Cryptography: The Sciene of Secure Communication

Jangala. Sasi Kiran M.Anusha, A.Vijaykumar, M.Kavya
Department of Computer Science and Engineering Vidya Vikas Institute of Technology, Chevella, R.R. Dt –Telengana, India - 501503
Nalla Malla Reddy Engineering College, Ghatkesar, R.R.Dist, T.S – India – 500088

Abstract
Day by day network and internet applications is becoming very popular. Sensitive information requires security and safety measures. Security is the most challenging aspect in the internet and network applications. Encryption algorithm provides the necessary protection against the data intruders' attacks by converting information from its normal form into an unreadable form. The majority of current web authentication is built on username/password. And the password replacement offers more security, but it is very much difficult to use and expensive to deploy. Security of data can be done by a technique called cryptography. So everybody say that cryptography is a developing technology, which is important for network security. Cryptography in the past was used in keeping military information secure to protect the national security. However, the use was limited. At present, the range of cryptography applications have been expanded a lot in the modern area after the development of communication means; cryptography is essentially required to ensure that data are protected against penetrations and to prevent the practice of spying. Cryptography is a developing technology, which is important for network security. Study on cryptography is still in its developing stages and a considerable research effort is still required for secured communication. This paper talks about the state of the art for a broad range of cryptographic algorithms that are used in networking applications.

KEYWORDS
Network security, cryptography, symmetric encryption, asymmetric encryption and Caesar table.

I. Introduction

Computer and network security is a new and fast moving technology and as such, is still being well-defined. When considering the desired learning outcomes of such a course, one could argue that a network security analyst must be capable of analyzing security from the business perspective in order to carryout recent security act, and from the technical view in order to understand and select the most appropriate security solution. Network security [16] originally focused on algorithmic aspects such as encryption and hashing techniques. While these concepts very often change, these skills alone are insufficient to protect computer networks. As crackers troubled away at networks and systems, courses occurred that emphasized the latest attacks. Currently, many gurus believe that to train people to secure networks, they must also learn to think like a cracker [3][14]. The following background information in security helps in making correct decisions: Attack Recognition, Encryption techniques, Network Security Architecture, Protocol analysis, Access control list and vulnerability. For Network security cryptography is present. In cryptography [13] data that can be read and understood without any special measures is called plaintext or clear text. The method of coverup plaintext in such a way as to hide its substance is called encryption. Encrypting plaintext results in unreadable data called cipher text. We use encryption to protect the information is hidden from anyone for whom it is not projected, even those who can see the encrypted data. The process of reversing cipher text to its original plain text is called decryption.

In cryptography three types of algorithms are present.

- Symmetric key algorithm,
- Asymmetric key algorithm
- Hash function.

Cryptographic algorithms play a major role for data user security. As the complexity of algorithm is high the risk of breaking the original plaintext from that of cipher text is less. Greater complexity means greater security. Encryption is the process of encoding plain text into cipher text (secure data).Decryption is the revoking of the encryption process by which cipher text is converted to plain text, as shown in figure (1).

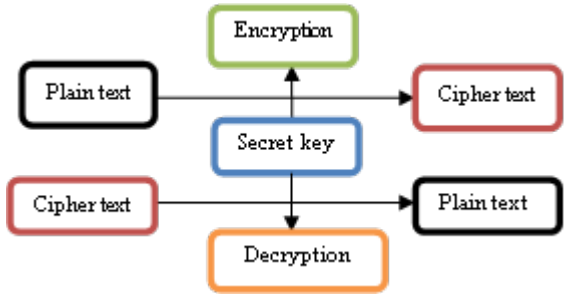

Figure 1: The Encryption and Decryption process by using the same key (Symmetric Key Cryptographic Algorithm).

Manuscript received April 5, 2016
Manuscript revised April 20, 2016

II. Literature Survey

C.Sanchez-Avila et.al analyzed the structure and design of Rijndael cipher (new AES), remarking its main advantages and confines, as well as its similarities and dissimilarities with DES and Triple-DES. Finally, a performance comparison among new AES, DES and Triple-DES for different microcontrollers has been carried out, showing that new AES have a computer cost of the same order than the one needed by T-DES [17]. PunitaMeelu et.al presented the fundamental mathematics behind the AES algorithm along with a brief description of some cryptographic primitives that are commonly used in the field of communication security since AES provides better security and has less implementation complexity and has emerged as one of the strongest and most efficient algorithms in existence today. It also includes several cyber issues, development of cipher as well as the analysis of AES security aspects against different kinds of attacks including the countermeasures against these attacks and also highlighted some of the important security issues of AES algorithm. The future work can be done for the distribution of secret key that is considered as a critical issue of AES like other symmetric encryption algorithm [15].Susan et.al concluded that the Security field is a new, fast moving profession. A focus on security stabilizes course material, reduces worry about student hacking, and helps to provide students that skills necessary to become security analysts. It also defines the set of skills desired by Network Security analysts as network Security skills emphasize legal foundations, business practices,attack recognition, network optimization and describes active learning exercises that assist the students in learning these important skills. This actually summarize all the skills relating to network security, and discussed active learning drills that assist students in learning these important skills. Main focus was on security information skills that are to be used in securing the network [8]. Aameer Nadeem et.al presented, performance of 4 secret key algorithms (DES, 3DES, AES, Blowfish) were compared by encrypting input files of various contents and sized on different hardware program. The algorithms have been implemented in a regular language, using their standard qualifications, to allow a fair evaluation of execution speeds. Pentium-II having frequency 266MHz and Pentium-IV with 2.4 MHz machine (running Windows XP OS) are the basis for time measurement with their goal to measure the encryption times of considered algos.[1].
Mohamed A. Haleem et.al [9] discussed a tradeoff between security and throughput in wireless network where Markov Decision Process and OFDM (orthogonal frequency Division Multiplexing) helped out to determine channel estimation, tracking and prediction. It also uses channel opportunities (acceptable signal to noise ratio) to maximize the throughput. It defines mathematical models to confine the security-throughput trade-off, adversary models and their effects, joint optimization of encryption and modulation (single and multirate), the use of Forward Error Correcting (FEC) codes to protect encrypted packets from bit errors, and simulation results for Rijndael cipher. Othman O. Khalifa et.al [18] discussed basic concepts, characteristics, and goals of various cryptography. In today's information age, communication plays an important role which is contributed to growth of technologies therefore privacy is needed to assure the security that is sent over communication media.Kyung Jun Choi et.al [6] investigated various cryptographic algorithms suitable for wireless sensor network based on MICAz-type motes in which MD5 and RC4 showed best performance in terms of power dissscipation and in terms of cryptographic processing time used.

III. Background and Goals

In this section we will give background information about the ongoing advance of browser-side cryptographic functionalities. Then we will identify properties mandatory to provide web masters and users with a mutual secure and practical authentication.

3.1. Browser Cryptographic Functionalities:

3.1.1 Browsers cryptographic libraries – To support the HTTPS protocol, all modern browsers provide support to some cryptographic operations (e.g. generating the client random certificate and then verify message in the Handshake phase of SSL/TLS protocol [5]). For example, one of the main cryptographic libraries is Network Security Services [10] which is a set of open source libraries designed to support cross-platform development of security-entitled applications.
3.1.2 JavaScript cryptography- In recent discussion of JavaScript cryptography, a notorious issue has been whether or not JavaScript should ever be used for cryptography. On the one hand, the author in [11] strongly argues that it is totally dangerous to use JavaScript cryptography inside the browser. However, the authors in [4], [12] argue that claims such as JavaScript crypto isn't a serious research area and is very bad for the improvement of security.
3.1.3 Crypto API - W3C has created the Web Cryptography Working Group to develop a re-commendation-track document that defines an API that lets developers implement secure application protocols on the level of Web applications, including message privacy and authentication services, by exposing trusted cryptographic primitives from the browser.
3.1.4 Certificate and password managers - The five most popular browsers (Firefox, Chrome, Internet Explorer, Safari, and Opera) provide certificate organization

services. Using this built-in functionality, users can display information about the installed certificate including personal and authority certificates that the browser trusts, and perform all the important certificate management actions (import, export, delete).

3.2 Design Requirements:

Learning from previous proposition boundaries and the ongoing advance in browser-side functionalities, we identify properties required to provide web masters and users with a common secure and practical web user authentication.

3.2.1 Security - It will be built on a mechanism that solves password security weaknesses User authentication qualifications should be stored securely and even with a database compromise, Strong*Auth* should not leak any information.

3.2.2 Usability - It will provide a similar user experience to the conventional password-based authentication. Even the most inexpert user can authenticate without even noticing the background tasks handle by the browser.

3.2.3 Adaptability - Users are unwilling for innovation that alters their behavior [2].

3.2.4 Deployability - Cryptographic algorithms will require minimal changes in the browser and the web application, and no additional hardware will be required.

3.2.5 Cost-efficiency - Cost is always a factor that plays a decisive role in real-world scenario. Therefore cryptographic algorithms will not involve superfluous cost per user, but instead be open source to implement and deploy by using existing technologies and standards.

3.2.6 Browser support - It will be implemented as part of the browser (core component or extension) to provide adequate security and functionality guarantees.

IV. Symmetric and Asymmetric Cryptography

4.1 Symmetric cryptography:

Encryption is the safest and the strongest way in securing data. Definitely, it is the most frequent one. Encryption systems are divided into two main types symmetric and asymmetric. Symmetric encryption is known as secret key or single key, The receiver and sender uses the same key to encrypt the data to decrypt the message,. This system was the only system used before discovering and developing the public key. A safe way of data transfer must be used to moving the secret key between the sender and the receiver in symmetric encryption. Figure 2 shows how the system works. Symmetric encryption occurs either by substitution transposition technique, or by a mixture of both. replacement maps each plaintext element into cipher text element, but transposition transposes the positions of plain text elements.

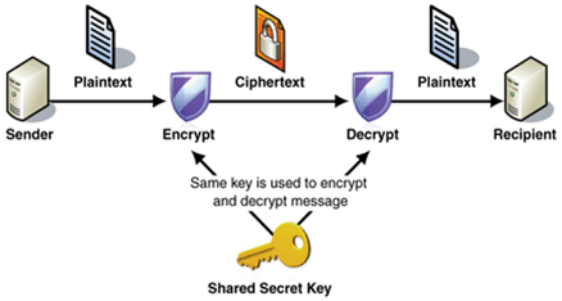

Figure 2: Simplified model of conventional encryption

Cipher is the algorithm that is used to transform plaintext to cipher text, this method is called encryption or enciphers (encode), in other words, it's a mechanism of converting readable and understandable data into "worthless" data, and it is represented as follows-

$$C = E_K(P) \quad (1)$$

Where E(k) is the encryption algorithm using key k.

The opposite of cipher mechanism is called decipher (decode) that is the algorithm which recovers the cipher text, this method is called decryption, in other words it's the mechanism of converting "meaningless" data into readable data.

$$P = D_{(K^{-1})}(C) \quad (2)$$

The common simplified cipher algorithm which assigns each character of plaintext into numerical value is called Caesar cipher, its sums the key value to the numerical value of plaintext character, and then assigns the rest of the division by modular value into cipher text character, where the modular value is the max numerical value plus one [19], The mathematical model of Caesar cipher is

At encryption side $E_n(x)=(x+n) \bmod p$ (3)

At decryption side: $E_n(x)=(x-n) \bmod p$ (4)

Where x is the plaintext character and x is shift value, the following example illustrates Caesar cipher model and the Caesar table will be:

Table 1:Caesar Table

A	B	C	D	E	F	G	H	I	J	K	L	M	N
0	1	2	3	4	5	6	7	8	9	10	11	12	13

O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25

Example:

Let the plaintext message is "TELANGANA" and the key value=12, and use the simplest symmetric encryption algorithm, which called "Caesar cipher",

Plaintext	Encryption Process	Cipher Text
T→19	(19+12)mod 26	5→F
E→4	(4+12)mod 26	16→Q
L→11	(11+12)mod 26	23→X
A→0	(0+12)mod 26	12→M
N→13	(13+12)mod 26	25→Z
G→6	(6+12)mod 26	18→S
A→0	(0+12)mod 26	12→M
N→13	(13+12)mod 26	25→Z
A→0	(0+12)mod 26	12→M

The cipher text which arrives to the receiver is "FQXMZSMZM ", and the cipher text is entered into decryption process in the receiver to decrypt the text as follow:

Cipher Text	Decryption Process	Plaintext
F→5	(5-12)mod 26	19→T
Q→16	(16-12)mod 26	4→E
X→23	(23-12)mod 26	11→L
M→12	(12-12)mod 26	0→A
Z→25	(25-12)mod 26	13→N
S→18	(18-12)mod 26	6→G
M→12	(12-12)mod 26	0→A
Z→25	(25-12)mod 26	3→N
M→12	(12-12)mod 26	0→A

Symmetric encryption has many advantages more than asymmetric. Firstly, it is faster since it doesn't use much time in data encryption and decryption. Secondly, it is easier than asymmetric encryption in secret key generation. However, it has some disadvantages, for example key distribution and sharing of the secret key between the sender and the receiver, also symmetric key encryption incompleteness, since some application like authentication can't be fully implemented by only using symmetric encryption [7].

4.2 Asymmetric Cryptography

In 1976 Diffie-Helman invented new encryption technique called public key encryption or asymmetric encryption; Asymmetric encryption is the opposite of symmetric encryption in safety, since it doesn't require sharing the secret key between the sender and the receiver. And this is the main difference between symmetric and asymmetric encryption, the sender has the public key of the receiver. Because the receiver has his own secret key which is really difficult or unfeasible to know through the public key, no shared key is needed; the receiver is responsible for establishing his private and public key, and the receiver sends the public key to all senders by any channel he needs, even unsecured channels to send his public key. Asymmetric key can use either the public or secret key to encrypt the data. Also it can use any of the keys in decryption, asymmetric encryption can be used to implement the authentication and non-repudiation security services, and also it can be used for digital signature and other application that never be implemented using symmetric encryption. Figure.3 shows how the system works.

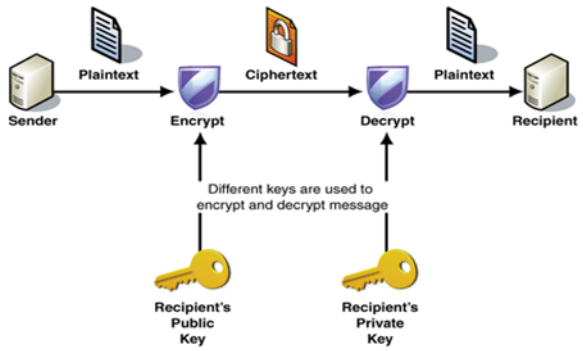

Figure 3: Simplified Model of Asymmetric Encryption

Asymmetric encryption is slower and very complicated in calculations than symmetric encryption. Therefore, asymmetric encryption deals with plaintext as a group of numbers which are manipulated in mathematics, while the plaintext in symmetric encryption deal as group of symbols and characters, the encryption process may permute these symbols, or may substitute one symbol by another. So the nature of the data determines the system of encryption type. And every system has its own uses. For example, asymmetric encryption may be used in authentication or in sending secret key for decryption. To understand asymmetric encryption, lets us take RSA model which is an example on asymmetric encryption, RSA model main steps-

RSA Model Steps:

- Each user generates a public/private key pair by selecting two large primes at random p,q.
- Computing modular value n=p×q
- Calculating the Euler's function Φ(n)=(p-1)×(q-1).
- Selecting at randomly the public encryption key e, where, 1<e<Φ (n), and e is a prime relative to the Φ (n).
- Solving the following equation to find private decryption key, d, e×d=1 mod Φ (n), and 0≤d≤n.
- Publishing their public encryption key: $P_k = (e, n)$.
- Keeping secret private decryption key: $p_r = (d, n)$.
- At the encryption side the sender uses encryption mathematical equation .C=$p^e mod\ n$.
- At the decryption side the receiver uses decryption mathematical equation .P=$c^d mod\ n$.

Example

Let a part of the plaintext message be "Telangana", then the RSA key generation process is:

Select two prime numbers: p=3 & q=11

- Computing n=p×q=3×11=33
- Computing Φ (n) = (p-1) × (q-1) =2X10=20.
- Selecting e: gcd (e, 20) =1; choose e=7.
- Determining d:d×e=1 mod 20 and d×7=1mod 20 we take d=3 i.e (3×7)mod 20 =1 so d=3 Publishing public key $p_k = (7,33)$
- Keeping private key secret $p_r = (3,33)$

The encryption process and decryption process then is applied to previously calculated parameters as follows

Plain text	Encryption Process
T→19	19^7 mod 33=13
E→ 04	04^7 mod 33=16
L→11	11^7 mod 33=11
A→00	00^7 mod 33=00
N→ 04	04^7 mod 33=16
G→06	06^7 mod 33=30
A→00	00^7 mod 33=00
N→ 04	04^7 mod 33=16
A→00	00^7 mod 33=00

The cipher text will arrive the receiver, and at the receiver the cipher text will be entered into decryption process to decrypt the text as follows-

Decryption process	Plain Text
13^3mod 33=19	19→T
16^3mod 33=04	04→E
11^3mod 33=11	11→ L
00^3mod 33=00	00→A
16^3mod 33=13	13→N
30^3mod 33=06	06→G
00^3mod 33=00	00→A
16^3mod 33=13	13→N
00^3mod 33=00	00→A

The mathematical model for symmetric and asymmetric encryption consists of key, encryption and decryption algorithm and powerful secured channel for transmitting the secrete key or any channel for transmitting the public key from the sender to the receiver, the mathematical model similar to equations.

At Encryption Side: $C=E_k(P)$

At Decryption Side: $P=D_k(C)$

V. Conclusion

Network Security is the most vital component in information security because it is responsible for securing all information passed through networked computers. Network security consists of the provisions made in an underlying computer network infrastructure, policies adopted by the network administrator to protect the network and the network-accessible resources from unauthorized access, and consistent and continuous monitoring and measurement of its effectiveness (or lack) combined together. We have studied various cryptographic techniques to increase the security of network.

Acknowledgements

I would like to express my cordial thanks to Sri. CA. Basha Mohiuddin, Chairman, Smt. Rizwana Begum-Secretary and Sri. Touseef Ahmed-Vice Chairman, Dr.M.Anwarullah, Principal - Vidya Group of Institutions, Hyderabad for providing moral support, encouragement and advanced research facilities. Authors would like to thank the anonymous reviewers for their valuable comments. And they would like to thank Dr.V. Vijaya Kumar, Anurag Group of Institutions for his invaluable suggestions and constant encouragement that led to improvise the presentation quality of this paper.

References

[1] Aameer Nadeem, Dr. M.Younus Javed, ―A performance comparison of data Encryption Algorithm‖, Global Telecommunication Workshops, 2004 Globe Com Workshops 2004, IEEE.

[2] C. Herley, "So long, and no thanks for the externalities: the rational rejection of security advice byusers," in Proceedings of the workshop on New security paradigms workshop, 2009, pp. 133–144.

[3] Computer Network Defense Course (CNDC), Army Reserve Readiness Training Center, Fort McCoy WI, http:/arrtc.mccoy.army.mil, Jan. 2004.

[4] "How to improve JavaScript cryptography." : http://hellais.wordpress.com/2011/12/27/how-to improve-java script-cryptography/.

[5] IETF, "RFC 5246 - The Transport Layer Security (TLS) Protocol Version 1.2.".: http://tools.ietf.org/html/rfc5246

[6] Kyung Jun Choi, John –In Song, "Investigation of feasible cryptographic Algorithm For wireless sensor network", International conference on ICACT Feb 20-22, 2006

[7] K .Thomas, : " The Myth Of The Skytale ". Taylor & Francis, (1998), Vol (33), pp: 244-260.

[8] Like Zhang, Gregory B. White, ―Anomaly Detection for Application Level Network Attacks Using Payload Keywords‖, Proceedings of the 2007 IEEE Symposium on Computational Intelligence in Security and Defense Applications (CISDA 2007).

[9] 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. 4.

[10] Mozilla, Overview "of NSS MDN: https://developer.mozilla.org/en-US/docs/Overview of_NSS.

[11] Matasano, "Javascript Cryptography Considered Harmful," 2011: http://www.matasano.com/articles/ javascript-cryptography/.

[12] N. Kobeissi, “Thoughts on Critiques of JavaScriptCryptography.”: http://log.nadim.cc/?p=33.
[13] 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.
[14] P.Mateti, “ A Laboratory-Based Course on Internet Security”, Proc. of 34th SIGCSE Technical Symp, on Computer Science Education, ACM, 2003, 252-256.
[15] Punita Mellu, et al ―AES: Asymmetric key cryptographic System‖, International Journal of Information Technology and Knowledge Management, 2011, Vol, No. 4 pp. 113-117.
[16] Susan J Lincke, Andrew Hollan, “Network Security: Focus on Security, Skills, and Stability”, Proceedings of 37th ASEE/IEEE Frontiers in Education Conference.
[17] Sanchez-Avila, C. Sanchez-Reillol, R, ―The Rijndael block cipher (AES proposal): A comparison with DES‖, 35th International Conference on Security Technology 2001, IEEE.
[18] 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.
[19] W .Stallings, “Cryptography and network security, Principles and practices ", Fourth Edition. Pearson Prentice Hall, (2006):, USA.

AUTHOR PROFILE

J. Sasi Kiran Graduated in B.Tech [EIE] from JNTU Hyd. He received Masters Degree in M.Tech [CSE] from JNT University, Hyderabad. He received Ph.D degree in Computer Science from University of Mysore, Mysore. At Present he is working as Professor in CSE and Dean – Administration in Vidya Vikas Institute of Technology, Chevella, R.R. Dist Telangana State, India. His research interests include Image Processing, Data Mining and Network Security. He has published 39 research papers till now in various National, International Conferences, Proceedings and Journals. He has received best Teacher award twice from Vidya Group, Significant Contribution award from Computer Society of India and Passionate Researcher Trophy from Sri. Ramanujan Research Forum, GIET, Rajuhmundry, A.P, India.

M. Anusha Graduated in B.Tech [CSE] from JNTU Hyd. She received Masters Degree in M. Tech from JNTU Hyd. Her Interested areas are Wireless Sensor Networks, Computer Organization, Network Security and Cryptography. Currently, she is working as an Associate Professor in Vidya Vikas Institute of Technology. She has published research papers in various National, International conferences, proceedings and Journals.

A.Vijaya Kumar completed his M.Tech from sathyabama university in 2007. Presently he is working as an Associate Professor in the IT Dept in Nalla Malla Reddy Engg. College, Hyderabad. His research interests include Network Security, Data Mining & Image Analysis. He has published research papers in various National, International conferences, proceedings and Journals.

M. Kavya Graduated in B.Tech [CSE] from JNTU Hyd. She received Masters Degree in M.Tech from CBIT, HYD. Her Interested areas are Digital Image Processing and Artificial Intelligence. Currently, she is working as an Assistant Professor in Vidya Vikas Institute of Technology. She has published research papers in various National, International conferences, proceedings and Journals.