A

Seminar report

on

Cryptography

Submitted in partial fulfillment of the requirement for the award of degree

Of Computer Science

SUBMITTED TO:

www.studymafia.com

SUBMITTED BY:

www.studymafia.com

Preface

I have made this report file on the topic **Cryptography**; I have tried my best to elucidate all the relevant detail to the topic to be included in the report. While in the beginning I have tried to give a general view about this topic.

My efforts and wholehearted co-corporation of each and everyone has ended on a successful note. I express my sincere gratitude to ……..who assisting me throughout the preparation of this topic. I thank him for providing me the reinforcement, confidence and most importantly the track for the topic whenever I needed it.

Index

- Introduction
- What is Cryptography?
- Purpose Of cryptography
- Architecture of cryptography
- Types of Cryptography
- Process of cryptography
- Types Of cryptography Algorithms
  Attacks of cryptography
- Conclusion
- References

ABSTRACT

Many organizations are working hard to secure themselves from the growing threats of message hacking through various trends in cryptography. Yet the headlines are dominated with the latest news of message passing disaster more frequently than any time before.

This document intends to review this problem and propose several possible solutions. The cryptographic industry has been responding to these threats with ever-quicker responses to the rapid onslaught of malicious techniques, while corporations establish strict cryptographic techniques.

Placing organizations cryptographic techniques at the desktop level is like closing all the doors in a house…..while leaving windows and other entry points open. The present document discusses various cryptographic techniques of all times such as the three basic algorithms namely private key algorithm, public key algorithm and the hash functions. The need for having three encryption techniques has also been encrypted .

A detailed discussion has been done on the classical cryptography and the drawbacks of the classical cryptography to ensure the need for going to new trends in cryptography like *quantum cryptography*, *elliptic curve cryptography*. These new techniques that has emerged out of various exploitations in the field of cryptography rises a fair amount of hope that we can overcome the problems we are facing in a head hoc way.

These proven technologies can meet the needs of the most demanding of environments while their respective focus on manageability has automated many tasks and simplified administrative functions through easy-to-use interfaces developed through years of customer feedback. And at the end of the document we can conclude that soon we can save secrecy involved in message passing from the dangerous clutches of message hackers.

INTRODUCTION

The Internet or the global Internet is the internationally connected network of computer networks with addresses that are administrated by IANA (Internet address and Naming Authority). It grew dramatically because anyone can connect to it and anyone connected to it can connect others to it as well.

Each site that connected to it, can become an Internet Service provider to other sites Does increased security provide comfort to paranoid people? Or does security provide some very basic protections that we are naive to believe that we don't need? During this time when the Internet provides essential communication between tens of millions of people and is being increasingly used as a tool for commerce, security becomes a tremendously important issue to deal with.

There are many aspects to security and many applications, ranging from secure commerce and payments to private communications and protecting passwords. One essential aspect for secure communications is that of cryptography. This paper has two major purposes. The first is to define some of the terms and concepts behind basic cryptographic methods, and to offer a way to compare the myriad cryptographic schemes in use today. The second is to provide some real examples of cryptography and new trends in use today.

I would like to say at the outset that this paper is very focused on terms, concepts, and schemes in current use and is not a treatise of the whole field.

What is Cryptography?

Cryptography derived its name from a Greek word called “krypto’s” which means “Hidden Secrets”.

Cryptography is the practice and study of hiding information. It is the Art or Science of converting a plain intelligible data into an unintelligible data and again retransforming that message into its original form.

It provides Confidentiality, Integrity, and Accuracy.

PURPOSE OF CRYPTOGRAPHY

Cryptography is the science of writing in secret code and is an ancient art; the first documented use of cryptography is writing dates back to circa 1900 B.C. when an Egyptian scribe used non-standard hieroglyphs in an inscription. Some experts argue that cryptography appeared spontaneously sometime after writing was invented, with applications ranging from diplomatic missives to war-time battle plans.

It is no surprise, then, that new forms of cryptography came soon after the widespread development of computer communications. In data and telecommunications, cryptography is necessary when communicating over any UN trusted medium, which includes just about *any* network, particularly the Internet.

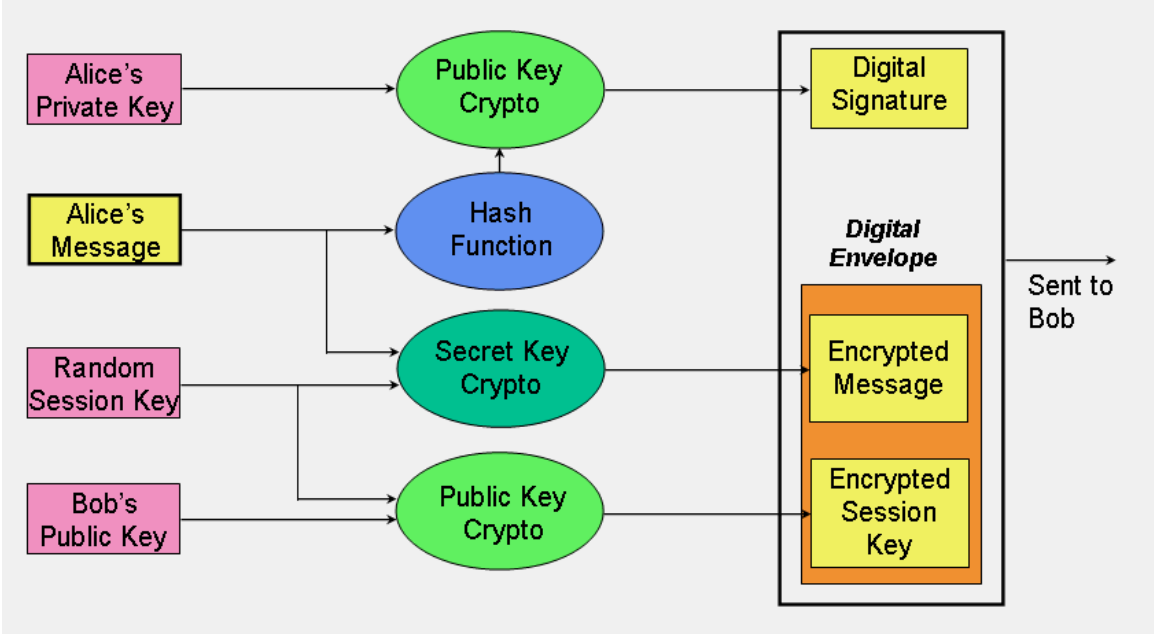
Within the context of any application-to-application communication, there are some specific security requirements, including:

- **Authentication:** The process of proving one's identity. (The primary forms of host-to-host authentication on the Internet today are name-based or address-based, both of which are notoriously weak.)
- **Privacy/confidentiality:** Ensuring that no one can read the message except the intended receiver.
- **Integrity:** Assuring the receiver that the received message has not been altered in any way from the original.
- **Non-repudiation:** A mechanism to prove that the sender really sent this message.

Cryptography, then, not only protects data from theft or alteration, but can also be used for user authentication. There are, in general, three types of cryptographic schemes typically used to accomplish these goals: secret key (or symmetric) cryptography, public-key (or asymmetric) cryptography, and hash functions, each of which is described below. In all cases, the initial unencrypted data is referred to as *plaintext*. It is encrypted into cipher text, which will in turn (usually) be decrypted into usable plaintext.

In many of the descriptions below, two communicating parties will be referred to as Alice and Bob; this is the common nomenclature in the crypto field and literature to make it easier to identify the communicating parties. If there is a third or fourth party to the communication, they will be referred to as Carol and Dave. Mallory is a malicious party, Eve is an eavesdropper, and Trent is a trusted third party.

Architecture of cryptography



Types of Cryptography

Secret Key Cryptography

• Single key used to encrypt and decrypt.
• Key must be known by both parties.
• Assuming we live in a hostile environment (otherwise - why the need for cryptography?), it may be hard to share a secret key.

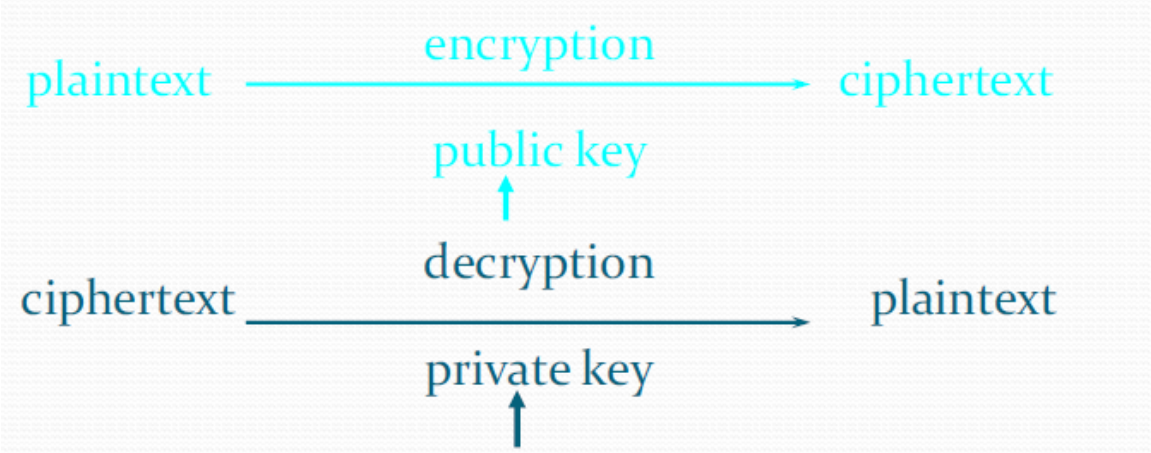
Public Key Cryptography

One of the keys allocated to each person is called the "public key", and is published in an open directory somewhere where anyone can easily look it up, for example by email address.

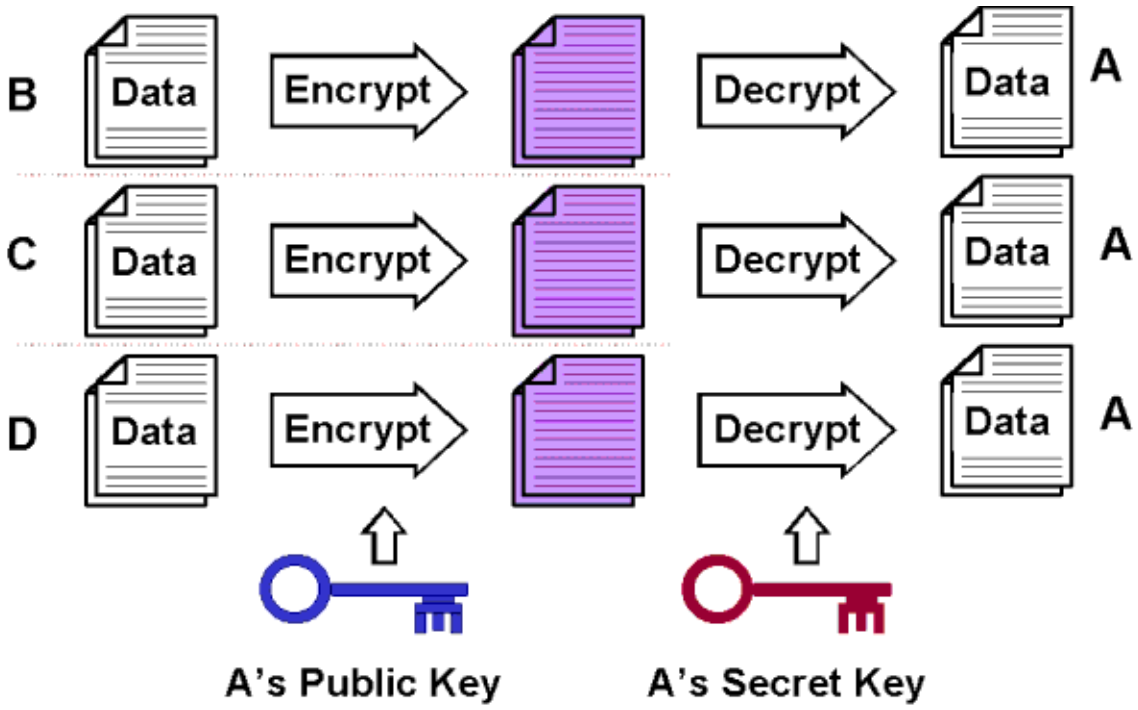
• Each entity has 2 keys:
– Private Key (A secret)
– Public key (well known).

Using Keys

• Private keys are used for decrypting.
• Public keys are used for encrypting.



Process of cryptography



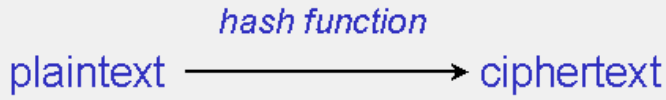
TYPES OF CRYPTOGRAPHIC ALGORITHMS

There are several ways of classifying cryptographic algorithms. For purposes of this paper, they will be categorized based on the number of keys that are employed for encryption and decryption, and further defined by their application and use. The three types of algorithms that will be discussed are

· Secret Key Cryptography (SKC): Uses a single key for both encryption and decryption
· Public Key Cryptography (PKC): Uses one key for encryption and another for decryption
· Hash Functions: Uses a mathematical transformation to irreversibly "encrypt" information

A) Secret key (symmetric) cryptography. SKC uses a single key for both encryption and decryption.

B) Public key (asymmetric) cryptography. PKC uses two keys, one for encryption and the other for decryption.



C) Hash function (one-way cryptography). Hash functions have no key since the plaintext is not recoverable from the ciphertext.

Public/Private Key Cryptography

Asymmetric key cryptography overcomes the key management problem by using different encryption and decryption key pairs. Having knowledge of one key, say the encryption key, is not sufficient enough to determine the other key - the decryption key.

Therefore, the encryption key can be made public, provided the decryption key is held only by the party wishing to receive encrypted messages (hence the name public/private key cryptography). Anyone can use the public key to encrypt a message, but only the recipient can decrypt it.

RSA is a widely used public/private key algorithm is, named after the initials of its inventors, Ronald L. Rivets, Adi Shamir, and Leonard M. Adelman [RSA 91]. It depends on the difficulty of factoring the product of two very large prime numbers. Although used for encrypting whole messages, RSA is much less efficient than symmetric key algorithms such as DES. ElGamal is another public/private key algorithm [El Gamal 85]. This uses a different arithmetic algorithm than RSA, called the discrete logarithm problem.

The mathematical relationship between the public/private key pair permits a general rule: any message encrypted with one key of the pair can be successfully decrypted only with that key's counterpart. To encrypt with the public key means you can decrypt only with the private key. The converse is also true - to encrypt with the private key means you can decrypt only with the public key.

Hash functions

"Is a type of one-way function this are fundamental for much of cryptography. A one way function - is a function that is easy to calculate but hard to invert. It is difficult to calculate the input to the function given its output. The precise meanings of "easy" and "hard" can be specified mathematically. With rare exceptions, almost the entire field of public key cryptography rests on the existence of one-way functions.

In this application, functions are characterized and evaluated in terms of their ability to withstand attack by an adversary. More specifically, given a message x, if it is computationally infeasible to find a message y not equal to x such that H(x) = H(y) then H is said to be a weakly collision-free hash function. A *strongly collision-free hash function* H is one for which it is computationally infeasible to find any two messages x and y such that H(x) = H(y).

The requirements for a good cryptographic hash function are stronger than those in many other applications (error correction and audio identification *not* included). For this reason, cryptographic hash functions make good stock hash functions--even functions whose cryptographic security is compromised, such as MD5 and SHA-1. The SHA-2 algorithm, however, has no known compromises"

hash function ca also be referred to as a function with certain additional security properties to make it suitable for use as a primitive in various information security applications, such as authentication and message integrity. It takes a long string (or message) of any length as input and produces a fixed length string as output, sometimes termed **a** message digest or a digital fingerprint.

Attacks of cryptography

1. Cipher text only attack
- The only data available is a target cipher text
2. Known plaintext attack
- A target cipher text
- Pairs of other cipher text and plaintext (say, previously broken or guessing)
3. Chosen plaintext attacks
- A target cipher text
- Can feed encryption algorithm with plaintexts and obtain the matching cipher texts
4. Chosen cipher text attack
- A target cipher text
- Can feed decryption algorithm with cipher texts and obtain the matching plaintexts

CONCLUSION

We use different types of algorithms to establish security services in different service mechanisms. We use either private key cryptography or public key cryptography according to requirement. If we want to send message quickly we use private key algorithm and if we want to send messages secretly we use public key algorithm.

References

www.studymafia.org

www.google.com

www.wikipedia.com