MAT JOURNALS

Journal of Embedded Systems and Processing
Volume 3 Issue 3

Cryptography: Symmetric vs Asymmetric Encryption

[1]Mr. Anurag Rawal, [2]Mr. Gaurav, [3]Mr. Hitesh Khanna, [4]Prof. Gaganjot Kaur
[1,2,3]Student, [4]Professor
Department of Computer Science & Engineering
Manav Rachna University, Faridabad, Haryana, India
***Email:** [1]anurag.rawal07@gmail.com, [2]gauravchhikara1999@gmail.com,*
[3]hiteshkhanna656h@gmail.com,[4] gaganjot@mru.edu.in
***DOI:** https://doi.org/10.5281/zenodo.1465672*

Abstract

With the arrival and outbreak of high speed internet, www (World Wide Web) and growth of social media, online transaction, application and business, organization across the globe produce too much amount of data every second. Data Security is the most basic and extreme measures to ensure secure passage of information through internet. As the number of user's increases rapidly throughout the globe tremendously which directly entice cracker for doing cyber-attack. Moreover data security is becoming necessity as we are heading towards digital globalization. In this paper we have discuss the 2 types of encryption i.e., Symmetric and Asymmetric. We briefly explain them how these encryption techniques work and in the end explain which one of these techniques is best and why.

Keywords: *Cryptography, Encryption, Decryption, Ciphers, Ciphers Text, Cryptosystem.*

INTRODUCTION

Cryptography is a Latin word compromised of two word Krypts and graphhein which means "hidden or secret" and "study or writing", respectively. Thus, cryptography is an art or way and the science behind secret writing.

Cryptography is about composing a set of protocols so that no one can understand the data except sender and receiver thus cryptography is very convenient for data integrity and authentication purposes. Cryptography has evolved too much from classical cipher, in which letter substitution took place to modern day cryptosystem in which it is very difficult for people to decrypt and encrypt data too easily.

Today's our entire world is relying on web and its application. Information security plays significant role in securing modern communication systems. The most important objectives of information security are authentication, confidentiality, data integrity and non-repudiation here come the requirement of securing our privacy by ways of Cryptography. Cryptography plays a significant role for secret writing. It is the art of securing data. Cryptography is used to assure that the contents of a message are very confidentiality transmitted and wouldn't be altered. Cryptography provides range of security goals to make sure of privacy of information. The idea of encryption by which we can encode our valuable data in secret code and not to be able readable by unauthorized person even it is hacked.

Cryptography plays an important role in securing information during data transmission which is a big issue for both sender and receiver. Thus, cryptography emerges as a significant tool for safer communication.

Cryptography allows the data or information to transmit through network in unidentified ways so that the intruder's cannot understand the data. Due to the

mechanism of cryptography only sender and intended receiver can read or understand the message. Cryptography has evolved throughout its lifetime, starting from letter substitution to modern day unbreakable public key cryptosystem.

Applications of cryptography include e-commerce, online truncation through credit or debit cards, crypto currencies, pc passwords, and military communications.
In Cryptography there are some Significant Terms:

Plain Text

Secrete message or information which is readable and will be encrypted.

Cipher Text or Encrypted Text

Data obtain after encrypting the information with the help of a key is known as cipher text.

Key

It is a word or value that is used for encryption of plaintext and decryption of cipher text.

Encryption

It is the technique of converting the data into encrypted form i.e. In non-understandable format with the help of key is called encryption

Decryption

It is the technique of converting the encrypted data in plain text i.e. In understandable format with the help of key is called decryption.

Crypto Analyst

Crypto Analyst is the person who is expert in breaking cipher text, cipher and cryptosystem.

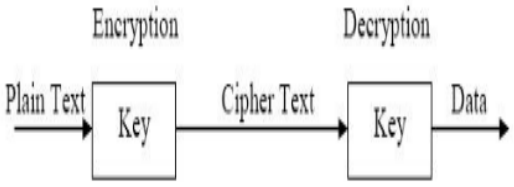

Fig: 1. *A simple block diagram to understand Cryptography*

The above block diagram shows how cryptography works, simple message or information which is readable gets converted into cipher text and then converted back to plain text with the help of decryption.

Objective of cryptography

1. *Authentication:* This mechanism facilitates to establish proof of identities. This method assures the origin of the message is properly known.
2. *Access Control:* This principle states that who have the control over the access of data.
3. *Availability:* The principle of availability states that resources ought to be out there to approve users.
4. *Confidentiality:* This Principle states that only sender and receiver can process the content of message or information.
5. *Integrity:* This mechanism assures the data or information reaches to receiver will remain the same.
6. *Nonrepudiation:* This mechanism refers to the ability to ensure that a user cannot deny the sending of data or message that they originate.

LITERATURE SURVEY

We studied many attacks which can be done on cryptography encryption standard to find it's strength. The basic intention of a hacker or attacker is to break encryption algorithm by means of finding plaintext from cipher text to obtain the key. Some of the attacks that were used by attacker are discussed as follows:

- *COA (Ciphertext Only Attacks)*: In this attack the attacker has a set of cipher text from which he or she computes the plaintext.
- *KPA (Known Plaintext Attack)*: In this attack the attacker knows plaintext of some cipher text from which he or she have to determine other cipher text.
- *CPA (Chosen Plaintext Attack)*: In this

attack the attacker has the text of his choice encrypted which means he or she has the cipher-text and plain-text pair of his or her choice through which he or she can determine the encryption key.

- *Dictionary Attack*: In this attack the attacker maintain the dictionary of cipher-text and the corresponding plain-text and to decrypt the data he or she refers to that dictionary.
- *Brute force Attack*: In this attack the attacker determine the key by attempting all possible keys. This attack takes too much amount of time.
- *MIM (Man in Middle Attack)*: In this attack the attacker determine the key during key exchange step in public key cryptography.
- *Fault analysis Attacks*: In this attack the attacker introduce some error in the algorithm and study the error to get some resourceful information which results in breaking of algorithm.

What is Asymmetric Encryption

In symmetric encryption there is only one key which is also known as private key which is used to encrypt and decrypt text. In nowadays era this personal or symmetric key can be a series of numbers alphabets and individual Ex. AsddErTY8944.

Suppose Alice wants to send an encrypted message to bob through internet, so she first tells bob about the private key through which she done encryption. Alice must find a way other than internet to tell bob about this encryption key. She can use postcard or she can handover the key to tom saying that "Anytime in future if she needed to communicate securely she can use this private key for encryption" . Moreover, bob can use that key for encryption too.

Example of symmetric Encryption

DES

DES stands for data Encryption popular, evolved within the early 1970 and uses the Fiestel characteristic for encryption and decryption information. Encryption and decryption key are equal in DES.

It is block cipher which has 64 bit block size out of which 56 bit for key period and rest 8 bit for errors detection. It makes use of 16 spherical of permutation for encrypting statistics. Decryption procedure is identical precisely as of encryption with the difference that decryption is done in reverse order.

AES

AES stands for Advanced Encryption standard, published in early 1977 to overcome the drawback of DES. It is a symmetric block cipher which means encryption and decryption key are exactly same. It has a 128 bit block size with variable key length of 128, 192 or 256 bits. It encrypts 128 bits data block into 10(128 bits), 12(192 bits) and 14(256 bits) round respectively according to the key size, mostly 256 bit key length is used. AES permutation has four stages of substitute bytes, shift rows, mix columns and add round key.

What is Asymmetric Encryption

Asymmetric encryption uses 2 keys i.e., private key and public key. Different encryption key is used in both end for secure communication between 2 parties.

Suppose Alice want to communicate with tom then tom have to tell Alice his public key through which she done encryption. Tom does not find a way to tell Alice about the public key as no one can decrypt the message. Note that if Tom want to communicate with Alice than Alice must generate her own private – public key pair and send the public key to Tom.

Example of Asymmetric Encryption

RSA

RSA is known as after the mathematicians Ron Rivest, Adi Shamir and leonard Adleman. First published in 1977, it is an asymmetric block cipher, which means that both encryption and decryption key are specific .RSA also known as public key algorithm as one of the secret is known to absolutely everyone. RSA uses a variable length encryption block and a variable length key.

For encryption purpose the RSA user posted the made from high quantity and one of the top variety that is of the order of 1028 bit or 309 decimal digits.

No one can determine the prime factor of the product from one auxiliary value, which makes it very difficult for attacker to decrypt data or information except user who knows the secret key. RSA algorithm ensures the safety of data.

ECC

ECC stands for Elliptic curve cryptography. First published in 1985, it is based on public key cryptography. ECC algorithm is an alternative for RSA as it works more efficiently than RSA algorithm. RSA algorithm is very difficult to break but ECC algorithm on the other hand is infeasible to break. To make RSA algorithm more secure, user increment the key size to 3072 bit RSA public key which work as efficiently as 256 bit ECC public key. ECC algorithm works on the mathematical problem i.e. it is impossible for anyone to find the logarithm of a random elliptic curve element with respect to a publicly known base point (which works as public key). ECC reduces the storage problem as it works too efficiently on smaller key size.

SYMMETRIC VS ASYMMETRIC

In this section we have discussed the drawback and advantages of both encryption system.

Why Symmetric is vastly better than Asymmetric

Cpu Speed , Memory And Power

The power consumption, cpu time and memory needed for RSA is more than that required for AES encryption. AES can easily be embedded in smart cards to encrypt and decrypt data.

Advances In Factorization

Public key – Private key approach uses the multiplication of 2 large prime number. Unauthorized decryption which means cracking or decrypting of an encrypted message with the help of factorization to find the original 2 numbers.

As advances in mathematical technique of factorization and in cpu continues which leads to the faster cracking of encrypted data.

Authentication Required

As mentioned earlier in this paper that sending or publishing a public key over the internet did not pose problem as it did not allow other party or intercepting party to decrypt message but it does allow them to create and send message as if from the destined party or user.

COMPARING EQIVALENT STRENGTH TABLE

Table: 1. *Above figure illustrate the equivalent strength of RSA and AES*

Equivalent Strengths Table

Enc. Bits	Symmetric Alg.	RSA
112	3DES	k = 2048
128	AES-128	k = 3072
192	AES-192	k = 7680
256	AES-256	k = 15360

It is clear from the above table that AES provide superior security over RSA using 15360 bits is just as secure as the AES with 256 bits. AES is clear cut better than RSA.

There is only one drawback of symmetric encryption over asymmetric encryption which we found that involves a logistics problem of transmitting symmetric key.

Suppose a user is buying something from e-commerce site, when placing order user have to enter his credit card details. It's obvious user want this transmission of credit card details should be encrypted. If symmetric encryption were to be used than user, somehow, must communicate with the e-commerce site and conveyed them the symmetric key which is quite inconvenient to both user and the merchant.

CONCLUSION

In this paper we reviewed about Symmetric and Asymmetric encryption. Clearly, each encryption standard has it's own strength.

We come to the conclusion that Symmetric encryption is more advanced than Asymmetric encryption.

ACKNOWLEDGMENT

We would like to express our thanks of gratitude to Accendere Knowledge Management Services for providing us the Platform & Opportunity to pursue the research.

REFERENCES

1. Global journals GJCST_Volume13/4-A-Study-of-Encryption-Algorithms https://globaljournals.org/GJCST_Volume13/4-A-Study-of-Encryption-Algorithms.pdf
2. Volume 8, No. 4, May 2017 International Journal of Advanced Research in Computer Science Review Article Available Online at www.ijarcs.info© 2015-19, IJARCS 358 A Review on Symmetric Key Cryptography Algorithms http://ijarcs.info/index.php/Ijarcs/article/viewFile/3777/3258
3. International Journal of Computer Applications (0975 –8887) Volume 61–No.20, January 2013 12 Symmetric Algorithm Survey: A Comparative Analysis https://arxiv.org/ftp/arxiv/papers/1405/1405.0398.pdf
4. International Journal of Computer Applications (0975 –8887) International Conference on Advancements in Engineering and Technology (ICAET 2015) 1 Asymmetric Algorithms and Symmetric Algorithms http://research.ijcaonline.org/icaet2015/number4/icaet4049.pdf
5. An overview on cryptography by Gary C. Kessler https://www.garykessler.net/library/crypto.html
6. http://www.geeksforgeeks.org/
7. http://cryptofundamentals.com/
8. https://www.tutorialspoint.com/
9. http://www.ijettcs.org/Volume4Issue1/IJETTCS-2015-01-01-12.pdf/
10. http://en.wikipedia.org/

Cite as:
Mr. Anurag Rawal, Mr. Gaurav, Mr. Hitesh Khanna, & Prof. Gaganjot Kaur. (2018). Cryptography: Symmetric vs Asymmetric Encryption. Journal of Embedded Systems and Processing, 3(3), 1–5. http://doi.org/10.5281/zenodo.1465672