**International Research Journal of Human Resource and Social Sciences**
**ISSN(O): (2349-4085) ISSN(P): (2394-4218)**
**Impact Factor 6.924 Volume 9, Issue 12, December 2022**
**Website**- www.aarf.asia, **Email** : editoraarf@gmail.com

# CRYPTOGRAPHIC AND KEY MANAGEMENT APPROACH FOR SECURING DATA IN THE CONTEXT OF PREVAILING CYBER SECURITY

**ARUN GUPTA**
RESEARCH SCHOLAR, SUNRISE UNIVERSITY, ALWAR

**DR. SUMIT BHATTACHARJEE**
ASSOCIATE PROFESSOR, SUNRISE UNIVERSITY, ALWAR

## ABSTRACT

*Generation, distribution, exchange, storage, usage, revocation, etc. of cryptographic keys are all part of key management in a cryptographic system. User protocols, policies, guidelines, policy standards, protocol design, key server, cryptographic algorithms, coordination among system components, group and subgroup management, peer-to-peer communication, system framework, user training, etc., are all part of key management. The key to every secure cryptosystem is the key itself. The cryptographic system's security relies heavily on the care with which cryptographic keys are handled. The true difficulty of key management is in the effective management of the whole key life cycle, not in the storage and encryption of keys. Cybercrime is defined as a crime in which a computer is the object of the crime or is used as a tool to commit an offense. Cyber Security is a system of defending information, servers and network from malicious attacks. Now a day's every information or data is digitalises which are stored in server, clouds and other resources.*

**Keywords: -** Cryptographic, Cyber Security, Key Management, Encryption, Network

## I. INTRODUCTION

Life of any key depends on various cryptographic parameters including the length of the key, strength of cryptographic algorithms, medium of key transmission, various possible attacks and availability of computational power to break that key.

If the length of the key is sufficiently large and cryptosystem is sufficient secure in terms of leakage of the secure key then existing key length sustains for a long time.

If any key is compromised by any means like distribution of key through insecure media, man in middle attack, small length of key, cryptographic attacks then key is need to be revoked.

Revocation of key is needed to limit the amount of information to be encrypted by any key, protects from various attacks, limits the system exposure, avoids certain cryptographic catastrophic failures (e.g. AES GCM mode loses protection if more than 64 GB is encrypted on the same key), protects against current or future algorithmic weakness that reduce key lifespan etc.

To manage the keys efficiently, key management framework plays an important role. Framework defines the life of the key and also provides the guidelines how to manage the key during the various stages.

In this chapter, key management life cycles (Symmetric and Asymmetric) and Key revocation model to revoke the keys are proposed.

## II. ASYMMETRIC AND SYMMETRIC KEY MANAGEMENT

Asymmetric key Management: In asymmetric key cryptographic systems, two cryptographic keys are used; out of these two keys, one is used for encryption and another for decryption.

Both keys are mathematically inverse of each other, when plaintext is encrypted by one key then corresponding cipher text is decrypted using the second key.

Encryption key is called Public key which is made available publicly.

Decryption key is called Private key and owner of this key keeps this key secretly. Asymmetric encryption / decryption methodology is given in Figure 1.

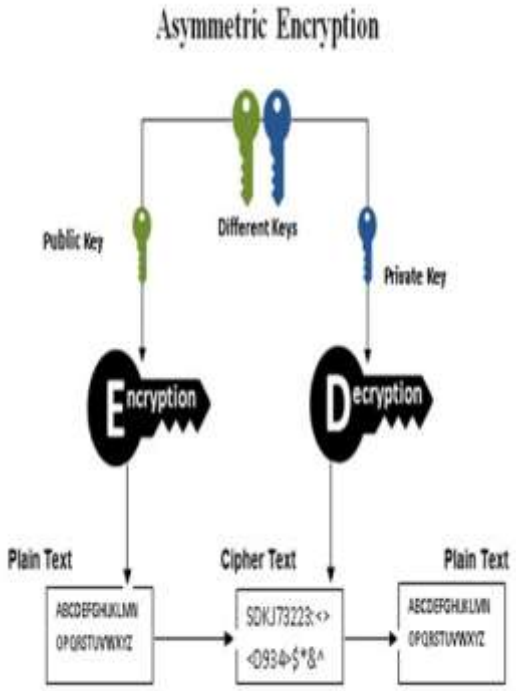


**Figure 1. Asymmetric Encryption/Decryption**

Asymmetric key encryption is much slower than symmetric key encryption and hence Asymmetric key encryption is primarily used for key exchanges and digital signature purpose only. For data transfer, Symmetric key is preferable.

## III. CRYPTOGRAPHY:

Cryptography is the art of secret writing which is used since Roman times to hide information secret or keeping the message. To keep information secret a widely used method is encryption and decryption which are the basic function of Cryptography. In cryptography the information is converted into unreadable format which is cipher text or cypher text which is cannot be understand by unauthorized user only a person who having a key can able to decode the information into original format which is called plaintext.

As we know that in the main goal of cyber security is securing the information and data from unauthenticated users. To secure the information or data we having cryptographic algorithms which are help to encrypt the data.

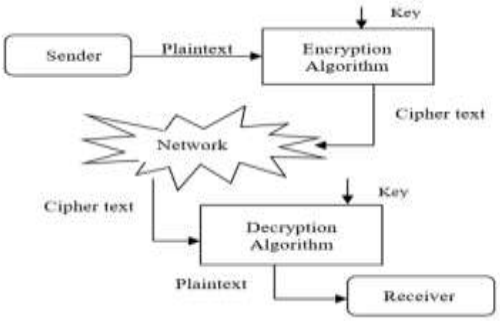


**Figure 2. Cryptography**

## IV. CLASSIFICATION OF CRYPTOGRAPHY:

Encryption algorithms can be classified into two categories- Symmetric and Asymmetric key encryption.

- Symmetric Algorithm
- Asymmetric Algorithm

### Symmetric Algorithm

In the symmetric key encryption, same key is used for encryption and decryption both. Symmetric key cryptosystems are faster than the asymmetric key cryptosystems. It is used to provide confidentiality of the messages. There are hundreds of different symmetric key algorithms available. Each has its own strengths and weaknesses. Some of the more common examples are DES, 3DES,ETC

**1. DES (Data Encryption Standard):** DES was originally developed in 1976. It has been one of the most widely used encryption algorithms. This is partially due to the fact that it was adopted as the government standard for encryption. The DES algorithm itself is very strong. The weakness of the original DES standard is that it uses a 56-bit encryption key.

**2. 3DES:** It is most commonly known as Triple DES. It applies the DES algorithm three times to each block of data that's why it's called 3DES. 3DES has overtaken its predecessor, DES, and is currently considered to be the most widely used standard for secure encryption. The algorithm itself is just as strong as DES and also has the advantage of being able to use longer key lengths. A key must be specified for each of the 3DES encryption. There is an option of using the same key for each, the same for two of the iterations, or a different key for each of the iterations. The most secure implementation is to use a different key for each iteration. If you use the same key for all three iterations, the key strength is considered to be 56 bits. That's basically the same as DES.

### Asymmetric Algorithm:

In the asymmetric cryptography a key can be divided into two parts, a public key and a private key. The public key can be available for everyone while the private key must be kept secret. Asymmetric cryptography has two major use cases: confidentiality and authentication. Using asymmetric cryptography, messages signed with a private key, and then anyone with the public key is able to verify that the message was created by someone possessing the corresponding private key. This can be combined with a proof of identity system to know what entity (person or group) actually owns that private key, providing authentication. Encryption with asymmetric cryptography works in different way from symmetric encryption. Asymmetric key algorithms aren't as widely used as symmetric counterparts. So we'll go over two of the big ones: Diffie-Hellman and RSA

**1. Diffie-Hellman:** The Diffie-Hellman algorithm was one of the earliest known asymmetric key implementations. The Diffie-Hellman algorithm is mostly used for key exchange. Although symmetric key algorithms are fast and secure, key exchange is always a problem. You have to figure out a way to get the private key to all systems. The Diffie-Hellman algorithm helps with this. The Diffie-Hellman algorithm was used to establish a secure communication channel used by the systems to exchange a private key. This private key is then used to do symmetric encryption between the two systems.

**2. RSA ( Rivest Shamir Adelman algorithm):** RSA was developed in 1978. RSA was the first widely used asymmetric algorithms used for signing and encryption. It supports key lengths of 768 and 1,024 bits. The RSA algorithm uses a three-part process. The first part is key generation. The keys used in the RSA algorithm are based on prime numbers. The second part of the process is encryption. This encryption is done using public key and private key pair. The third part of the process is decryption. The decryption is done using the private key.

## V. TRENDS OF CYBER SECURITY

### 1. Web servers

The risk of assaults on web applications to separate information or to circulate malicious code perseveres. Cybercriminals convey their code using good web servers they have traded off. In any case, information taking attacks, a considerable lot of which get the deliberation of media, are also a significant risk. Currently, individuals need a more unusual accentuation on securing web servers as well as web applications (Bendovschi, 2015). Web servers are mainly the preeminent stage for these cybercriminals to take the information. Thus, one should reliably utilize an additional secure program, mainly amid vital exchanges all together not to fall as a quarry for these defilements.

### 2. Mobile Networks

The risk of assaults on web applications to separate information or to circulate malicious code perseveres. Cybercriminals convey their code using good web servers they have traded off. In any case, information taking attacks, a considerable lot of which get the deliberation of media, are also a significant risk. Currently, individuals need a more unusual accentuation on securing web servers as well as web applications (Bendovschi, 2015). Web servers are mainly the preeminent stage for these cybercriminals to take the information. Thus, one should reliably utilize an additional secure program, mainly amid vital exchanges all together not to fall as a quarry for these defilements.

### 3. Encryption

It is the method toward encoding messages so programmers cannot scrutinize it. In encryption, the message is encoded by encryption, changing it into a stirred-up figure content. It commonly completes with the use of an "encryption key," that demonstrates how the message is to encode. Encryption at the earliest reference point level secures information protection and its respectability (Sharma, 2012). Additional use of encryption obtains more problems in cybersecurity. Encryption is used to ensure the information in travel, for instance, the information being exchanged using systems (for example the Internet, online business), mobile phones, wireless radios and so on.

### 4. ADP's and targeted attacks

Advanced Persistent Threat (APT) is a whole of the dimension of cybercrime ware. For quite a long time network security capacities. For example, IPS or web filtering have had a key influence in distinguishing such focused-on assaults (Bendovschi, 2015). As attackers become bolder and utilize increasingly dubious methods, network security must incorporate with other security benefits to identify assaults. Thus, one must recover our security procedures to counteract more dangers coming later on. Subsequently the above is a portion of the patterns changing the essence of cybersecurity on the planet. The top network threats are showing in figure 3.

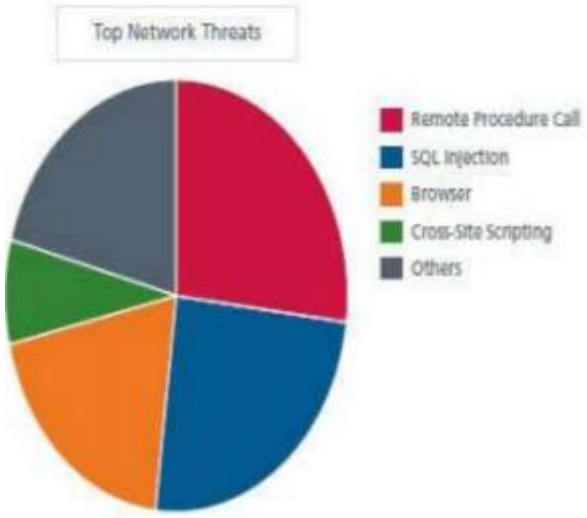


**Figure 3. Threats for Cyber Security**

## VI. CONCLUSION

Cyber-security is both about the insecurity made by and through this new space and about the practices or procedures to make it (progressively) secure. Exertion to verify the cyberspace should give a definitive need else the "information technology" will not be viably used by clients. The terrorist of things to come will win the wars without discharging a shot just by crushing the country's necessary substructure if steps are not taken to handle the pervasiveness of the expansion in such a cyber-attack. They can bring an unknown look into the lives of others, regardless of whether they live nearby or over the globe.

With the increase in the users of internet, the increase in cyber-crimes can also be seen. Cyber-crime can be done mainly by using the technique of hacking. Hacking is the method in which the criminals get access to the victim's system without their knowledge. All the persons who use internet and especially those make money transactions through internet must be beware of the cyber criminals. It is the need of today's world to have knowledge about the crimes that are associated with the internet. It is the duty of each one of us to be aware of the basic internet security like changing the passwords regularly, keeping long passwords, avoids disclosing personal information to strangers on the internet or entering credit card details on unsecured websites to avoid any fraud, etc. Government is also making efforts to have a control on these cyber-crimes. IT Act 2000 is made to deal with the cyber-crimes.

**References:-**

1. Sutton, D. (2017). Cyber Security : A Practitioner's Guide. Swindon, UK: BCS, the Chartered Institute for IT.

2. Sreenu, M., & Krishna, D. V. (2017). A General Study on Cyber-Attacks on Social Networks. IOSR Journal of Computer Engineering (IOSR-JCE), 19(5), pp. 01-04

3. Sharma, R. (2012). Study of Latest Emerging Trends on Cyber Security and its challenges to Society. International Journal of Scientific & Engineering Research, 3(6).

4. Samuel, K. O., & Osman, W. R. (2014). Cyber Terrorism Attack of The Contemporary Information Technology Age: Issues, Consequences and Panacea. International Journal of Computer Science and Mobile Computing, 3(5), pp. 1082-1090.

5. Panchanatham, D. N. (2015). A case study on Cyber Security in E-Governance. International Research Journal of Engineering and Technology.

6. Kumar, S., &Somani, V. (2018). Social Media Security Risks, Cyber Threats And Risks Prevention And Mitigation Techniques. International Journal of Advance Research in Computer Science and Management, 4(4), pp. 125-129.

7. Hua, J., &Bapna, S. (2013). The economic impact of cyber terrorism. The Journal of Strategic Information Systems, 22(2), pp. 175-186.

8. Gross, M. L., Canetti, D., &Vashdi, D. R. (2017). Cyberterrorism: its effects on psychological well-being, public confidence and political attitudes. Journal of Cybersecurity, 3(1), 49–58. doi:10.1093/cybsec/tyw018

9. Solving Cyber Security Challenges using Big Data, PrajaktaJoglekar, NitinPise, International Journal of Computer Applications (0975– 8887)Volume 154–No.4, November 2016

10. Cardenas, P. K. Manadhata, S. P. Rajan, Big Data Analytics for Security, IEEE Security and Privacy, 11 (6), 2013, pp. 74 -76.

11. Enhancing Cyber security with Big Data: Challenges and Opportunities December 2, 2016 by Emmeline Short.