RESEARCHERID
THOMSON REUTERS

[Chawla* 4(6): June, 2017] ISSN 2349-4506
Impact Factor: 2.785

Global Journal of Engineering Science and Research Management

ANALYSIS OF OPEN SOURCE CRYPTOGRAPHIC SYSTEMS

Rashmeet Kaur Chawla*, Sunil Kumar Muttoo
* Department of Computer Science University of Delhi Delhi, India
Department of Computer Science University of Delhi Delhi, India

DOI: 10.5281/zenodo.814821

KEYWORDS: Cryptography, ciphers, authentication, Cryptographic Systems.

ABSTRACT

Today's high speed digital world has eased the process of data transmission. Large amount of data can be transferred in small amount of time which has raised a big question on the secrecy of data, since it can easily be accessed and modified by any third party. Digital Steganography is the science of communicating secret data in an appropriate multimedia carrier such that the existence of communication remains hidden.

Cryptography means "secret writing". It is the art and science of concealing the messages to introduce secrecy in information security. It has various aspects such as data confidentiality, data integrity, authentication, and non-repudiation, which are central to modern cryptography.

A cryptosystem is an implementation of cryptographic techniques and their accompanying infrastructure, to provide information security services. Choosing a secure cryptosystem is not enough, it is also important to make sure that the system is used in a manner that does not compromise its security. In this review paper, we provide the analysis of available open source cryptographic systems.

INTRODUCTION

Cryptography is one of the many aspects that ensure computer security. Cryptography is about constructing and analyzing protocols that prevent third parties from reading private messages. [1]

Four important aspects of cryptography are:- confidentiality(which ensures that the message or data does not fall into the wrong hands), integrity(ensuring that data is not changed), authentication(meaning that the receiver can verify that the message was indeed sent by the sender) and non-repudiation(meaning that the sender cannot deny sending the message.) [2]

Use of cryptosystems, also alert the adversary that some sensitive information is being transmitted and so they put all efforts on cryptanalysis of the messages or somehow intercepting them.

There are many problems inherent in using cryptosystems such as:

- Key exchange: When both the sender and receiver, wish to communicate using a secret key cryptosystem, they must agree on a key known only to them before starting the transmission of the messages.
- Man in the middle attack: When the sender and receiver decide to exchange the key by using public-key cryptography and some malicious person tries to destroy communication between two.
- Digital signatures: The sender can digitally sign his/her message while sending it to the receiver and vice versa to ensure that the message is coming from an authenticated source.
- Timestamps: Message can also be "digitally stamped" with the time of its sending. [2]

In cryptography, encryption is the process of obscuring information to make it unreadable without special knowledge. E**ncryption** is the process of encoding a message or information in such a way that only authorized parties can access it.

A *cipher* (or *cypher*) is a pair of algorithms that create the encryption and decryption. The detailed operation of a cipher is controlled by the algorithm and the key. The key is a secret (ideally known only to the communicants),

usually a short string of characters, which is needed to decrypt the cipher text. Ciphers are often used directly for encryption or decryption without authentication or integrity checks. [1]

A "cryptosystem" is the ordered list of elements of finite possible plaintexts, finite possible cypher texts, finite possible keys and the encryption and decryption algorithms which correspond to each key. There are two kinds of cryptosystems: **symmetric and asymmetric**. [1]

In symmetric systems the same key (the secret key) is used to encrypt and decrypt a message. Symmetric models include AES (Advanced Encryption Standard) and DES (Data Encryption Standard). [2]

Asymmetric systems use a public key to encrypt a message and a private key to decrypt it. Use of asymmetric systems enhances the security of communication. Examples of asymmetric systems include RSA (Rivest- Shamir-Adleman) and ECC (Elliptic Curve Cryptography). Data manipulation in symmetric systems is faster than asymmetric systems as they generally use shorter key lengths.[2]

Cryptanalysis is the term used for the study of methods for obtaining the meaning of encrypted information without access to the key i.e. it is the study of how to crack encryption algorithms or their implementations.[2]

Classic Cryptography
Classic cryptography is concerned with developing algorithms which may be used to conceal the context of the message from all except the sender and recipient and verify the correctness of a message to the recipient.[5]

The main classical cipher types are **transposition ciphers and substitution ciphers**. Transposition ciphers rearrange the order of letters in a message (e.g., 'hello world' becomes 'ehlol owrdl' using a simple rearrangement scheme) and substitution ciphers systematically replace letters or groups of letters with other letters or groups of letters (e.g., 'fly at once' becomes 'gmz bu podf' by replacing each letter with the one following it). Simple versions of either have never offered much confidentiality from enterprising opponents. [5]

An early version of substitution cipher is the Caesar cipher, in which each letter in the plaintext was replaced by a letter some fixed number of positions further down the alphabet.

Vigenère cipher is another substitution cipher which uses a *key word*, that controls letter substitution depending on which letter of the key word is used.[5]

Modern cryptography
Modern cryptography relies on publicly known mathematical algorithms for coding the information. Secrecy is obtained through a secrete key which is used as the seed for the algorithms. The computational difficulty of algorithms, absence of secret key, etc., make it impossible for an attacker to obtain the original information even if he knows the algorithm used for coding. Modern cryptography requires the sender and the receiver in secure communication to possess only the secret key. [6]

Digital data is represented in strings of binary digits (bits) unlike alphabets. Modern cryptosystems need to process these binary strings to convert in to another binary string. In Symmetric-key cryptography, both the sender and receiver share the same key. Symmetric key ciphers are implemented as either block ciphers or stream ciphers. [6]

A block cipher takes input in blocks of plaintext. The Data Encryption Standard (DES) and the Advanced Encryption Standard (AES) are block ciphers. A stream cipher is a symmetric key cipher where plaintext digits are combined with a pseudorandom cipher digit stream (keystream). In a stream cipher, each plaintext digit is encrypted one at a time with the corresponding digit of the keystream, to give a digit of the cipher text stream. RC4 is a widely used stream cipher [7]

Cryptographic hash functions
Cryptographic hash functions take a message of any length as input and output a short, fixed length hash, which can be used in (for example) a digital signature. For good hash functions, an attacker cannot find two messages that produce the same hash. Eg MD-4 and MD-5 were widely used.[1]

Cryptosystems
One or more cryptographic primitives are often used to develop a more complex algorithm, called a cryptographic system, or *cryptosystem.*[2]

In public-key cryptosystems, the public key may be freely distributed, while its paired private key must remain secret. Here the *public key* is used for encryption while the *private* or *secret key* is used for decryption. Diffie–Hellman key exchange protocol is widely used in secure communications to allow two parties to secretly agree on a shared encryption key.[2]

OPEN SOURCE CRYPTOSYSTEMS

2.1 **Bitlocker** - It is an open source software available in disk encryption category for Windows 8.1 or Windows 7 users. It can encrypt full volumes using AES-256 and can leverage boot PINs, TPM modules and two-factor authentication to secure access to the data on the volume.[3]
Bitlocker can be applied to the operating system volume, to other volumes individually or to all volumes on a machine. Recovery keys can be stored in Active Directory, making this a very good choice for the enterprise that wants to ensure the company never loses access to encrypted data.[3]

2.2 **Disk Cryptor:** It is an open source software that can encrypt entire volumes using AES 256, Twofish, and Serpent. It takes advantage of AES offloading in newer CPU models, works with Linux and Windows and can be used with external USB drives and optical media as well. [3]

2.3 **FileVault**: It is specially developed for Mac users. It uses 128 bit AES and requires you to set up a recovery key. The operating system uses an encrypted sparse disk image (a large single file) to present a volume for the home directory.[3]
When FileVault is enabled the system invites the user to create a master password for the computer. If a user password is forgotten, the master password or recovery key may be used to decrypt the files instead.[8]

2.4 **The Linux Unified Key Setup**: It comes with Ubuntu Linux to provide full disk in their operating system too. It's a selectable option during install and uses AES 128 to secure your data. [3]
Shredding- When we want to give away or donate a drive, we need to be sure there is nothing on drive and all our data has been permanently deleted from it. [3]The following two softwares are used for this purpose:-

2.5 **Eraser** - When you delete a file, the operating system does not really remove the file from the disk, it only removes the reference of the file from the file system table. The file remains on the disk until another file is created over it and even after that, it might be possible to recover data by studying the magnetic fields on the disk platter surface.[9]
Before the file is overwritten, anyone can easily retrieve it with a disk maintenance or an undelete utility. So, this software provides secure deletion of data from storage.[9]

2.6 **Darik's Boot and Nuke (**DBAN) – It deletes information stored on hard disk drives (HDDs) in PC laptops, desktops or servers. It also removes viruses/spyware from Microsoft Windows installations.[3]

File encryption softwares:-

2.7 **AES Crypt -** It is open source file encryption software that uses AES-256 that can run on Windows, Linux, Mac and even iOS and Android devices. [3]
AES Crypt is the perfect tool for anyone who carries sensitive information with them while traveling, uploads sensitive files to servers on the Internet or wishes to protect sensitive information from being stolen from home or office. AES Crypt is also the perfect solution for those who wish to backup information and store the data at a bank, in a cloud-based storage service and any place where sensitive files might be accessible by someone else.[10]

2.8 **Challenger** - It can encrypt files and folders on local storage and is available at no charge for personal use but also with enterprise class features including more options for key length and the ability to encrypt remote data on network drives.[3]
Challenger is ideal for all security aware users, especially in areas such as patent development, development engineers, journalists, lawyers and upper level management. Challenger has been developed for local data protection and communication in closed networks. It excels not only through its secure encryption algorithm but also through its ease of use.[11]

Steganography Softwares:-

2.9 **Steg -** It runs on Linux, Windows, OS X and can be used to securely hide data inside of other files. Steg's best feature may be that you can evaluate the changes that will be made to the host file so that you can determine if they will be obvious to anyone who views the file that something else is going on. [3]

2.10 **OpenPuff -** It is a program for securely encrypting and hiding files inside of other files. It has unique layers of security and obfuscation like 256bit+256bit symmetric-key cryptography (with KDF4 password extension) and 256bit symmetric-key data scrambling (CSPRNG-based shuffling). [12]

Email encryption Softwares:-

2.11 **iSafeguard** offers a freeware version that users can use to both sign and encrypt email and its attachments.[3] It provides low cost, easy to use and highly secure encryption and digital signature solutions for every type of users. Our software is used to:

- Sign and encrypt your files of any types.
- Sign and encrypt your emails.
- Search Internet Directory Services for other people's certificates.
- Backup your data securely
- Wipe files and disk free space to ensure deleted files are safe from recovery.
- Manage the passwords of your online accounts
- Supports smartcards/security tokens. [13]

2.12 **HushMail -** It is a service used when you need to send an encrypted email and/or attachments. There are both free and premium versions of the service available. [3]
When you use Hushmail, you own your data and your emails are not analyzed to display advertising. Your data is never sold to anyone. [14]

2.13 **Sbwave** - It is also used to send an encrypted mail by simply using your browser. The recipient needs a valid email address and the password to decrypt the message. [3]
The Encryption Code is NOT included with the email. The encryption code must be communicated to the recipient by phone, in person or by any secure method. The email recipient must know the exact code that was used to encrypt the message. Extra spaces, changes in case, missing or additional punctuation will prevent decryption.[15]

Portable drive encryption softwares:-

2.14 **Rohos Mini Drive** – It enables you to encrypt and password protect USB drives and local directories using AES-256. The free version can encrypt up to an 8GB partition and we can purchase a license for larger disks.[3]
It creates an encrypted partition or container on a USB flash drive or portable hard disk. Encrypted partition is protected by a password. [16]

2.15 **Bitlocker to Go** – It is available for Windows 8.1 or Windows 7. This can encrypt portable media using AES-256. [3]

2.16 **SecurStick** – It is another portable media encryption tool that uses AES-256 to secure all the data stored on USB drives and removable media. One major advantage of using SecurStick is that we do not have to be an administrator on our workstation to use it. Also it works in Windows, Linux and Mac operating systems. [3]

Remote management encryption Softwares:-

2.17 **OpenSSH** - It is a secure command-line administrative service and client for administering Linux systems. [3] It is the premier connectivity tool for remote login with the SSH protocol. It encrypts all traffic to eliminate eavesdropping, connection hijacking and other attacks. [17]

2.18 **PowerShell** - It is the remote management tool for Windows. It can use HTTPS to provide session-based encryption, but even connections over HTTP are encrypted using HTTP-Kerberos-session.[3]

2.19 **Remote Desktop Connection Manager** – It is a Windows tool from Microsoft that lets you manage multiple remote connections using RDP to your various Windows servers. RDP connections use encryption and you can also securely store credentials to your servers in encrypted connection files so you can easily and securely remote into your systems. [3]

Multitasker Softwares:-

2.20 **7-Zip** - It is a compression program that can encrypt files using AES-256. It also integrates into the Windows Explorer menu, can compress-encrypt-email as an attachment in one click and makes working with all formats of compressed files easy. It a good multipurpose tool.[3]

2.21 **GPG** - It has the ability to encrypt files, directories, volumes, emails, attachments and runs on Windows, Linux and Mac. [3]

2.22 **Sophos Free Encryption** – It can be used to encrypt files or directories and can also be used to send encrypted attachments to emails. [3]

2.23 **Cloudfogger** - It is a useful tool for providing file level encryption for cloud storage services like Dropbox, Box, OneDrive, etc. It can also be used to encrypt files stored locally or stored to portable media, ensuring encryption of all your data. [3]

ANALYSIS

We can analyze some of the above described cryptosystems on the basis of following properties:-

- Pre-boot authentication: Whether authentication can be required before booting the computer, thus allowing one to encrypt the boot disk.
- Custom authentication: Whether custom authentication mechanisms can be implemented with third-party applications.
- Multiple keys: Whether an encrypted volume can have more than one active key.
- Hardware acceleration: Whether dedicated cryptographic accelerator expansion cards can be taken advantage of.
- Two-factor authentication: Whether optional security tokens are supported.

Name	Pre-boot authentication	Custom authentication	Multiple keys	Hardware acceleration	Two-factor authentication
Bit Locker	No	Yes	Yes	Yes	Yes
Disk-cryptor	No	No	No	No	No
File Vault	No	No	Two passwords	-	No
File Vault 2	No	No	Yes	Yes	No
Loop-AES	No	Yes	Yes	Yes	Yes
GPG Disk	No	-	Yes	-	Yes
Safe Guard Easy	No	No	Yes	No	Yes
Safe Guard Enterprise	No	No	Yes	No	Yes
Safe Guard Private Disk	No	No	Yes	No	Yes

CONCLUSION

We have studied different types of open source cryptographic systems that can be used for secure communication between the sender and the receiver. We have also analysed some of them on the basis of 5 features namely, Pre-boot authentication, Custom authentication, Multiple keys, Hardware acceleration and Two-factor authentication. All of the softwares have their own pros and cons and have their own importance based on its utility. These softwares can also be categorised as File encryption softwares, Steganography Softwares, Email encryption Softwares, Portable drive encryption softwares, Remote management encryption Softwares and Multitasker Softwares.

REFERENCES

1. https://en.wikipedia.org/wiki/Cryptography
2. Alasdair McAndrew, Introduction to cryptography with Open Source software, CRC Press, A Chapman and Hall Book, 2011.
3. https://techtalk.gfi.com/the-top-24-free-tools-for-data-encryption/
4. https://en.wikipedia.org/wiki/Comparison_of_disk_encryption_software
5. https://www.eng.tau.ac.il/~yash/crypto-netsec/classical.htm
6. https://www.tutorialspoint.com/cryptography/modern_cryptography.htm
7. https://en.wikipedia.org/wiki/Stream_cipher
8. https://en.wikipedia.org/wiki/FileVault
9. https://eraser.heidi.ie/
10. https://www.aescrypt.com/
11. http://www.encryption-software.de/challenger/en/index.html
12. http://embeddedsw.net/OpenPuff_Steganography_Home.html
13. http://www.mxcsoft.com/
14. https://www.hushmail.com/about/
15. http://www.sbwave.com/enkryptor/encrypt.html
16. http://www.rohos.com/products/rohos-mini-drive/
17. http://www.openssh.com/