JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

A Review of Data Encryption techniques used for different social media

Dr. Ranjit D. Patil[1], Dr. Sonali Nemade[2], Dr. Sunayana Shivthare[3]

[1]Principal, Dr. D.Y. Patil ACS College, Pimpri, Pune, [2]Assistance Professor, Dr. D.Y. Patil ACS College, Pimpri, Pune, [3]Assistance Professor, Dr. D.Y. Patil ACS College, Pimpri, Pune,

Abstract :

In the demand for new technologies based on software is increasing rapidly. These technologies are used in computers and smartphones or any other electronic device. For faster communication, most of the confidential data is exchanged through networks as electronic data. Today most people have their accounts on Facebook, Whatsapp and other means of social media. But the problem of security arises at the same time that how secure our personal information is on these social media sites. Security is the most challenging aspect of the internet and network applications. Hence the search for the best solution to offer the necessary protection against the data intruders' attacks along with providing these services in time is one of the most interesting subjects in the security. Cryptography is one of the main aspects of computer security that converts information from its normal form into an unreadable form. In this paper, we have studied some of the conventional encryption algorithms used in social media.

IndexTerms - Cryptography, Symmetric Encryption, Asymmetric Encryption, Public key, Private Key, Social Media.

I. INTRODUCTION

Every user needs the security of his data and personal information from hackers and any other harmful attacks on their social media accounts. To do this there is an immense need for a special technique called cryptography. Cryptography is a powerful tool used to protect information in computer systems. For private communication through a public network, cryptography plays a very important role.

The main mechanism is encryption and decryption which guide the flow of data. Cryptography has two modes of encryption known as the public key and secret key. The shared between two parties is actually the secret information that needs to be transferred over the network. The use of the secret key is sometimes known as a symmetric key and that of an asymmetric key is known as the public key. In asymmetric transformation the private or secret key is used to transform the original data into a ciphered form, then at the other end, the public key is used to convert the data into decrypted data again. The public key provides slow data transformation and it is suitable to be used for converting a small amount of data. The main goals of using cryptography are authentication, integrity, confidentiality, non-repudiation, and availability.

Cryptography is usually referred to as "the study of secret". Cryptography helps in the security of the data storage and transmission with the goal that only expected users can view it. It completely hides data from the third party (attacker/intruder). It is about analyzing the protocols which are associated with knowledge safety for instance information secrecy, access control, data reliability, and validation. Cryptography includes the following important terms:

Plain Text- It is the original text on the sender's side.

Cipher Text-It is the encoded text of the main text.

Encryption -The procedure of transforming clear text into encrypted text is Encryption.

Decryption-The method of changing secret message code back into the ordinary readable form of the message is Decryption.

In social media apps, using E2EE(End to End Encryption) encryption means that only the sender and receiver can read the encrypted data because the key to decrypt the data lies only with the end user. No other person including the service provider has the capacity to decrypt the data even though the data travels through their servers. Not all social media platforms use end-2-end encryption. There are some apps like Facebook Messenger where encryption applies only to the circulated data. Other apps encrypt the data but store the decryption keys thereby creating the possibility for inspection by law enforcement agencies. Apps like Snapchat encrypt only data in transit but the messages are deleted from the server once the recipient reads it.

II. NEED FOR ENCRYPTION

Due to the fast growth in both computer technologies and the Internet, the security measures of information are considered one of the most significant factors of Information Technology and Intelligence. With the invention of social media on the Internet, the means of communication also grew with time. Earlier there were email lists and bulletin boards which allowed the people to collect

and share the information across the world. But today we have many advanced applications on the Internet through which we can communicate with each other and can exchange our information all around the world. But the drawback of this advancement e is that the data is not secure on social media as we can share almost everything like text, images, video, audio, etc. Even if we try to keep our information safe by doing personal settings in privacy, our information will be kept hidden only by the persons whom we don't want to show it. Rather all the information is collected by the owner of the site. It is the procedure of transforming normal information (called plaintext) into unreadable text (called cipher-text). So if we work with shared grid services it is vital to know the confidentiality and safety issues that they lift. Prior to working on any public networking site, it becomes essential to realize how they compose us exposed and further take initiatives to defend ourselves and the public we do our job. Hence there arises a need for encryption of data to make ourselves free from any kind of malicious attacks as much as possible.

Advantages of using encryption for social media

1) Encrypted Data Maintains Integrity

Hackers can steal information, as well as they also can benefit from altering data. It may happen that it is possible for a skilled person to modify encrypted data, but the receiver of the data can detect the malicious data, which allows for a quick response to the cyber-attack.

2) Encryption Protects Privacy

Encryption is used to protect sensitive information, including the personal information of individuals. This helps to ensure privacy. Encryption technology is so powerful that some governments are attempting to put limits on the effectiveness of encryption which does not ensure privacy for companies or individuals.

3) Encryption is Part of Compliance

Many industries have strict compliance requirements to help protect those whose personal information is stored by organizations. HIPAA, FIPS, and other regulations rely on security methods such as encryption to protect data, and businesses can use encryption to achieve comprehensive security.

4) Encryption Protects Data across Devices

Different devices are (and mobile) a part of our lives, and transferring data from device to device is not secure. Encryption technology can help protect store data across all devices, even during transfer. Additional security measures like advanced authentication help to protect data from unauthorized users.

III. DATA ENCRYPTION METHODS USED FOR SOCIAL MEDIA:

There are two types of data encryption techniques,

1. Symmetric Key Cryptography:

It is also called secrete key cryptography. It uses a single key. In this encryption process, the receiver and the sender have to agree upon a single secret (shared) key. Encryption is the process in which the original message (called plaintext) is converted into an unreadable message using the secret key. Decryption is the reverse of encryption and uses the same key as encryption.
The following Symmetric Key encryption algorithms:

a) Advanced Encryption Standard (AES):

AES is an iterative cipher. It is based on a 'substitution–permutation network'. It comprises a series of linked operations, some of which involve replacing inputs with specific outputs (substitutions) and others involve shuffling bits around (permutations).

The features of AES are as follows −

- Symmetric key symmetric block cipher
- 128-bit data, 128/192/256-bit keys
- Stronger and faster than Triple-DES
- Provide full specification and design details

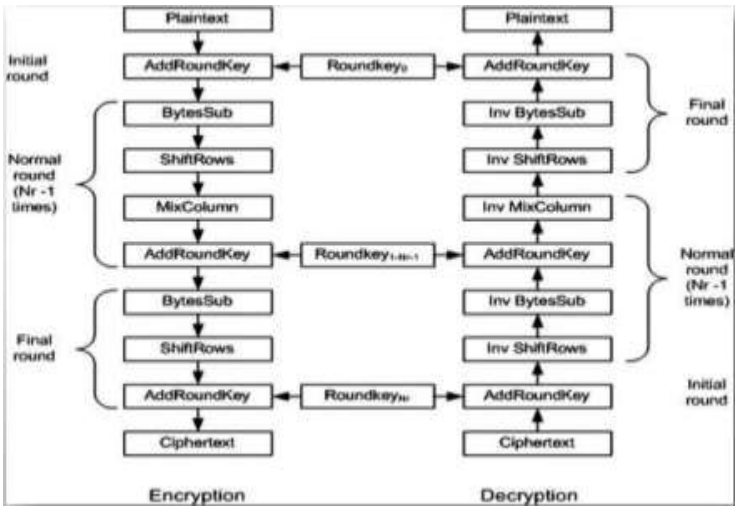

Figure 1.1 AES Algorithm

b) Data Encryption Standard (DES):

The Data Encryption Standard (DES) is a symmetric-key block cipher published by the National Institute of Standards and Technology (NIST). It uses 16 round. The block size is 64-bit. The key length is 64-bit, DES has an effective key length of 56 bits, since 8 of the 64 bits of the key are not used by the encryption algorithm.

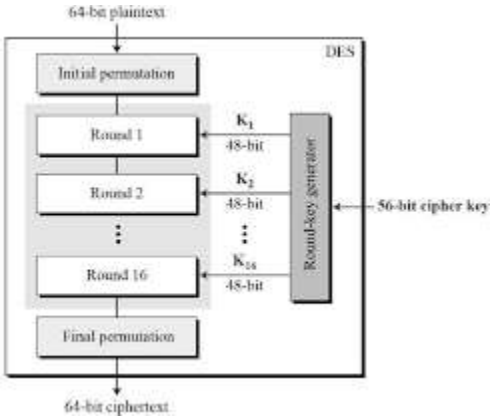

Figure 1.2 DES Algorithm

c) Blowfish Encryption Algorithm:

Blowfish has a 64-bit block size and a key length of anywhere from 32 bits to 448 bits. It is a 16-round and uses large key-dependent S-boxes. It is similar in structure to CAST-128, which uses fixed S-boxes. In Blowfish each line represents 32 bits. The algorithm keeps two subkey arrays: the 18-entry P-array and four 256-entry S-boxes. The S-boxes accept 8-bit input and produce 32-bit output. One entry of the P-array is used every round, and after the final round, each half of the data block is XORed with one of the two remaining unused P-entries. The diagram to the right shows Blowfish's F-function. The function splits the 32-bit input into four eight-bit quarters, and uses the quarters as input to the S-boxes. The outputs are added modulo 232 and XORed to produce the final 32-bit output.

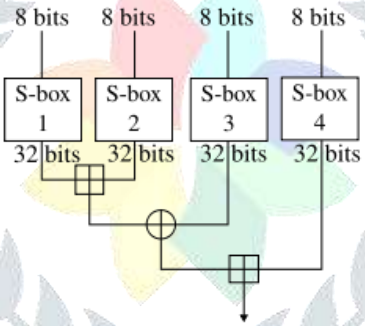

Figure 1.3 Blowfish Algorithm

2. Asymmetric Key Cryptography:

It is also called as public key cryptography. It uses public and private **keys** to encrypt and decrypt data. Public key, which is known to the both sender and receiver, used for encryption and private key, which is known only to the user of that key, used for decryption. The public and the private keys are related mathematically to each other. We can say, data encrypted by one public key can be encrypted only by its corresponding private key.

a) Deffiee Hellman algorithm

1. Firstly, A and B agree on two large prime numbers n and g. These two integers need not be kept secret. A and B can use an insecure channel to agree on them .
2. A chooses another large random number x and calculates c such that
c=g x mod n
3. A sends the number c to B
4. B independently chooses another large random integer y and calculate d such that
d=g y mod n
5. B sends number d to A
6. A now compute the secreate key K1 as follows
K1= d x mod n
7. B now computes the secret key K2 as follows.
K2=c y mod n

b) RSA algorithm

RSA involves a public key and a private key. The public key can be known by everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted in a reasonable amount of time using the private key. The keys for the RSA algorithm are generated in the following way

1. Choose two distinct prime numbers p and q.
2. Compute n = p*q.
3. Select the public key (i.e. the encryption key) e such that it is not factor of (p-1) and (q-1)
4. Select the public key (i.e. the decryption key) d such that the following equation is true.

(d*e) mod (p-1)*(q-1)=1.

5. For encryption calculate the cipher text CT from the plane text PT as follows

CT=PT e mod n

6. Send CT as the cipher text to the receiver.
7. For decryption, calculate the plane text PT from the cipher text CT as follows.

CT d mod n

c) DSA algorithm

Key generation

- Select a prime q of 160 bits
- Choose 0≤t≤8, select 2511+64t<p<2512+64t with q/p-1
- Select g in Zp and a=g(p-1)/q mod p.α≠ 1
- Select 1≤ a ≤ q-1, compute y= α b mod p.
- Public key (p,q, α ,y) private key a

Signing

- Select a random integer k, 0<k< q.
- Compute r= (α k mod p) mod q.
- Compute k-1 mod q.
- compute s=k-1*(h(m)+ar) mod q.
- Signature=(r,s).

Verification :

- Verify 0<r<q and 0<s<q, if not, invalid
- Compute w=s-1 mod q and h(m).
- Compute u1=w*h(m) mod q. u2=r*w mod q.
- Compute v=(α u1yu2 mod p)mod q.
- Valid if v=r.

IV. CURRENT TECHNIQUES USED ON SOCIAL MEDIA FOR ENCRYPTION:

1. Facebook

This social media site has developed various complex systems which work in the back end so as to keep the user absolutely secure from attacks. Facebook has even created some advanced features by which user can protect themselves such as Distant Logout and OTP (One Time Passwords). Such attributes are helpful when one is not sure about the security of the network or computer systems. In Facebook forward secrecy is a way of encrypting internet traffic. The connection between a website and your browser is so that it's harder for a third party to decrypt the pages being viewed, even if the server's key becomes compromised.

In regular HTTPS connections, those key exchanges are protected by a single "master" (private) key held by the server, which is fine unless the server's key is compromised; sites use forward secrecy exchange keys differently so that a criminal or an intelligence agency sucking up internet traffic can't retroactively decrypt all of the site's communications if they get the server's private key. Facebook uses passwords to protect accounts and an MD5 hash as authorization, their use of encryption is nonexistent. All authorization information is sent in the clear, including the account passwords, making them exceedingly easy to sniff on a public network. This is clearly inferior to the current best practices for password protection.

2. Whatsapp

This messaging app has been providing powerful encoding to the people who use it since 2014, creating it very tricky for the establishment to discover the messages of its service. Whatsapp already offers IPhone and Android users encrypted messaging. It has also planned to provide users encrypted voice calls, group messages etc. That would make whatsapp very difficult to be tapped by authorities. Whatsapp also has planned to announce officially about its extended encoded aids.

WhatsApp's end-to-end encryption is available when a user and the person he/she messages to is using the latest version of the app. According to WhatsApp, "Many messaging apps only encrypt messages between you and them, but WhatsApp's end-to-end encryption ensures only you and the person you're communicating with can read what is sent, and nobody in between, not even WhatsApp. This is because your messages are secured with a lock, and only the recipient and you have the special key needed to unlock and read them. For added protection, every message you send has its own unique lock and key."

3. Amazon

Data protection refers to protecting data when it is in transmission phase and at rest. Data in transmission phase can be protected using SSL client side encryption. One has following options for securing stationary data in Amazon S3.

3.1 Server Side Encryption

User can demand Amazon S3 to encode his/her entity prior to discounting it on disc and decode it when user has to download the object.

3.2 Client Side Encryption

Users can encode data on the side of client and can transfer the encoded data to Amazon S3.Here user can administer encoded keys, encryption procedure and its devices. Amazon encrypts user data using 256 bit AES encryption also known as AES-256.User can apply encrypt the data stored using Amazon S3's set or Condensed Repetition cache choices. The whole process of encoding, managing keys, and decoding is searched and checked private at frequent intervals of time as a part of Amazon's existing audit process.

4. Twitter:

Twitter data must start encrypting all of their communications with the Twitter API (application programming interface), in order to improve security and maintain data integrity. In a short message posted on its service. All data requests sent to the Twitter API must be done through the SSL (Secure Socket Layer) protocol, or its successor, the TLS (Transport Layer Security) protocol. To date, sending a data request to Twitter in most cases could be carried out by using a simple HTTP request in plain text. Now they must be done by HTTPS (HTTP Secure), which layers TSL/SSL on top of HTTP (Hypertext Transfer Protocol).

The SSL protocol establishes encrypted communications between two parties. It provides a way for a client and server to agree on the cipher they will use to encrypt and decrypt the messages between the two.

Using a digital certificate signed by a third party, SSL will also verify for the client that the server sending the information (Twitter in this case) is in fact the genuine party, thereby eliminating the chance of someone intercepting and changing the data en route.

V. CONCLUSION

In this paper existing data encryption methods have been studied and analyzed. It is also analyzed that all techniques are essential for real time encryption. We have also studied current different encryption algorithms done on social media. Every day innovative encoding system is developing and hence data encryption tools provide faster and high rate of security.

REFERENCES

[1] Yousif Elfaith Yousif, Dr. Amin Babiker A/Nabi Mustafa,Dr. Gasm Elseed Ibrahim Mohammed, " Review on Comparative Study of Various Cryptographic Algorithm" http://www.ijarcsse.com/ISSN:2277128X, volume 4 issue 5,2015.

[2] Chetan, Deepak Sharma, "A Review on Image Compression and Stenography".

[3] Singhal, Nidhi and Raina, J P S. "Comparative Analysis of AES and RC4 Algorithms for Better Utilization", International Journal of Computer Trends and Technology, ISSN: 2231-280, July to Aug Issue 2011, pp. 177-181.

[4] Idrizi, Florim, Dalipi, Fisnik & Rustemi, Ejup. "Analyzing the speed of combined cryptographic algorithms with secret and public key". International Journal of Engineering Research and Development, e-ISSN: 2278-067X, p-ISSN: 2278-800X, www.ijerd.com Volume 8, Issue 2 (August 2013), pp. 45

[5] Abdul.Mina, D.S, Kader, H.M. Abdual & Hadhoud, M.M. "Performance Analysis of Symmetric Cryptography". pp. 1.

[6] Terremark Worldwide, Inc. \Facebook Expands Operations at Terremark's NAP West Facility" Tuesday November 1, 8:30 am ET.