CRYPTOGRAPHY

Dr. Vinod Kumar
Assistant Professor
Department of Computer Science
Dev Samaj College for Women
Ferozepur City

Er.Gagandeep Raheja
Assistant Professor
Department of Computer Science
Dev Samaj College for Women
Ferozepur City

Ms Subeena Sareen
Assistant Professor
Department of Computer Science
Dev Samaj College for Women
Ferozepur City

ABSTRACT

To prevent the dissemination of sensitive information from the database to unauthorized users or outside competitive or hostile agents, an organization must establish effective security policies. The art of protecting information by transforming it into an unreadable format, called cipher text. Only those who possess a secret key can decipher (or decrypt) the message into plain text. Encrypted messages can sometimes be broken by cryptanalysis, also called codebreaking, although modern cryptography techniques are virtually unbreakable. Database security policies are guidelines for present and future decisions regarding the maintenance of the database security. Database security mechanisms are the functions used to enforce the database security policies. There are number of security policies that can be applied on data in order to protect the data against unauthorized access. Protecting the data is the prime need of an organization.

KEYWORDS: Ciphertext, encryption, decryption, plain text.

1.1 INTRODUCTION

Cryptography is the practice and study of techniques for secure communication in the presence of third parties. It is about constructing and analyzing protocols that overcome the influence of adversaries and which are related to various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation.

1.2 DATA ENCRYPTION

Data encryption is a process in which plaintext data is converted into ciphertext so that it cannot be read. Often it is hard to prevent people from copying the database and then hacking into the copy at another location. It is easier to simply make copying the data a useless activity by encrypting the data. This means that the data itself is unreadable unless you know a secret code. The encrypted data in combination with the secret key is needed to use the DBMS.

Data encryption encodes the data such that nobody can understand the actual data contents. His encryption not only useful to secure the data stored on disks but also for exchanging the information over a network. This encoded data can be decoded (decrypted) only by than authorized users that know what the code is Authorization security control ensures that only privileged user can manipulate the data in the way they are allowed to do. The database management system must determine that which users are allowed to perform which functions and which data portion is accessible by them.

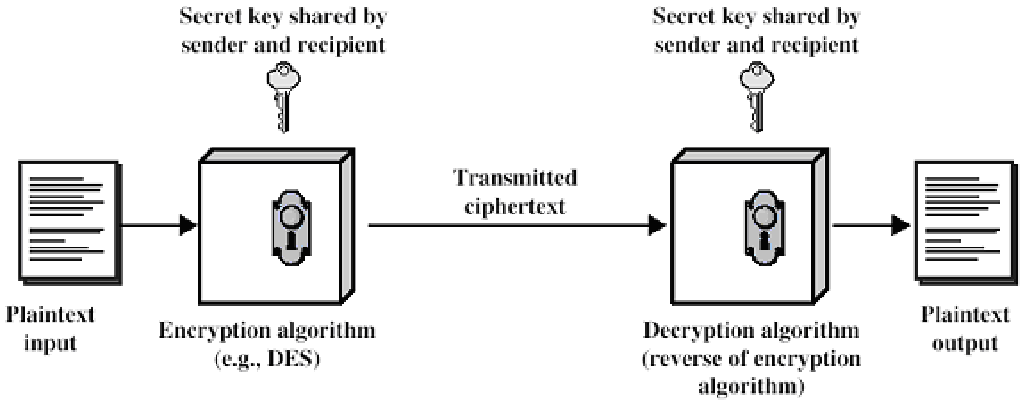
Authorization controls are different in a centralized database to the distributed database environment. Authorization control definition in a distributed database system is derived from that in centralized system but in the context of distributed system some additional complexity is also considered.

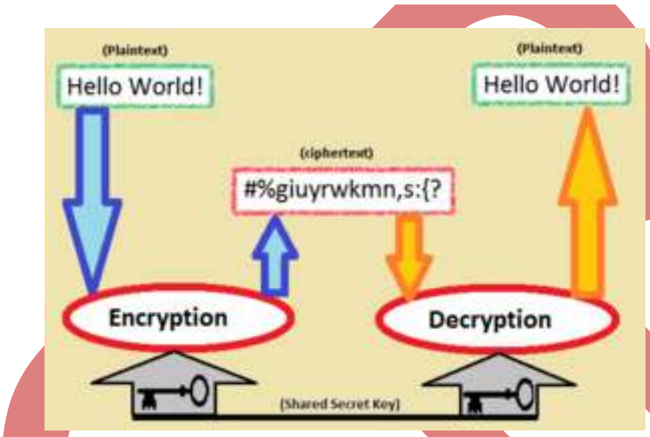
1.3 CONVENTIONAL ENCRYPTION

The Conventional encryption was the only encryption available before the introduction of public key encryption. It is also called symmetric encryption or single key encryption. A conventional encryption scheme has five stages:

- ✓ Plaintext
- ✓ Encryption algorithm
- ✓ Secret Key
- ✓ Ciphertext
- ✓ Decryption algorithm

- **Plain Text:** It is the original message that is used for input.
- **Encryption Algorithm:** It performs different transformations on the plain text.
- **Secret Key:** It is input to encryption algorithm.
- **Cipher Text:** It is the scrambled message as an output. As we know that we have number of encrypted methods so the cipher text depends upon the plain text and the secret key used for the encryption.
- **Decryption Algorithm:** It performs on cipher text and gives the original message as an output.


Secret key shared by sender and recipient
Secret key shared by sender and recipient
Transmitted ciphertext
Plaintext input
Encryption algorithm (e.g., DES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output



An encryption algorithm transfers the sender's plaintext using the secret key into ciphertext. The encrypted message can be sent via insecure path. Using the same private key, the algorithm applies an inverse transformation to ciphertext to reconstruct the original message.

1.4 TECHNIQUES USED FOR ENCRYPTION

There are basically two techniques used for data encryption and they are as under:

1.4.1 TRANSPOSITION CIPHER

A transposition cipher is a method of encryption by which the positions held by units of plaintext (which are commonly characters or groups of characters) are shifted according to a regular system, so that the ciphertext constitutes a permutation of the plaintext. That is, the order of the units is changed. Transposition ciphers encrypt plaintext by moving small pieces of the message around. Anagrams are a primitive transposition cipher. This text shows "**VOYAGER**" being encrypted with a primitive transposition cipher where every two letters are switched with each other:

Plaintext: VOYAGER

Ciphertext: OVAYEGR

However this method is not very good from the security point of view. So other rules for encryption can also be used and for permutation to form four character block and permute as 1234 to 3124. So the original plain message will become: **YVOARGE.**

1.4.2 SUBSTITUTION CIPHER

In cryptography, a substitution cipher is a method of encryption by which units of plaintext are replaced with ciphertext according to a regular system; the "units" may be single letters (the most common), pairs of letters, triplets of letters, mixtures of the above, and so forth. The receiver deciphers the text by performing an inverse substitution.

Substitution ciphers can be compared with transposition ciphers. In a transposition cipher, the units of the plaintext are rearranged in a different and usually quite complex order, but the units themselves are left unchanged. By contrast, in a substitution cipher, the units of the plaintext are retained in the same sequence in the ciphertext, but the units themselves are altered.

There are a number of different types of substitution cipher. If the cipher operates on single letters, it is termed a simple substitution cipher; a cipher that operates on larger groups of letters is termed polygraphic. A monoalphabetic cipher uses fixed substitution over the entire message, whereas a polyalphabetic cipher uses a number of substitutions at different times in the message, where a unit from the plaintext is mapped to one of several possibilities in the ciphertext and vice-versa.

Substitution over a single letter—simple substitution—can be demonstrated by writing out the alphabet in some order to represent the substitution. This is termed a substitution alphabet. The cipher alphabet may be shifted or reversed (creating the Caesar and Atbash ciphers, respectively) or scrambled in a more complex fashion, in which case it is called a mixed alphabet or deranged alphabet. Traditionally, mixed alphabets are created by first writing out a keyword, removing repeated letters in it, and then writing all the remaining letters in the alphabet.

Examples

Using this system, the keyword "zebras" gives us the following alphabets:

Plaintext alphabet: abcdefghijklmnopqrstuvwxyz

Ciphertext alphabet: ZEBRASCDFGHIJKLMNOPQTUVWXY

Example: vinod can be written as UFKLR

1.5 DATA ENCRYPTION STANDARD

The Data Encryption Standard (DES) is a block cipher that was selected by the National Bureau of Standards as an official Federal Information Processing Standard (FIPS) for the United States in 1976 and which has subsequently enjoyed widespread use internationally. It is based on a symmetric-key algorithm that uses a 56-bit key.

DES is the archetypal block cipher — an algorithm that takes a fixed-length string of plaintext bits and transforms it through a series of complicated operations into another ciphertext bitstring of the same length. In the case of DES, the block size is 64 bits. DES also uses a key to customize the transformation, so that decryption can supposedly only be performed by those who know the particular key used to encrypt.

The key ostensibly consists of 64 bits; however, only 56 of these are actually used by the algorithm. Eight bits are used solely for checking parity, and are thereafter discarded. Hence the effective key length is 56 bits, and it is usually quoted as such.

Like other block ciphers, DES by itself is not a secure means of encryption but must instead be used in a mode of operation.

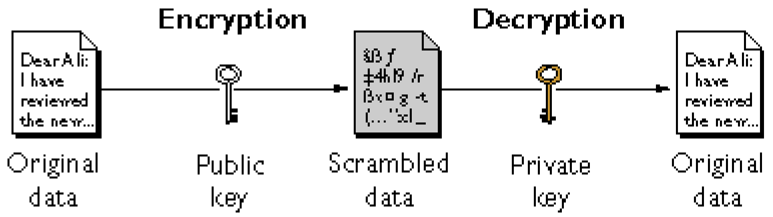
1.6 PUBLIC KEY ENCRYPTION

The concept of "public key" was first developed in the 1970's to solve the problem of exchanging the key over a network. Since everyone connected to the network has the receiver's public key, anyone can send him/her a message by encrypting it with that public key. Only the receiver can read the message by decrypting it with his/her private key. In this way, there is no need to exchange a sensitive or secret key, reducing the risk of exposing the message. In cryptography, a public key is a value provided by some designated authority as an encryption key that, combined with a private key derived from the public key, can be used to effectively encrypt messages and digital signatures.

Public key encryption refers to a type of cipher architecture known as public key cryptography that utilizes two keys, or a key pair), to encrypt and decrypt data. One of the two keys is a public key, which anyone can use to encrypt a message for the owner of that key. The encrypted message is sent and the recipient uses his or her private key to decrypt it. This is the basis of public key encryption.

Public key encryption is considered very secure because it does not require a secret shared key between the sender and receiver. Other encryption technologies that use a single shared key to both encrypt and decrypt data rely on both parties deciding on a key ahead of time without other parties finding out what that key is. However, the fact that it must be shared between both parties opens the door to third parties intercepting the key. This type of encryption technology is called symmetric encryption, while public key encryption is known as asymmetric encryption.

Data encrypted with your public key can be decrypted only with your private key.



The distinguishing technique used in public key-private key cryptography is use of asymmetric key algorithms because the key used to encrypt a message is not the same as the key used to decrypt it. Each user has a pair of cryptographic keys — a public key and a private key. The private key is kept secret, while the public key may be widely distributed. Messages are encrypted with the recipient's public key and can only be decrypted with the corresponding private key. The keys are related mathematically, but the private key cannot be feasibly (ie, in actual or projected practice) derived from the public key. It was the discovery of such algorithms which revolutionized the practice of cryptography beginning in the middle 1970s.

1.6.1 Advantages

- The primary advantage is increased security and convenience. Since the receiver decrypts the message by using his/her private key, there is no need to expose the secret key to the insecure transmission medium. This is a convenient and secure property of public key encryption.
- They provide a method for digital signature, which prevents a sender from denying the validity of a previously authenticated message.

1.6.2 Disadvantages

- In most cases, public key systems, such as PGP (Pretty Good Privacy), are much slower than secret key systems. If the message sent is too big, public key systems will need to encrypt large amounts (for example, megabytes) of data, which will take a long time. Therefore, public key systems are more suitable for encrypting small amounts of data, such as messages sent through email.

1.7 RSA PUBLIC KEY ENCRYPTION ALGORITHM

In 1977, shortly after the idea of a public key system was proposed, three mathematicians, Ron Rivest, Adi Shamir and Len Adleman gave a concrete example of how such a method could be implemented. To honour them, the method was referred to as the RSA Scheme. The system uses a private and a public key. To start two large prime numbers are selected and then multiplied together; n=p*q.

If we let f(n) = (p-1) (q-1), and e>1 such that GCD(e, f(n))=1. Here e will have a fairly large probability of being co-prime to f(n), if n is large enough and e will be part of the encryption key. If we solve the Linear Diophantine equation; ed congruent 1 (mod f(n)), for d. The pair of integers (e, n) are the public key and (d, n) form the private key. Encryption of M can be accomplished by the following expression; Me = qn + C where 0<= C < n. Decryption would be the inverse of the encryption and could be expressed as; Cd congruent R (mod n) where 0<= R < n. RSA is the most popular method for public key encryption and digital signatures today.

1.8 CONCLUSION

In the last few years cryptography and cryptographic protocols became a part of our everyday life. Here are a few examples. When sending an e-mail, we are sometimes asked" do you need encoding"? an owner of a smart bank card addressing the bank through a terminal starts with the card authentication. Users of the internet surely know about discussions concerning the adoption of the digital signature standards for pages containing crucial information

REFERENCES

http://www.webopedia.com/TERM/C/cryptography.html

http://www.google.co.in/imgres?imgurl=http://upload.wikimedia.org/wikipedia/commons/thumb/f/f8/Crypto.png/300px-Crypto.png&imgrefurl=http://en.wikipedia.org/wiki/Cryptography&h=201&w=300&sz=38&tbnid=mbjtkrg-mmtXfM:&tbnh=82&tbnw=123&zoom=1&usg=__SQm9-A6cWtR1JwtsYRJd9LVAi9s=&docid=ghih9TsPuuKjAM&hl=en&sa=X&ei=OOXuUPu8HYbekgXDwYHIAQ&sqi=2&ved=0CEMQ9QEwAw&dur=3900