ORIGINAL RESEARCH PAPER
Volume - 11 | Issue - 07 | July - 2022 | PRINT ISSN No. 2277 - 8179 | DOI : 10.36106/ijsr
INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH

A SYNOPSIS OF PURE AND APPLIED CRYPTOGRAPHY

Information Technology

MaherAli Rusho

ABSTRACT

The literature of cryptography has a curious story. Secracy, of course , played a central role ,but until the first World war , important developments appeared in print in a more or less timely fashion. After the first world war ,however things began to change.US. Army and Navy organizations working entirely in secret. In the "imitation Game " we see that Allen turing build a machine called "The Enigma Machine ". And using statistical method he inspired to win The world war . This was an extraordinary example of the application of mathematics to see how math works in every section of life. I am going to write a series of paper of cryptology for everyone . It will be a good reading for anyone interest in cryptology and want to know more !!

KEYWORDS

Encryption , Decryption , plain text ,Cypher-text Symmetric Algorithm , Public-Key Algorithm , Known Plain -Text attack ,Rubber-hose cryptoanalysis , chosen cyper-text attack ,Security of Algorithms,Steganography

INTRODUCTION

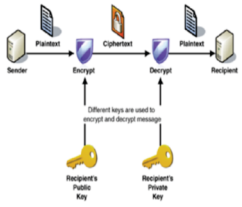
Sender and Receiver:-

Suppose a sender wants to send a message to a receiver . Moreover this sender wants to send a message securely. She wants to make sure an eavesdropper can not read the message .

Messages and Encryption :

A message is a plaintext (Sometimes called cleartext).The process of disguising a message in such a way as to hide it's substance is encryption .An encrypted message is ciphertext . The process of disguising a message and turning cypher-text back into plain text is decryption. The art and science of keeping messages secure is cryptography .

The process of encryption and decryption can be seen by this

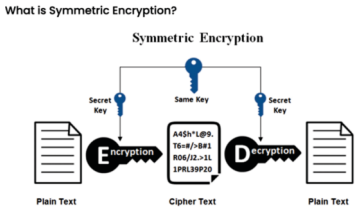


src: https://www.ssl2buy.com/wiki/what-is-encryption-and-decryption

eavesdroppers knows your algorithm ;if she doesn't know your particular key ,she can'r read you message. A cryptosystem is a algorithm plus all possible plaintext ,cipher text and keys .

Symmetric Algorithms :

There are two general types of key-based algorithm: symmetric and Public key . Symmetrical algorithms, sometimes called conventional algorithms ,are the algorithms where the encryption key can be calculated from the decryption key and vice versa . In most symmetric algorithms,sometimes called conventional algorithms ,are algorithms where the encryption key can be calculated from thedecryption key and vice versa . In most symmetric algorithm the encryption and decryption key are the same . .These algorithms are also called the secret key algorithm ,single key algorithm or one-key algorithm ,require that the sender and receiver agree on a key before they can communicate securely . The security of a symmetric algorithm rests in the key . divulging the key means that anyone could encrypt and decrypt messages.



SRC: https://www.ssl2buy.com/wiki/symmetric-vs-asymmetric-encryption- what-are-differences

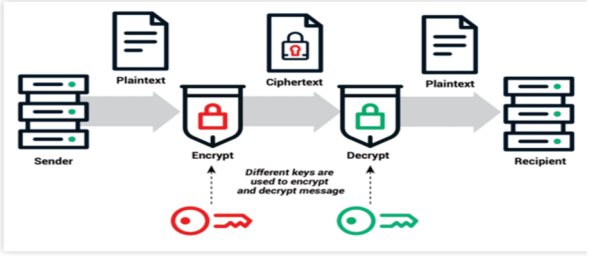
Encryption and decryption with a symmetric algorithm are defined by mathematically :

$E_{k(M)}$=C---------(1)

D^{k}(C-)=M------(2)

Symmetrical algorithms can be divided into two catagories . Some operate on the plaintext a single bit or spme byte . these are called stream ciphers . Others operate on the plain text in group of bits , .The group of bits are called blocks . large enough to preclude analysis and small enough to be workable . Before computers algorithms generally operated on a plain text one character at a time . This is also a stream of characters .

[Public-KeyAlgorithms:-



The motivation for using public key authentication over simple passwords is security. Public key authentication provides cryptographic strength that even extremely long passwords can not offer. With SSH, public key authentication improves security considerably as it frees the users from remembering complicated passwords (or worse yet, writing them down).

In addition to security public key authentication also offers usability benefits - it allows users to implement single sign-on across the SSH servers they connect to. Public key authentication also allows automated, passwordless login that is a key enabler for the countless secure automation processes that execute within enterprise networks globally. Public key cryptography revolves around a couple of key concepts. The sections below explain these.

Asymmetric Cryptography - Algorithms

As with any encryption scheme, public key authentication is based on an algorithm. There are several well-researched, secure, and trustworthy algorithms out there - the most common being the likes of RSA and DSA. Unlike the commonly known (symmetric or secret-key) encryption algorithms the public key encryption algorithms work with two separate keys. These two keys form a pair that is specific to each user.

Key Pair - Public and Private

In the SSH public key authentication use case, it is rather typical that the users create (i.e. provision) the key pair for themselves. SSH

implementations includeeasily usable utilities for this (for more information see ssh-keygen and ssh- copy-id).

Each SSH key pair includes two keys:

- A public key that is copied to the SSH server(s). Anyone with a copy of the public key can encrypt data which can then only be read by the person who holds the corresponding private key. Once an SSH server receives a public key from a user and considers the key trustworthy, the server marks the key as authorized in its authorized_keys file. Such keys are called authorized keys.
- A private key that remains (only) with the user. The possession of this key is proof of the user's identity. Only a user in possession of a private key that corresponds to the public key at the server will be able to authenticate successfully. The private keys need to be stored and handled carefully, and no copies of the private key should be distributed. The private keys used for user authentication are called identity keys.

Setting Up Public Key Authentication for SSH

The following simple steps are required to set up public key authentication (for SSH):

1. Key pair is created (typically by the user). This is typically done with ssh- keygen.
2. Private key stays with the user (and only there), while the public key is sent to the server. Typically with the ssh-copy-id utility.
3. Server stores the public key (and "marks" it as authorized).
4. Server will now allow access to anyone who can prove they have the corresponding private key.

Handling of the Private Key

It is extremely important that the privacy of the private key is guarded carefully. For most user-driven use cases this is accomplished by encrypting the private key with a passphrase.

When a private key is needed the user is asked to supply the passphrase so that the private key can be decrypted. The handling of passphrases can be automated with an SSH agent.

In most automated use cases (scripts, applications, etc) the private keys are not protected and careful planning and key management practises need to be excercised to remain secure and compliant with regulatory mandates.

From Chaos to Order - SSH Key Management

In environments where users are free to self-provision authentication keys it is common that over the years the numbers of provisioned and deployed keys grow very large. Since there is no way to find out who owns or has originally provisioned a given public key found on a server, and since these keys never expire, the true state of access control in large unmanaged environments can be very unclear or outright chaotic.

Managing and controlling access to servers and other IT infrastructure is a legal requirement for any enterprise that operates on regulated markets such as finance, energy, healthcare, or commerce. These enterprises need to employ solutions for SSH key management to control the access granted by SSH keys.]

Given from [SRC: https://www.ssh.com/academy/ssh/public-key-authentication]

Even though the public key and private key are different but they are symbolized by same mathematical processes.\

Cryptoanalysis:

The whole point of crytptography is to keep the plain text (or the key or both)secret from eavesdroppers .There are four genral types of cryptoanalytic attacks :

1) Cipher-text Only attack

GIVEN : P1,C1=$E_{K(P1),P2,C2=\ E}^{(K)(P2),C\text{---------}C}$I=EK(PI)

DEDUCE: EITHER k or an algorithm to infer pi+1 from Ci+1

2)Known -plain text attack

3)Chosen plain text attack

4)Adaptive chosen plain text attack

5)Chosen-Cipher text attack

6)Chosen-Key attack

7)Robber =-hose cryptoanalysis

We afe giving just one example of cryptoanalysis because all other analytic attacks are same formate in mathematicallySteganography: Steganography serves to hide secret messages in other messages .such that the secret's very existence is concealed . Generally the sender writes an innocuous message and then conceals a secret message on the same piece of paper . Historical tricks include hidden and invisible link . Pencil marks on typewritten characters ,minute difference between hand written characters , grills which covers most of the message except for a few characters .

What Are Some Examples of Steganography?

Steganography breaks down into five types

Text Steganography

This type of steganography involves using white spaces, capital letters, tabs, and other characters

.Audio Steganography

Audio steganography is used with digital audio formats like WAVE, MIDI, and AVI MPEG, using echo hiding, parity coding, and LSB coding, to name a few.

Video Steganography

Video steganography deals with video formats like H.264, Mp4, MPEG, and AVI. In addition, it employs pictures to carry concealed data.

Image Steganography

Pixel intensities are employed to hide information.

Network Steganography

[Network protocols use TCP, UDP, and IP as carriers.Text steganography is arguably the easiest type to work with. Obviously, writing is a simple exercise and doesn't require special skills or tools. People can use text steganography in many everyday uses. Steganography, however, has specific conditions of its use. For instance, everyone in the message chain, for example, must be aware that there's a hidden message. The secret would be lost if the reader is unaware of the code! Remember to let the recipient know that they should be looking for the embedded message. Eventually, they'll find it.

Steganography also covers certain instances of watermarks embedded in images. Anyone who has worked with online photo collections has encountered watermarks on licensed images. Though not all such watermarks are considered steganography, some steganographic techniques store watermarks in data.

Now for that promised fun exercise. Take a look at the previous paragraph. There's a top-secret message embedded in it! Can you find the message? If not, you'll find the answer at the end of the article!

Other steganography examples include:

- Writing with invisible ink
- Embedding text in a picture (like an artist hiding their initials in a painting they've done)
- Backward masking a message in an audio file (remember those stories of evil messages recorded backward on rock and roll records?)
- Concealing information in either metadata or within a file header
- Hiding an image in a video, viewable only if the video is played at a particular frame rate
- Embedding a secret message in either the green, blue, or red channels of an RRB imageSteganography can be used both for constructive and destructive purposes. For example, education and business institutions, intelligence agencies, the military, and certified ethical hackers use steganography to embed confidential messages and information in plain sight.

On the other hand, criminal hackers use steganography to corrupt data files or hide malware in otherwise innocent documents. For example, attackers can use BASH and PowerShell scripts to launch automated attacks, embedding scripts in Word and Excel documents. When a poor, unsuspecting user clocks one of those documents open, they activate the secret, hidden script, and chaos ensues. This process is a favored ransomware delivery method.] Given from : https://www.simplilearn.com/what-is-steganography-article

Security of Algorithms :

Lars Knusdsen classified these different catagories of breaking an algorithm >in decreasing order of severity :

1) Total Break: A cryptanalyst finds the key ,K ,such that D_k ©=P
2) Global Deduction ; A cryptoanalyst finds an alternative algorithm ,A,equivalent to $D_{k©\ ,Without}$ knowing K
3) Instance Deduction: A cryptoanalyst finds the plaintext of an intercepted ciphertext
4) information deduction: A cryptanalyst gains some information about the key or plaintext .

There are some complexity of algorithms like

1) Data Complexity
2) Processing Complexity
3) Storage requirements

Historical Terms=>

Historically a code refers to a cryptosystem that deals with linguistic units ,words ,phrases ,sentences and so forth .For example the word "OCELOT" might be the cipher text of "Turn left 90 degrees" .If you say "LOLIPOP" It's cipher text is TURN RIGHT 90 DEGREES".If your code has no entry for "ANTEATERS" Then you can not say anything about Cipher text >

REFERENCES:

1) Book of Bruice Scaneier of App lied Cryp tology
2) https://en.wikipedia.org/wiki/Encryption
3) https://www.simplilearn.com/what-is-steganography-article
4) https://www.simplilearn.com/what-is-steganography-article
5) https://www.ssl2buy.com/ wiki/what -is-encryption-and decry ption
6) https://www.ssl2buy.com/wiki/symmetric-vs-asymmetric-encryption-
7) https://www.ssl2buy.com/wiki/what-is-encryption-and-decryption
8) https://www.schneier.com/books/applied-cryptography/
9) https://www.schneier.com/essays/archives/2016/04/the_value of_encrypt.html
10) https://www.schneier.com/essays/national/