Collage of Natural and computational science

Department of Mathematics

Project on cryptography

Prepared by: Yodit Samson

Advisor: Waltengus Dagne

A project submitted to the Department of Mathematics, Wolkite University in partial Full filament of the Requirements of the Bachelor of Science Degree in Mathematics

Contents

Acknowledgment

Frist of all I would like to give special thanks to God because he is the main cause for me to be in this level Next my sincere thanks to all my Family who have been constant source of encouragement and financial support throughout my study. I also want to thank Faculty of Natural and computational science Department of Mathematics and I would like to express my deep gratitude and grateful respect to my Advisor Waltengus Dagne (M.sc) for his patient guidance, encouragement and use full critiques of this project.

Abstract

The project is an over view of the cryptography and its encryption methods. It specially focuses on cryptography common encryption methods. Chapter one starts by define the context of cryptography and the security services it occurs. It also defines well cryptography algorithms by classifying in two main groups symmetric-key and Asymmetric-key with examples. In chapter two widely describes about RSA Key Generating method. It deeply expresses how to encrypt and decrypt by using RSA, Encryption Algorithm.

Chapter one

Introduction

1.1. Short story of Cryptography

Human Bing from ages had two inherent needs to communicate selectively. These two needs gave rise to the art of coding the messages in such a way that only the Intended people could not extract any information, even if the scrambled messages fill in their hand. The art of cryptography is considered be born along with the art of writing

As civilization evolved, human beings got organized in tribes, groups and kingdoms. This led to the emergence of ideas such as power, battles supremacy and p the natural need of people to communicate selectively with selective recipient who in turn ensured the continuous evolution of cryptography as well. The roots of cryptography are found in Roman and Egyptian civilization. The art and science of concealing the messages to introduce secrecy in information security is recognized as cryptography. The word cryptography was coined by combining two Greek words 'krypto' meaning hidden and 'graphene' writing.

The development of digital computers and electronics after 2^{nd} world war made possible much more complex chipper. Furthermore, computers allowed for the encryption of any kind of data represent able in any binary format unlike classical ciphers which only encrypted written language this was new and significant.

Basic Terms

- **Encryption:** The process by which plaintext is converted into cipher text.
- **Decryption:** Recovering plain text from the cipher text
- **Cryptanalysis:** The study of "breaking the code".
- **Cryptology:** Cryptography and cryptanalysis together constitute the area of cryptology.

1.2. Context of Cryptography

Cryptology, the study of cryptosystems, can be subdivided into two branches

- Cryptography and Cryptanalysis

Cryptography is the science and art of transforming messages to make them secure from attacks.

Cryptography deals with the actual securing of digital data. It refers to the design of mechanisms based on mathematical algorithms that provide fundamental information security services. You can think of cryptography as the establishment of a large toolkit containing different techniques in security applications. Cryptography is the art and science of making a cryptosystem that is capable of providing information security.

The sender uses an encryption algorithm and the receiver uses a decryption algorithm.

1.3. Security Services of Cryptography

The primary objective of using cryptography is to provide the following four fundamental information security services.

Let us now see the possible goals intended to be fulfilled by cryptography.

- **Confidentiality** is the fundamental security service provided by cryptography. It is a security service that keeps the information from an unauthorized person. It is sometimes referred to as privacy or secrecy. Confidentiality can be achieved through numerous means starting from physical securing to the use of mathematical algorithms for data encryption.
- **Data Integrity** It is security service that deals with identifying any alteration to the data. The data may get modified by an unauthorized entity intentionally or accidently. Integrity service confirms that whether data is intact or not since it was last created, transmitted, or stored by an authorized user. Data integrity cannot prevent the alteration of data, but provides a means for detecting whether data has been manipulated in an unauthorized manner.
- **Authentication** provides the identification of the originator. It confirms to the receiver that the data received has been sent only by an identified and verified sender.
- **Non-repudiation** it is a security service that ensures that an entity cannot refuse the ownership of a previous commitment or an action. It is an assurance that the original creator of the data cannot deny the creation or transmission of the said data to a recipient or third party. Non-repudiation is a property that is most desirable in situations where there are chances of a dispute over the exchange of data. For example, once an order is placed

electronically, a purchaser cannot deny the purchase order, if non-repudiation service was enabled in this transaction.

Cryptography has five ingredients:

- **Plain text**-The original message, before being transform
- **Chiphrtext** -After the message is transformed.
- **Secret key**- Used to set some or all of the parameters/numbers used by the encryption algorithm.
- **Decryption algorithm**-transforms the cipher text back in to plain text.

Security depends on the secrecy of the key, not the secrecy of the algorithm

To encrypt a message, we need an encryption algorithm, encryption key, and the plain text. These create the Chiphrtext. To decrypt a message we need a decryption algorithm, a decryption key, and the cipher text .This reveal the original plaintext. .we can divide all the cryptography algorithms (ciphers) into two groups:

- Symmetric-key (secret key) cryptography algorithm and
- Asymmetric-key Cryptography

1.3.1. Symmetric-key Cryptography

Symmetric-key cryptography started thousands of years ago when people needed to exchange secrets (for example, in a war). .we still mainly uses symmetric-key cryptography in our network security. In symmetric-key cryptography, the same key is used by both parties. The sender uses this key and an encryption algorithm to encrypt data; the receiver uses the same key and the corresponding decryption algorithm to decrypt the data. The key has to be kept secret. The key has to be communicated using a secure chases A substitution cipher text replaces one symbol with another.

Example

The following shows a plaintext and its corresponding cipher text. Is the cipher polyalphabetic?

Plaintext: EGG

Cipher text: TMH

Solution:

The cipher is probably polyalphabetic because occurrences of G's are encrypted as M and H.

Symmetric key- systems are simpler and faster, but their main drawback is that the two parties must somehow exchange the key in a secure way. Public key can be distributed in a non-secure way, and the private key is never transmitted

Examples of symmetric algorithms are

DES, 3DES, and AES

Merits and Demerits

Merits

- Faster
- Simpler

Demerits

- Two parties must somehow exchange the key in secure way
- Public key is distribution anon secure way between clients/sever
- Easy for hackers to get the key as it is shared in unsecure way.

1.3.2. Asymmetric-key Cryptography

In Asymmetric-key Cryptography, there are two keys: public key and private key.

The private key is kept by the receiver.

The public key is announced to the public

In public key encryption/decryption, the public key that is used for encryption is different from the private key that used for decryption.

Examples

Use the shift cipher with key =15 to decrypt the message "WTAAD" Solution We decrypt one character at a time. Each character is shifted 15 characters up. Letter W is decrypted to H Letter T is decrypted to E The first A is decrypted to L the second A is decrypted to L And finally D is decrypted to O The plaintext is HELLO.

Example, 2

The following shows a plaintext and its corresponding cipher text. Is the cipher Monoalphabetic?

Plaintext: HELLO

Chiphrtext: ABNNF

Solution:

The cipher is not polyalphabetic it is Monoalphabetic because each occurrence of L is encrypted by the same character. Both encrypted as N .The shift cipher is sometimes referred to as the Caesar cipher. .In this cipher the encryption algorithm is "shift key characters down' 'with key equal some number. .The decryption algorithm is "Shift key characters up"

Example

Use the shift cipher with key=15 to encrypt the message "CAFE" Solution We encrypt one character at a time. Each character is shifted 15 characters down. Letter C is encrypted to R Letter A encrypted to p Letter F encrypted to U Letter E encrypted to T. The cipher text is RPUT.

.

1.3.3. APPLICATON OF CRYPTOGRAPHY

- Secure communication
- To prevent eavesdropping war time communication and business transactions.
- Identification and Authentication.
- Checking the integrity.
- Secret sharing /data hiding
- Hide something that has been written
- E-commerce/ E-payment
- Certification

Certification is a scheme by which trussed agents such as certifying authorities guarantee for unknown agents, such as users.

- Key recovery
- It is a technology that allows a key to be reveled under certain circumstances without the owner of the key revealing it.
- Remote access
- Password gives a level of security for secure access
- Cell phone
- Prevent people from stealing cellphone numbers access or eavesdropping.
- Access control
- Regulate access to satellite and cable TV
- E-mail
- Smart cards
- ATM.

This day's affine example of cryptography is credit card with smart card capabilities. The 3-by-5-mm chip embedded in the card. Smart cards combine low coast and probability with the power to compute cryptographic algorithms

Chapter Two

RSA-key Generating method

RSA is a public -key Cryptosystem that is widely used for secure data transmission.it is also one of the oldest. The acronym RSA comes from the surnames of Ron Rivist, Adi Shamir and Leonard Adelman who publicly described the algorithm in 1977. The RSA algorithm is an asymmetric cryptography algorithm this means that it uses a public key and private key.

Key Generation of RSA

Pair each person or a party who desires to participate in communication using encryption needs to generate a pair of keys, namely public key and private key. The process followed in the generation of keys is described below

- ✓ Generate the RSA modulus n
  - Select two large primes, p and q.
  - Calculate $n = p \times q$. For strong unbreakable encryption, let n be a large number, typically a minimum of 512 bits.
- ✓ Find Derived Number e
  - Number e must be greater than 1 and less than$(p-1)(q-1)$
  - There must be no common factor for e and p−1q−1 except for 1. In other words two numbers e and $(-1)(q-1)$ are cop prime.
- ✓ Form the public key
  - The pair of numbers n,e form the RSA public key and is made public.
  - Interestingly, though n is part of the public key, difficulty in factorizing a large prime number ensures that attacker cannot find in finite time the two prime's p & q used to obtain n. This is strength of RSA. Numbers e and $p-1q-1$ are cop rime.
- ✓ Generate the private key
  - Private Key d is calculated from p, q, and e. For given n and e, there is unique number d.
  - Number d is the inverse of $e\ modulo(p-1)(q-1)$. This means that d is the number less than $p-1q-1$ such that when multiplied by e, it is equal to1 $modulo(p-1)(q-1)$.

- relationship is written mathematically as follows

$$ed = 1\ mod(P-1)(q-1)$$

The Extended Euclidean Algorithm takes p, q, and e as input and gives d as output.

Example

2.1. RSA-Encryption and Decryption

- **RSA-Encryption**
  - **sender a dose the following1**
  - Obtains the recipient B's public key (n, e) .
  - Recipients the plaintext message m^e e as a positive integer m .
  - Compute the cipher text c=m mod n .
  - Sends the cipher text C to B

RSA-Decryption

- Recipient B doses the following.
- uses his private key (n, d) to compute m =c^d mod n
- Extracts the plaintext from the message representative m

Example

Encryption (5, 14)

Text =2

2^5(Mod 14)=32 (mod 14)

=4(mod 14)

Cipher text=D =4

Decryption (11, 14)

$\mathbf{4^{11}}$(Mod 14)=4194304(mod 14)

=299593.1429…..

2(mod 14) =B

Bob use the following steps to select the private and public keys:

1,Bob chooses two very large prime numbers p and q. Remember that a prime number is one that can be divide evenly only by one I and itself.

2, Bob multiplies the above two primes to find n, the modulus for encryption and decryption. IN other words, $\boldsymbol{n = p \times q}$.

3, Bob calculates another number $\boldsymbol{F = (p - l) \times (q - I)}$

4, Bob chooses a random integer e. He then calculates d so that $\boldsymbol{d \times e = I \bmod F => dxe - I}$ evenly divide F

5, Bob announces e and n to the public he keeps F and d secret.

Example

1. We have to pick two prime no p and q Let p=2, q=7
2. Then we have to find N $N = P \times Q$ 2 × 7 =14 SO N= 14
3. $\varphi(N) = (P - 1)(q - 1)$

   = (2-1) (7-1)

   =1 × 6

   N= 6
4. Choose $(1 < e < \varphi(N)$

   Co-prime with $N, \varphi(N)$

We have to Pick out co prime with N=6 the numbers between 1 up to 6.Now let's cheek

(2, 3, 4, 5) between this numbers only 5 is does not have a common factor with 6 so know we get our e = 5

5. Choose D =$de\big(mod\varphi(n)\big) = 1$

   $5d(mod\ 6) = 1$

   (5, 11)

Conclusion

In this project, we have presented on our view of Cryptography and its encryption methods. In this project Cryptography described well and one of its encryption method RSA. cryptography protects the security of data and to protect confidentiality, integrity and authenticity of data at rest beyond standard content encryption. Each Encryption Method have its own Encryption and decryption methods and we have tried to see How to Encrypt and decrypt our data by using the above encryption Algorithm RSA.

Bibliography

1, Cryptography and NETWORK SECURITY (4TH Edition William Stallings

2, Cryptography Quick Guide

3, Hand book of applied cryptography

3, Google searches