the encryption and decryption process the same key is used. Hence the secrecy of the key is maintained and it is kept private. It works with high speed. The symmetric key encryption takes place in two methodologies either as the block ciphers or as the stream ciphers. One of the main advantages of using the symmetric key encryption is that the computational power to this encryption technique is small. The keys for this are unique or there exists a simple transformation between the two keys[17].

Asymmetric key encryption is the technique in which the keys are different for the encryption and the decryption process. They are also known as the public key encryption. Public key methods are important because they can be used for transmitting encryption keys or other data securely even when the both the users have no opportunity to agree on a secret key in private, Algorithm[18]. Asymmetric algorithms are generally slow and it is impractical to use them to encrypt large amounts of data. The keys used in public-key encryption algorithms are usually much longer that improves the security of the data being transmitted[4].

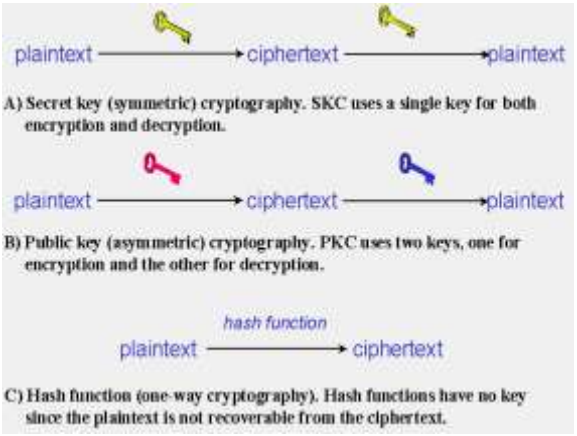

Figure 2. Cryptographic Schemes

2.1 How Encryption Works in Cryptography

Encryption is not just a tool for spies and hackers, it can be a valuable asset even in the business world. For example, say you're an engineer for a company like Beyond the Office Door, an office furniture company that designs adjustable desks, and you just came up with a fantastic new adjustable desk design that will blow the world away. You can be pretty sure that your email is secure when sending information, but is "pretty sure" good enough when you're sending information on a new prototype adjustable desk? It's not, and thus it would be a perfect time for encryption to be used in the business world. And of course, there are many other valuable applications for encryption that are more mundane than trade secrets, like financial data, medical or legal information and so on.

The easy part of encryption is applying a mathematical function to the plaintext and converting it to an encrypted cipher. The harder part is to ensure that the people who are supposed to decipher this message can do so with ease, yet only those authorized are able to decipher it. We of course also have to establish the legitimacy of the mathematical function used to make sure that it is sufficiently complex and mathematically sound to give us a high degree of safety[5].

2.2 Classification Of Encryption Schemes

2.2.1 Symmetric Key Encryption

2.2.1.1 DES(Data Encryption Standard)

DES is a symmetric block cipher developed by IBM. The algorithm uses a 56-bit key to encipher/decipher a 64-bit block of data. The key is always presented as a 64-bit block, every 8th bit of which is ignored. However, it is usual to set each 8th bit so that each group of 8 bits has an odd number of bits set to 1.

2.2.1.2 Triple DES(3DES)

3DES is an enhancement of DES; it is 64 bit block size with 192 bits key size. In this standard the encryption method is similar to the one in the original DES but applied 3 times to increase the encryption level and the average safe time. It is a known fact that 3DES is slower than other block cipher methods[3].

2.2.1.3 AES

AES is a block cipher .It has variable key length of 128, 192, or 256 bits; default 256. It encrypts data blocks of 128 bits in 10, 12 and 14 round depending on the key size[16]. AES encryption is fast and flexible; it can be implemented on various platforms especially in small devices. Also, AES has been carefully tested for many security applications[11].

2.2.1.4 BlowFish

Blowfish algorithm is the important type of the symmetric key encryption that has a 64 bit block size and a variable key length from 32 bits to 448 bits in general. Since the key size is larger it is complex to break the code in the blowfish algorithm. Moreover it is vulnerable to all the attacks except the weak key class attack.

2.2.1.5 RC4

RC4 is recognized as the most commonly utilized stream cipher in the world of cryptography. RC4 has a use in both encryption and decryption while the data stream undergoes XOR together with a series of generated keys. It takes in keys of random lengths and this is known as a producer of pseudo arbitrary numbers.The output is then XORed together with the stream of data in order to generate a newly-encrypted data.

2.2.2 Asymmetric Key Encryption

2.2.2.1 RSA

Rivest-Shamir-Adleman is the most commonly used public key encryption algorithm. It can be used to send an encrypted message without a separate exchange of secret keys. It can also be used to sign a message. In RSA, this asymmetry is based on the practical difficulty of factoring the product of two large prime numbers, the factoring problem. RSA computation occurs with integers modulo n = p * q, for two large secret primes p, q. To encrypt a message m, it is exponentiated with a small public exponent e. For decryption, the recipient of the cipher text c = me (mod n) computes the multiplicative reverse d = e-1 (mod (p-1)*(q-1)) (we require that e is selected suitably for it to exist) and obtains cd = m e * d = m (mod n). The key size should be greater than 1024 bits for a reasonable level of security.

2.2.2.2 Diffie-Hellman Algorithm

The Diffie–Hellman key exchange method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel. This key can then be used to encrypt subsequent communications using a symmetric key cipher. The Diffie-Hellman protocol is generally considered to be secure when an appropriate mathematical group is used[10].

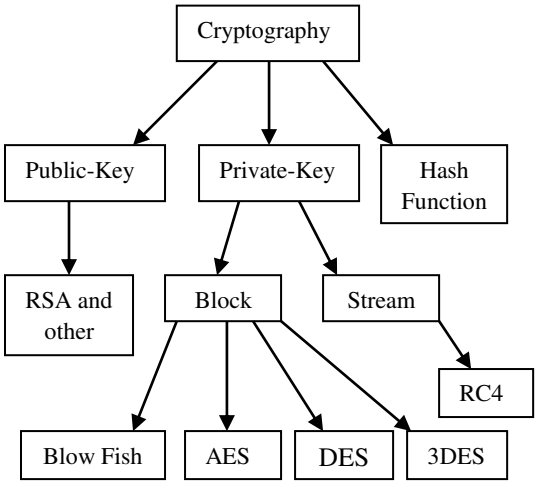

Figure 3. Model for Cryptography

2.3 Quantum Cryptography: A New Approach To Security

Quantum cryptography is a technology in which two parties can secure network communications by applying the phenomena of quantum physics. The security of these transmissions is based on the inviolability of the laws of quantum mechanics. Quantum cryptography is only used to produce and distribute a key, not to transmit any message data. Quantum cryptography is different from traditional cryptographic systems in that it relies more on physics, rather than mathematics, as a key aspect of its security model. Quantum cryptography uses our current knowledge of physics to develop a cryptosystem that is not able to be defeated - that is, one that is completely secure against being compromised without knowledge of the sender or the receiver of the messages. The genius of quantum cryptography is that it solves the problem of key distribution. A user can suggest a key by sending a series of photons with random polarizations. This Sequence can then be used to generate a sequence of numbers. The process is known as quantum key distribution. If the key is intercepted by an eavesdropper, this can be detected and it is of no consequence, since it is only a set of random bits and can be discarded. The sender can then transmit another key. Once a key has been securely received, it can be used to encrypt a message that can be transmitted by conventional means: telephone, e-mail, or regular postal mail[6].

2.4 Selection Of Right Cryptographic Scheme

The selection of right cryptographic technique relies on following constraints:

2.4.1 Time

How much time will be needed for encrypting and decrypting the data and how much time is need to fulfill the pre-requisites before starting an encryption how much time is need to fulfill the pre-requisites before starting an encryption.

2.4.2 Memory

How much memory will be need especially in case of small devices like PDAs, smart cards, RFID tags.

2.4.3 Security

Selected encryption scheme should meet the confidentiality, integrity (authentication, non-repudiation) and availability.

2.4.4 *Nature Of Data*

Nature of data means the communicating information is how much confidential or important. If the information is small in size and not too much important; then any encryption scheme is suitable. If information is highly secret or important then joint hybrid combination of symmetric + asymmetric scheme will be suitable[13].

2.4.5 *Type Of Data*

In case of video data the privacy is more valuable and considerable constraint. If the data is small and in video format the previous described constrains (Time, memory, security) suggest the use of asymmetric scheme but this selection is not sufficient because the third party especially in case of Identity based Public Key Cryptography (ID-PKC) can view the video clip as they have all information (key(s), encrypted data). So in this case the privacy is nothing. That's why the type of data constraint is highly important constraint which should not be neglected in case of right selection of cryptographic scheme. If data type is confidential multimedia (personal video clip) then the symmetric scheme is good but hybrid encryption method (symmetric + asymmetric) can provide all security objectives[12].

2.5 Performance Factors

Various important factors on which performance of cryptographic algorithms depend are:

2.5.1 *Tunability*

It could be very desirable to be able to dynamically define the encrypted part and the encryption parameters with respect to different applications and requirements. Static definition of encrypted part and encrypted parameters limits the usability of the scheme to a restricted set of applications.

2.5.2 *Computational Speed*

In many real-time applications, it is important that the encryption and decryption algorithms are fast enough to meet real time requirements.

2.5.3 *Key Length Value*

In the encryption methodologies the key management is the important aspect that shows how the data is encrypted. The image loss the encryption ratio is based on this key length. The symmetric algorithm uses a variable key length which is of the longer. Hence, the key management is a considerable aspect in encryption processing.

2.5.4 *Encryption Ratio*

The encryption ratio is the measure of the amount of data that is to be encrypted. Encryption ratio should be minimized to reduce the complexity on computation[8].

2.5.5 *Security Issues*

Cryptographic security defines whether encryption scheme is secure against brute force and different plaintext-cipher text attack? For highly valuable multimedia application, it is really important that the encryption scheme should satisfy cryptographic security. In our analysis we measure cryptographic security in three levels: low, medium and high[9].

Table 1. Comparison table for various cryptographic algorithms

Algorithm	Key Size(s)	Speed	Speed Depends On Key?	Security
DES	56 bits	Slow	Yes	Insecure
3DES	112/168 bits	Very Slow	No	Moderately secure
AES	128, 192, 256 bits	Fast	Yes	Secure
BLOW-FISH	32-448 bits	Fast	No	Believed secured, but less attempted crypt-analysis than other algorithms
RC4	256 bytes	Very Fast	No	Moderately secure
RSA	1024 bits and above	Fast	Yes	Secure

2.6 Trend In Cryptographic Protocol

In this section we describe what we see as some of the emerging trends in cryptographic protocols. These trends present new challenges to protocol analysis

2.6.1 *Greater Adaptability and Complexity:*

Probably one of the most obvious trends is the increasing different kinds of environments that protocols must interoperate with. As networks handle more and more tasks in a potentially hostile environment, cryptographic protocols take on more and more responsibilities. As networking becomes more widespread, and different platforms must interoperate, we see protocols such as the Internet Key Exchange (IKE) protocol that not only must agree upon encryption keys, but on the algorithms that are to use the keys. Or, we may see protocols such as SET that must be able to process different types of credit card transactions.One way of attempting to meet this challenge is to increase the complexity of the protocol. This of course, not only makes verification but implementation more difficult as well, and as a result there is always resistance to this approach. However, the tendency to greater complexity will always be there, and it will ultimately have to be met at least part of the way by anyone who is attempting to perform any type of security analysis[7].

2.6.2 *Adoption of New Types of Cryptographic Primitives*

In general, it is it is accepted that a conservative approach to algorithm is best when designing cryptographic protocols;

only tried and true algorithms should be used. But, as the field matures the number of algorithms that are considered to have received enough scrutiny has increased. Moreover, as computing power increases, algorithm that were once considered prohibitively expensive have become easier to implement, while others, such as DES, are widely regarded as no longer providing adequate security[20].

2.6.3 New Types of Threats:

In the early years of computer security, much of the threat analysis was hypothetical, and focused on attacks in which there would be a clear(usually monetary) gain for the attacker. Now, with more experience, we see that there are other types of attacks, most of them related to denial of service, that can prevent a network from fulfilling its functions. Many denial of service attacks can be countered by good resource management. But sound protocol design can do much to help, for example by keeping a responder from committing its resources to communicating with an initiator until it has adequate assurance that it knows who it's talking to. This can be a delicate problem however, since many of the techniques used for authentication themselves require commitment of resources, and since the decision of how much resources to commit, and when, can be very implementation-dependent. Successful analysis will depend to some extent on the ability to compare the resources expended by an attacker to the resources expended by a defender.

Other threats, such as traffic analysis, focus on problems that are not really an issue until adequate cryptographic protection for communication secrecy has already been attained. Protection against traffic analysis is one of these. Even when encryption is used source and destination of message traffic is not hidden, and it can be possible for an observer to learn much from this alone. A number of different systems have been developed that attempt to solve this problem with varying degrees of completeness. However, without some ability to evaluate and compare the degree of protection offered by these systems, it is difficult to assess what amount and kind of security they offer. Such analysis methods should take statistical techniques into account, since much traffic analysis depends on statistical analysis[19].

A somewhat different type of threat emerges when we look at electronic commerce protocols. In this type of protocol, the parties involved participate in a transaction that results in certain levels of payoff to each principal involved. Moreover, the protocol may either depend upon or try to guarantee liveness or fairness properties as well as safety properties. A principal may try to cheat by trying to increase its payoff at the expense of those of other parties, but will not engage in behavior that will result in a lowering of its payoff, or put it at a disadvantage with respect to the others[15].

3. CONCLUSION

Cryptography is an emerging technology which is important for network security. Some well-known cryptographic algorithms have been analyzed in this paper to demonstrate the basic differences between the existing encryption techniques. Regardless of the mathematical theory behind an algorithm, the best algorithm are those that are well-known and well-documented because they are well-tested and well-studied. In-fact time is the only true test of good cryptography, any cryptographic scheme that stays in use year after year is most likely good one. The strength of cryptography lies in the choice of the key; longer key resist attack better than shorter keys. No one can guarantee 100% security. But we can work toward 100% risk acceptance. Fraud exists in current commerce systems: cash can be counterfeited, checks altered, credit card numbers stolen. A good cryptographic system strikes a balance between what is possible and what is acceptable. Thus considerable research effort is still required for secured communication.

4. REFERENCES

[1] William Stallings "Network Security Essentials (Applications and Standards)", Pearson Education, 2004.

[2] W. Stallings. "Cryptography and Network Security", Prentice Hall, 1995.

[3] National Bureau of Standards, "Data Encryption Standard," FIPS Publication 46, 1977.

[4] E. Thambiraja, G. Ramesh, Dr. R. Umarani, "A Survey on Various Most Common Encryption Techniques" International Journal of Advanced Research in Computer Science and Software Engineering, VOL. 2, Issue 7 July 2012, Page 226-233.

[5] Sumedha Kaushik, Ankur Singhal, "Network Security Using Cryptographic Techniques" International Journal of Advanced Research in Computer Science and Software Engineering, VOL.2, Issue 12 December 2012, Page 105-107.

[6] Vishwa gupta, Gajendra Singh, Ravindra Gupta, "Advance cryptography algorithm for improving data security" International Journal of Advanced Research in Computer Science and Software Engineering, VOL.2, Issue 1 January 2012.

[7] Nagamalleswara Rao. Dasari, Vuda Sreenivasarao, "PERFORMANCE OF MULTI SERVER AUTHENTICATION AND KEY AGREEMENT WITH USER PROTECTION IN NETWORK SECURITY" International Journal on Computer Science and Engineering, VOL.2, Issue 05 2010, Page 1705-1712.

[8] AL. Jeeva, Dr. V. Palanisamy, K. Kanagaram, "COMPARATIVE ANALYSIS OF PERFORMANCE EFFICIENCY AND SECURITY MEASURES OF SOME ENCRYPTION ALGORITHMS" International Journal of Engineering Research and Applications (IJERA), VOL.2, Issue 3,May-Jun 2012, Page 3033-3037.

[9] G. Ramesh, R. Umarani, "Performance Analysis of Most Common Encryption Algorithms on Different Web Browsers "I.J. Information Technology and Computer Science, Issue Nov 2012, Page 60-66.

[10] Zirra Peter Buba & Gregory Maksha Wajiga "Cryptographic Algorithms for Secure Data Communication "in International Journal of Computer Science and Security IJCSS, Volume no 5, Issue 2.

[11] Daemen, J., and Rijmen, V. "Rijndael: The Advanced Encryption Standard." Dr. Dobb's Journal, March 2001.

[12] Pranay Meshram,Pratibha Bhaisare, S.J.Karale,",comparative study of selective encryption algorithm for wireless adhoc network" ,IJREAS Volume 2, Issue 2 , in International Journal of Research in Engineering & Applied Sciences.

[13] Yudhvir Singh, Yogesh Chaba, ―Information Theory test based Performance Evaluation of Cryptographic Techniques , International Journal of Information

Technology and Knowledge Management, Vol 1,No.2,2008 , pp. 475-483.

[14] A. Menezes, P. van Oorschot, S. Vanstone, Algorithm 9.53 Secure Hash Algorithm - revised (SHA-1), Handbook of Applied Cryptography, CRC Press, 1997.

[15] M. Merkow, J. Breithaupt, J. Breithaupt, The Complete Guide to Internet Security, AMACOM, 2000.

[16] Punita Mellu & Sitender Mali, "AES: Asymmetric key cryptographic System" International Journal of Information Technology and Knowledge Management, 2011, Vol, No. 4 pp. 113-117.

[17] Suhaila Orner Sharif, S.P. Mansoor, ―"Performance analysis of Stream and Block cipher algorithms", 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), 2010.

[18] Murat Fiskiran, Ruby B. Lee, "Workload Characterization of Elliptic Curve Cryptography and other Network Security Algorithms for Constrained Environments" IEEE International Workshop on Workload Characterization, 2002. WWC-5. 2002.

[19] Othman O. Khalifa, MD Rafiqul Islam, S. Khan and Mohammed S. Shebani,"Communication Cryptography", 2004 RF and Microwave Conference, Oct 5-6, Subang, Selangor, Malaysia.

[20] Mohamed A.Haleem, Chetan N. Mathur, R. Chandramouli, K. P. Subbalakshmi, "Opportunistic Encryption: A tradeoff between Security and Throughput in Wireless Network" IEEE Transactions on Dependable and secure computing, vol. 4, no. 3.