International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 4, Issue 1, pp 32-37, January-2020

# Cryptography

[1]Pranali Pund, [2]Yamini Bhele, [3]Prof. M.R.Khan

[1,2]PG Student, Final Year MCA, Department of MCA, Vidyabharti Mahavidayalaya, Amravati(M.S), India
[3]Professor, Department of MCA, Vidyabharti Mahavidayalaya, Amravati(M.S), India

***Abstract* - Network and Internet applications are becoming more and more popular every day, sensitive information requires security and safety measures. Security is the most difficult aspect of Internet and network applications. The encryption algorithm provides the necessary protection against hacker attacks by converting information from its normal form to an unreadable form. Most of the current web authentication is based on username / password. and password replacement is safer, but very difficult to use and expensive to deploy. Data security can be done using a technique called cryptography. Cryptography is therefore an evolving technology that is important for network security. In the past, national security cryptography was used to protect military information. However, use was limited. At present, the spectrum of cryptographic applications in the modern field has been considerably widened after the development of the means of communication; Cryptography is basically necessary to protect data from intrusion and prevent spying. Cryptography is an evolving technology that is important for network security. The study of cryptography is still in the development stage and considerable research is still needed for secure communication. This article describes the state of the art for a wide range of cryptographic algorithms used in network 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 leaming outcome 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 act and from the technical view in order to understand and select the most appropriate security solution. Network security originally focused on algorithmic aspect such as encryption and hashing techniques. While these concepts very often change, these skills alone are insufficient to protect computer networks.

As crackers swirled around networks and systems, courses were held on the latest attacks. Many gurus now think they need to learn how to train people on secure networks to think like a hacker. The following basic security information helps you make the right decision: attack detection, encryption techniques, network security architecture, protocol analysis, access control list, and vulnerability. Cryptography is available for network security. In cryptography, data that can be read and understood without special measures is called plain text or plain text. The method of concealing plain text in such a way that its substance remains hidden is called encryption. Encryption of plain text leads to unreadable data, known as encrypted text. We use encryption to protect the information of anyone for whom it was not intended, including those who may see the encrypted data. Reversing the ciphertext 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 an important role in the security of data users. The complexity of the algorithm being high, there is less risk of separating the original plain text from that of the encrypted text. More complexity means more security. Encryption is the process of encoding plain text into encrypted text (secure data). Decryption is the removal of the encryption process by which encrypted text is converted to plain text, as shown in Figure (1).

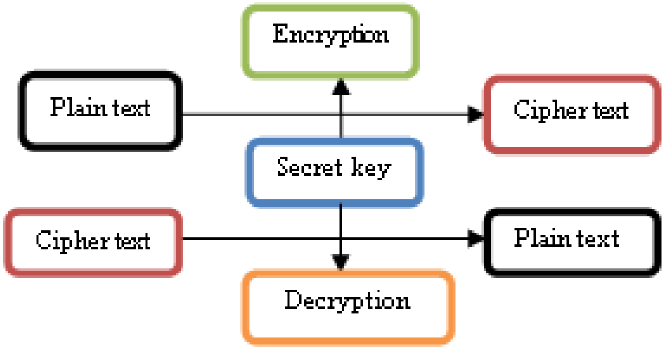

**Figure 1: The Encryption and Decryption process by using the same key (Symmetric Key Cryptographic Algorithm)**

## II. Literature Survey

C. Sanchez-Avila et al. analyzed the structure and design of Rijndael encryption (new AES) and found the main advantages and limitations as well as the similarities and differences with DES and Triple-DES. Finally, a performance comparison between the new AES, DES and triple-DES was carried out for different microcontrollers, which shows that the IT costs for the new AES are of the same order of magnitude as for the T-DES.

Punita Meelu et al. Introduced the basic math behind the AES algorithm as well as a brief description of some of the basic cryptographic elements that are commonly used in communications security, as AES provides better security and less complexity of implementation, and has become one of the most powerful and efficient algorithms that exist today. It also covers various cyber issues, developing encryption and analyzing AES security aspects against various types of attacks, including countermeasures against these attacks, and also highlighted some important security aspects of the AES algorithm. Future work can be done on the distribution of secret keys, which, like other symmetric encryption algorithms, is considered a critical problem by AES. It also defines the skills required for network security and is a new and rapidly evolving profession. The focus on security stabilizes the course material, reduces the fear of student hacking and helps students acquire the skills required for analysts, as network security skills focus on the legal underpinnings, business practices, attack detection and network optimization, and describe active learning exercises that help students learn to help these important skills. This article summarizes all of the network security skills and presents active learning exercises that help students learn these important skills. The main focus was on the security information to be used to secure the network.

Aameer Nadeem et al. presented that the performances of 4 secret key algorithms (DES, 3DES, AES, Blowfish) have been compared by encrypting input files with different contents and sizes on different hardware programs. The algorithms have been implemented using their standard qualifications in regular language to allow a fair assessment of execution speeds. The Pentium-II with a frequency of 266 MHz and the Pentium-IV with a 2.4 MHz computer (under Windows XP) constitute the basis of time measurement in order to measure the encryption times of the persons concerned.

Mohamed A. Haleem al discussed a compromise between security and speed in wireless networks in which the Markov decision process and the OFDM (Orthogonal Frequency Division Multiplexing) helped to determine the estimation, monitoring and channel prediction. Channel options are also used (acceptable signal-to-noise ratio) to maximize throughput. He defines mathematical models

Limit the trade-off between security throughput, opposing models and their effects, joint optimization of encryption and modulation (single and multiple rates), use of FEC (Forward Error Correcting) codes to protect encrypted packets against bit errors and simulation results for Rijndael encryption.

Othman O. Khalifa et al. discussed the basic concepts, properties and objectives of various cryptography. In today's information age, communication plays an important role that contributes to the growth of technology. Data protection is therefore necessary to ensure the security that is sent via communication media.

Kyung Jun Choi and. studied various cryptographic algorithms that are suitable for wireless sensor networks based on MICAz patterns, in which MD5 and RC4 have given the best results in terms of power dissipation and 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). For example, one of the main cryptographic libraries is Network Security Services 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 strongly argues that it is totally dangerous to use JavaScript cryptography inside the browser. However, the authors in 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.

### *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 system is 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.

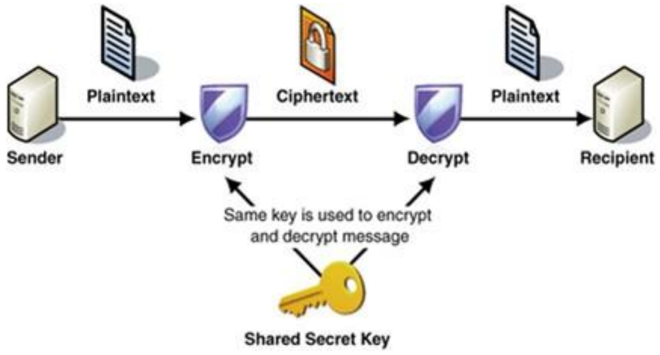

**Figure 2: Simplified model of conventional encryption**

***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 asfollows-

$$CC = EE(\mathbf{P}) \qquad \textbf{(1)}$$

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.

$$P=(\boldsymbol{KK}-\mathbf{11})C \qquad \textbf{(2)}$$

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 , The mathematical model of Caesar cipheris

$$\text{Atencryptionside}\mathit{EE}_{nn}\mathbf{(x)=(x+n)modp} \qquad \textbf{(3)}$$

$$\text{Atdecryptionside:}\mathbf{(x)=(x-n)modp} \qquad \textbf{(4)}$$

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

**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 | CipherText |
|---|---|---|
| T→19 | (19+12)mod26 | 5→F |
| E→4 | (4+12)mod26 | 16→Q |
| L→11 | (11+12)mod26 | 23→X |
| A→0 | (0+12)mod26 | 12→M |
| N→13 | (13+12)mod26 | 25→Z |
| G→6 | (6+12)mod26 | 18→S |
| A→0 | (0+12)mod26 | 12→M |
| N→13 | (13+12)mod26 | 25→Z |
| A→0 | (0+12)mod26 | 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)mod26 | 19→T |
| Q→16 | (16-12)mod26 | 4→E |
| X→23 | (23-12)mod26 | 11→L |
| M→12 | (12-12)mod26 | 0→A |
| Z→25 | (25-12)mod26 | 13→N |
| S→18 | (18-12)mod26 | 6→G |
| M→12 | (12-12)mod26 | 0→A |
| Z→25 | (25-12)mod26 | 3→N |
| M→12 | (12-12)mod26 | 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.

### 4.2 Asymmetric Cryptography

In 1976, Diffie-Helman invented a new encryption technique called public key encryption or asymmetric encryption. For security reasons, asymmetric encryption is the opposite of symmetric encryption, since the secret key does not have to be shared between the sender and the recipient. And this is the main difference between symmetric and asymmetric encryption, the sender has the recipient's public key. Since the recipient has their own secret key, which is difficult or impossible to determine using the public key, no common key is required. The recipient is responsible for establishing their private and public key for all senders on any channel they need, including unsecured channels, to send their public key. The asymmetric key can use the public key. The asymmetric key can use the public or secret key to encrypt the data. In addition, any of the keys can be used in decryption, asymmetric encryption can be used to implement security services for authentication and non-rejection, and it can also be used for digital signatures and d other applications that are never implemented with symmetric encryption. Figure 3 shows how the system works.

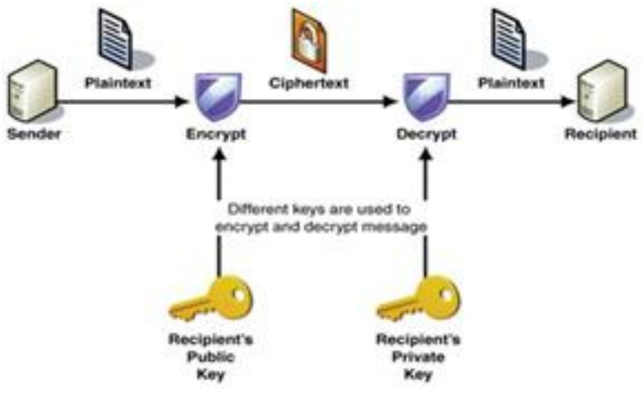

**Figure 3: Simplified Model of Asymmetric Encryption**

Asymmetric encryption is slower and the calculation is very complicated than symmetric encryption. As a result, asymmetric encryption treats plain text as a group of numbers manipulated in math, while in symmetric encryption, plain text treats the encryption process as a group of symbols and characters. The data type thus determines the encryption type system. And each system has its own uses. For example, asymmetric encryption can be used for authentication or when sending a secret key for decryption. To understand asymmetric encryption, let's take the RSA model, an example of asymmetric encryption, and the main steps of the RSA model:

**RSA Model Steps:**

- Each user generates a public/private key pair by selecting two large primes at randomp,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), and0≤d≤n.
- Publishing their public encryption key: $Pkk$=($ee$,$nn$).
- Keeping secret private decryption key: $pprr$=($dd$,$nn$).
- At the encryption side the sender uses encryption
- Mathematical equation C=$ppeemmmmddnn$.
- At the decryption side the receiver uses decryption mathematical equation. P=$ccddmmmmddnn$.

**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; choosee=7.
- Determining d:d×e=1 mod 20 and d×7=1mod 20 we taked=3i.e(3×7)mod20=1sod=3Publishing public key $ppkk$ =(7,33)
- Keeping private key secret $pprr$=(3,33)

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

| Plaintext | Encryption Process |
|---|---|
| T→19 | $19^{7}$ mod 33=13 |
| E→04 | $04^{7}$ mod33=16 |
| L→11 | $11^{7}$ mod33=11 |
| A→00 | $00^{7}$ mod33=00 |
| N→04 | $04^{7}$ mod33=16 |
| G→06 | $06^{7}$ mod33=30 |
| A→00 | $00^{7}$ mod33=00 |
| N→04 | $04^{7}$ mod33=16 |
| A→00 | $00^{7}$ mod33=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 | PlainText |
|---|---|
| $13^{3}$mod33=19 | 19→T |
| $16^{3}$mod33=04 | 04→E |
| $11^{3}$mod33=11 | 11→L |
| $00^{3}$mod33=00 | 00→A |
| $16^{3}$mod33=13 | 13→N |
| $30^{3}$mod33=06 | 06→G |
| $00^{3}$mod33=00 | 00→A |
| $16^{3}$mod33=13 | 13→N |
| $00^{3}$mod33=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=(P)

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

## V. Conclusion

Network security is the most important element of information security as it is responsible for securing all information transmitted via computers on the network. Network security includes the precautions taken in an underlying computer network infrastructure, the directives defined by the network administrator to protect the network and the resources accessible by the network against unauthorized access, as well as monitoring and consistent and continuous measurement of their effectiveness (or lack thereof). We have studied various cryptographic techniques to increase network security.

**ACKNOWLEDGEMENT**

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 suggestion 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 by users," 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-javascript-cryptography/

[5] IETF, "RFC 5246 - The Transport LayerSecurity (TLS)

[6] Protocol Version 1.2.".: http://tools.ietf.org/html/rfc5246

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

[8] K .Thogmas, "The Myth of the Skytale ". *Taylor & Francis, (1998),* Vol (33), pp:244-260.

[9] 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 (CISDA2007).*

[10] 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.

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

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

**Citation of this Article:**

Pranali Pund, Yamini Bhele, Prof. M.R.Khan, "Cryptography" Published in *International Research Journal of Innovations in Engineering and Technology (IRJIET),* Volume 4, Issue 1, pp 32-37, January 2020.

*******