International Journal of Research

International Journal of Research (IJR)

e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 05, May 2015

Available at http://internationaljournalofresearch.org

Science and Study of Secret Writing: Cryptography

Ms. Parveen Kumari

Asst. Prof. in CISKMV Fatehpur Pundri (Kaithal)

Pinubattan5@gmail.com, battanparveen8@gmail.com

Abstract:

Cryptographic systems become essential in today's online communication. Effectiveness of the Cryptography: A Security Measure". Cryptography defined as "the science and study of secret writing,". The basic service provided by cryptography is the ability to send information between participants in a way that prevents others from reading it. Computer data often travels from one computer to another. Once the data is out of hand, people with bad intention could modify or forge your data for their own benefit. Cryptography can transform and reformat our data, making it safer on its path between computers. The technology that protects our data in powerful ways is based on the essentials of secret codes, augmented by modern mathematics. The goal of cryptography is CIA (Confidentiality, Integrity and Availability) Confidentiality: Information while exchange should remain secret. Integrity: Technique to ensure integrity of data. Availability: Data must be available to authorized users. In this paper we will look at some basic principal of cryptography, Cryptography technique encryption & decryption with its basic components. We will look at a glance about Keys, Cipher, Intruder etc. we will examine some of the fundamental algorithm used for cryptography these are Symmetric Key and Public Key algorithms. Cryptography is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. The term most often associated with scrambling plain text (ordinary text) into cipher text (the process called Encryption) then back again (by the process known as decryption).

Cryptography is the science of using mathematics to encrypt and decrypt data. Cryptography enables you to store sensitive information or transmit it across insecure networks (like the Internet) so that it cannot be read by anyone except the intended recipient.

Keywords: Cryptography; Encryption; Decryption; Techniques; Communication; Keys; Cipher text etc

Abbreviation:

DES, ATM, USA, AES, RSA, CIA.

Introduction:

In today's life communications such as electronic mail or the use of World Wide Web browsers are not secure for sending and receiving information. The sending information may be their sensitive personal data that should not be intercepted. Everyone wants a secure, private communication with the other part, we can say that no one wants the third parties read their E-mails or alter their content.

Cryptography comes from the Greek words for 'secret writing'. Except for physical layer security, nearly all security is based on cryptography principal. This is the science of providing security for information. Modern electronic crypto systems use complex mathematical algorithms & technique.

Historically: The groups that have and contributed to the art of cryptography are: The military, the diplomatic crops, the diarists, the lovers etc. All of these the military had played important role in this field, over the centuries.

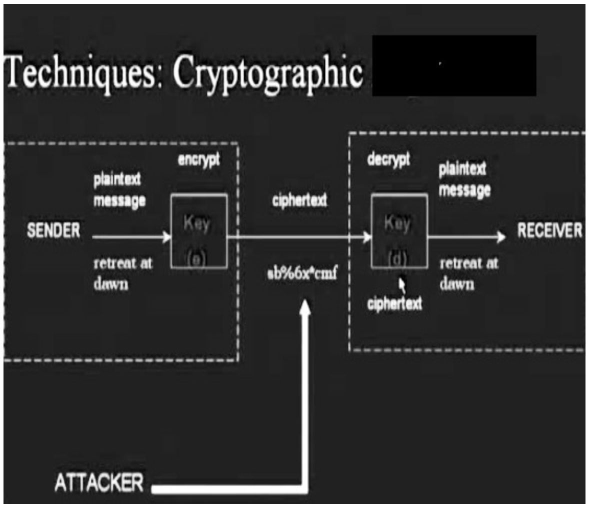
The most successful code ever devised was used by the U.S. Armed forces during world was second in pacific.

Model of Cryptography:

Active Intruder   **Passive Intruder**

↓   ↓

Plain text   Encryption Method   Cipher Text   Decryption Method   Plaintext
(Sender Site)   (Encryption Key K_1)   ($C=E_k$ (P))   (Decryption Key,K_2)   (Receiver Site)



Plaintext:

The Message to be encrypted and we can say a message at receiver site after Decryption. The information before it has been encrypted. The original message that sender want to sent.

Key:

Info used in cipher known only to sender/receiver

- **Symmetric $k_1=k_2$**
- **Asymmetric $k_1 \neq k_2$**

Cipher text:

This text comes after Encryption Process. Many encryption systems carry many layers of encryption, in which the cipher text output becomes the plaintext input to another encryption layer. The process of decryption takes cipher text and transforms it back into the original plaintext.

Intruder:

One of the most publicized attacks to security is the intruder, generally referred to as hacker or cracker. We assume that the enemy hears and accurately copies down the complete text, but he does not know the decryption key. That's why they can't decrypt the cipher text easily.

- **Active Intruder**
- **Passive Intruder**

Sometimes these intruders not only listen the communication but can also record even can play them message back latter. But the active intruder can inject his own Message or modify before this get to receiver.

Encryption and Decryption:

Encryption is one specific element of cryptography in which one hides data or information by transforming it into an unreadable code. Encryption is basically a suggestion of users' suspect of the security of the system, the owner or operator of the system, or law enforcement authorities." Encryption is also used to protect data being transferred between devices such as Automatic Teller Machines (ATMs), Mobile Telephones, and many more. Encryption is most used among transactions over insecure channels of communication, such as the internet. Encryption typically uses a specified parameter or key to perform the data transformation. Encryption is used in everyday modern life. Some encryption algorithms require the key to be the same length as the message to be encoded, yet other

encryption algorithms can operate on much smaller keys relative to the message. Encryption can be used to create digital signatures, which allow a message to be authenticated.
Decryption of encrypted data results in the original data. Decryption is often classified along with encryption as it's opposite.

Classical Encryption Techniques

Substitution Techniques

Mono Alphabetic:

In this technique a particular alphabet is replaced by a single character. Even if there may be more than one occurrence of signal character. This is Symbol for Symbol substitution.
Example: Attack is transferred to QZZQEA.

M A R A C T
M D R D C T

Poly Alphabetic:

When at different occurrence it is replaced by different alphabet. Signal Character is replaced every time by different alphabet.

M A R A C T
M D R S C T

Caesar:

This is the oldest method, in which a becomes d, b becomes e, c becomes f,……….., and z becomes c, for example, attack becomes dwwdfn. (In example, plaintext is given in lower case letters and cipher text in uppercase letters).
Caesar cipher allows the cipher text alphabet to be shifted k letters, instead of always z then k become a key.

One Time Pad

It is an unbreakable cryptosystem. It represents the message as a sequence of 0s and 1s.this can be accomplished by writing all numbers in binary, for example, or by using ASCII. The key is a random sequence of 0‟s and 1‟s of same length as the message. Once a key is used, it is discarded and never used again.
The system can be expressed as
Follows:
Ci = Pi Ki Ci - ith binary digit of cipher text
Pi - ith binary digit of
Plaintext Ki - ith binary digit of key
Exclusive OR operation
Thus the cipher text is generated by performing the bitwise XOR of the plaintext and the key. Decryption uses the same key. Because of the properties of XOR, decryption simply involves the same bitwise operation:
Pi = Ci Ki
e.g., plaintext = 0 0 1 0 1 0 0 1
Key = 1 0 1 0 1 1 0 0
Cipher text = 1 0 0 0 0 1 0 1

Advantage:
Encryption method is completely unbreakable for a cipher text only attack.
Disadvantages
It requires a very long key which is expensive to produce and expensive to transmit.
Once a key is used, it is dangerous to reuse it for a second message; any knowledge on the first message would give knowledge of the second.

Transposition Techniques

A very different kind of mapping is achieved by performing some sort of Permutation on the plaintext letters. This technique is referred to as a transposition cipher. Reorder the letter by column matrix or by other encoding methods.

Rail fence:

Rail Fence is simplest of such cipher, in which the plaintext is written down as a sequence of diagonals and then read off as a sequence of rows.
Plaintext = meet at the school house
To encipher this message with a rail fence of depth 2, we write the message as follows:
m e a t e c o l o s
e t t h s h o h u e
The encrypted message is
MEATECOLOSETTHSHOHUE

Row Transposition Ciphers:

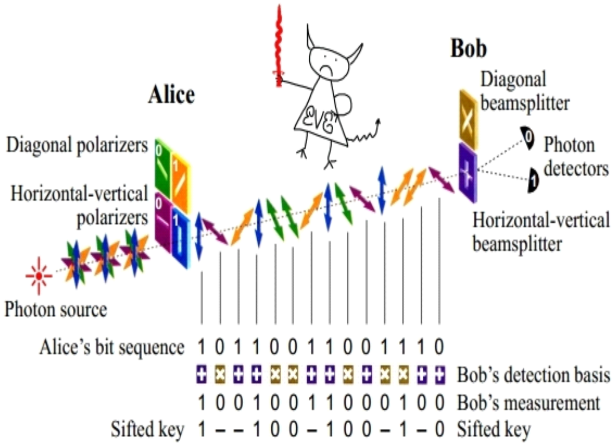
A more complex scheme is to write the message in a rectangle, row by row, and read the message off, column by column, but permute the order of the columns. The order of columns then becomes the key of the algorithm.
e.g., plaintext = meet at the school house

Key = 4 3 1 2 5 6 7
PT = m e e t a t t
h e s c h o o
l h o u s e

CT = ESOTCUEEHMHLAHSTOETO
A pure transposition cipher is easily recognized because it has the same letter frequencies as the original plaintext. The transposition cipher can be made significantly more secure by performing more than one stage of transposition. The result is more complex permutation that is not easily reconstructed.

Quantum cryptography:

Describes the use of quantum mechanical effects (in particular quantum communication and quantum computation) to perform cryptographic tasks or to break cryptographic systems. Well-known examples of quantum cryptography are the use of quantum communication to exchange a key securely (quantum key distribution) and the hypothetical use of quantum computers that would allow the breaking of various popular public-key
encryption and signature schemes
(e.g., RSA and El Gamal).The advantage of quantum cryptography lies in the fact that it allows the completion of various cryptographic tasks that are proven or conjectured to be impossible using only classical (i.e. non-quantum) communication (see below for examples). For example, quantum mechanics guarantees that measuring quantum data disturbs that data; this can be used to detect eavesdropping in quantum key distribution.


Bob
Diagonal beamsplitter
Photon detectors
Horizontal-vertical beamsplitter
Alice
Diagonal polarizers
Horizontal-vertical polarizers
Photon source
EVE
Alice's bit sequence 1 0 1 1 0 0 1 1 0 0 1 1 1 0
Bob's detection basis
1 0 0 1 0 0 1 1 0 0 0 1 0 0 Bob's measurement
Sifted key 1 – – 1 0 0 – 1 0 0 – 1 – 0 Sifted key

Quantum cryptography Technique

Cryptography Principal:

- **Redundancy:**

  Message Must Contain Redundancy. The first principle is that all encrypted messages must contain some redundancy, that is, information not needed to understand the message. Cryptographic principle 1: “**Messages must contain some redundancy.**” In other words, upon decrypting a message, the recipient must be able to tell whether it is valid by simply inspecting it and perhaps performing a simple computation. This redundancy is needed to prevent active intruders from sending garbage and tricking the receiver into decrypting the garbage and acting on the "plaintext. "However, this same redundancy makes it much easier for passive intruders to break the system.

- **Freshness:**

  Some method is needed to replay Foil Attacks. The second cryptographic principle is that some measures must be taken to ensure that each message received can be verified as being fresh, that is, sent very recently. This measure is needed to prevent active intruders from playing back old messages. Cryptographic principle 2: "**Some method is needed to foil replay attacks.**" One such measure is including in every message a timestamp valid only for, say, 10 seconds. The receiver can then just keep messages around for 10 seconds, to compare newly arrived messages to previous ones to filter out duplicates. Messages older than 10 seconds can be thrown out, since any replays sent more than 10 seconds later will be rejected as too old.

Algorithms for Cryptography:

- **Symmetric Key with DES and AES**
- **Public Key RSA Algorithms**

Symmetric (Private) key:

Private Key systems use a single key. The single key is used both to encrypt and decrypt the information. Both sides of the transmission need a separate key and the key must be kept secret from. The security of the transmission will depend on how well the key is protected. The US Government developed the Data Encryption Standard ("DES") which operates on this basis and it is the actual US standard. DES keys are 56 bits long. The length of the key was criticised and it was suggested that the short key was designed to be long enough to frustrate corporate eavesdroppers, but short enough to be broken by the National Security Agency ("NSA"). Export of DES is controlled by the State Department. DES system is getting old and becoming insecure. US government offered to replace the DES with a new algorithm called Skipjack which involves escrowed encryption.

The encryption and decryption keys are known both to sender and receiver. The encryption key is shared and the decryption key is easily calculated from it. In many cases, the encryption and decryption keys are the same.

Public key:

In the public key system there are two keys: a public and a private key. Each user has both keys and while the private key must be kept secret the public key is publicly known. Both keys are mathematically related. If A encrypts a message with his private key then B, the recipient of the message can decrypt it with A's public key. Similarly anyone who knows A's public key can send him a message by encrypting it with his public key. A will than decrypt it with his private key. Public key cryptography was developed in 1977 by Rivest, Shamir and Adleman ("RSA") in the US. This kind of cryptography is more efficient than the private key cryptography because each user has only one key to encrypt and decrypt all the messages that he or she sends or receives. Encryption key is made public, but it is computationally infea.

RSA example:

We pick two prime numbers *p* and *q*:

p = 251

q = 269

The number n is therefore:

n = 251 * 269 = 67519

The Euler Totient function for this value is:

$\phi(n)$ = (251-1) (269-1) = 67000

Let's arbitrarily pick e as 50253. d is then:

d = e^{-1} mod 67000 = 27917

Because:

50253 * 27917 = 1402913001 = 20939 * 67000 + 1 = 1 (mod 67000)

Using n = 67519 allows us to encode any message M that is between 0 and 67518. We can therefore use this system to encode a text message two characters at a time. (Two characters have 16 bits, or 65536 possibilities.) Using e as our key, let's encode the message "RSA works!" The sequence of ASCII characters encoding "RSA works!" is shown in the following table

RSA Encoding Example:

ASCII	Decimal Value	Encoded Value
"RS"	21075	48467
"A"	16672	14579
"wo"	30575	26195
"rk"	29291	58004
"s!"	29473	30141

As you can see, the encoded values do not resemble the original message. To decrypt, we raise each of these numbers to the power of d and take the remainder mod n. After translating to ASCII, we get back the original message. When RSA is used for practical applications, it is used with numbers that are hundreds of digits long. Because doing math with hundred-digit-long strings is time consuming, modern public key applications are designed to minimize the number of RSA calculations that need to be performed. Instead of using RSA to encrypt the entire message, RSA is used to encrypt a session key, which itself is used to encrypt the message using a high-speed, private key algorithm such as DES or IDEA.

Conclusion:

In Modern World Cryptographic System based on the principal of having a algorithm public and keys secret. Algorithms of Public Key and Private Key have their own ways to secure the cipher text. Here we conclude that algorithms need not to keep in more privacy, but key should be. However if Quantum Cryptography can be made Practical, the use of one time pads may provide truly unbreakable crypto system cryptographic system is Public key system and private key system.

Reading List and Bibliography:

[1.] Computer Networks 4th Edition bynAndrew S. Tanenbaum.

[2.] William Stallings, “Cryptography and Network Security: Principals and Practice”, Pearson Education.

[3.] Cryptography and Network Security Principles and Practice, 5th Edition.

[4.] Ast, Present, And Future Methods of Cryptography and Data Encryption: A Research Review byNicholas G. McDonald Nicholas G. McDonald Department of Electrical and Computer Engineering University of Utah.

[5.] Anderson,"Why Cryptosystem Fail", Communication of ACM, Vol. 37, PP 32-40, Nov., 1984.

[6.] Aderson," Security Engineering, New York: Wiley, 2001.

[7.] Aderson," Network Security, 2nd Ed.

[8.] Behrouz A. Frouzan: Cryptography and Network Security, TMH.

References:

[1.] http://www.leeds.ac.uk/law/pgs/yaman/cryptog.htm.

[2.] https://sites.google.com/site/gtublog/sem4/640001/fundamentalcryptographicprinciples

[3.] http://b2b.cbsimg.net/blogs/qkd2.jpg

[4.] https://www.google.co.in/#q=quantum+cryptography

[5.] http://www.uptu.ac.in/pdf/sub_eit_701_30sep14.pdf

[6.] http://textofvideo.nptel.iitm.ac.in/106105031/lec2.pdf

[7.] http://www.ggu.ac.in/download/Class-Note14/public%20key13.02.14.pdf

[8.] ftp://ftp.pgpi.org/pub/pgp/7.0/docs/english/IntroToCrypto.pdf