ORIGINAL RESEARCH PAPER

Information Technology

CRYPTOGRAPHY

KEY WORDS: Security, Cryptography, Encryption, Decryption

Shital Ganesh Kene

Asst. Prof., Department of Computers and Management, DAIMSR, Nagpur

ABSTRACT

In computer science, cryptography refers to secure information and communication techniques derived from mathematical concepts and a set of rule-based calculations called algorithms to transform messages in ways that are hard to decode. These deterministic algorithms are used for cryptographic key generation and digital signing and verification to protect data privacy, web browsing on the internet and confidential communications such as credit card transactions and email.

The requirements of information security within an organization have undergone two major changes in the last several decades. Before the widespread use of data processing equipment, the security of information felt to be valuable to an organization was provided primarily by physical and administrative means. With the introduction of computer the need for automated tools for protecting files and other information stored on the computer became an evident. This is especially the case for a shared system, such as timesharing system and the need are even more acute for systems that can be accessed for a public telephone or a data network. The generic names for the collection of tools to protect data and to thwart Hackers are "computer security".

This paper help to guide how Cryptography help to make every individual different, this is very needful now a days so people turn to prefer this technique for their privacy and security of their uniqueness and assets.

INTRODUCTION

Privacy and Authentication is the way to understand the identity of every individual. So now days it is very important tool to secure our massage from unauthorized access and stop theft of data transformation. The word "cryptography" is derived from the Greek kryptos, meaning hidden. The origin of cryptography is usually dated from about 2000 B.C., with the Egyptian practice of hieroglyphics. These consisted of complex pictograms, the full meaning of which was only known to an elite few. The first known use of a modern cipher was by Julius Caesar (100 B.C. to 44 B.C.), who did not trust his messengers when communicating with his governors and officers. For this reason, he created a system in which each character in his messages was replaced by a character three positions ahead of it in the Roman alphabet.

In recent times, cryptography has turned into a front line of some of the world's best mathematicians and computer scientists. The ability to securely store and transfer sensitive information has proved a critical factor in success in war and business.

Because governments do not wish certain entities in and out of their countries to have access to ways to receive and send hidden information that may be a threat to national interests, cryptography has been subject to various restrictions in many countries, ranging from boundaries of the usage and export of software to the public broadcasting of mathematical concepts that could be used to develop crypto systems. However, the internet has allowed the spread of powerful programs and, more importantly, the underlying techniques of cryptography, so that today many of the most advanced cryptosystems and ideas are now in the public domain.

Encryption and decryption

Cryptography can be strong or weak. Cryptographic strength can be measured in the time it takes for one to recover the plaintext. The result of strong cryptography is a cipher text that is very difficult to decipher without possession of the proper decoding tools.

According from another source, Cryptography is where security engineering meets mathematics. It provides us with tools that underlie most modern security protocols. It is widely used in the modern era to protect distributed systems from the wrong thing, or used to protect them in the wrong way.

Cryptography based on my other references is the study of methods to send and receive secret messages. The goal of cryptography to help a sender communicate a message to a receiver without the adversary learning what the message was. We know that there are tons of hackers who would want infiltrate a system and get information. Some will use that information in evil ways, some will sell it to companies and some just do it for fun. That's why cryptography is very essential to be learned and used especially when you are in the industry of modern technology.

Cryptography is also said to be the science and art of secret writing. It can protect data from unauthorized and unwanted disclosure; it can also authenticate the identity of a user of a program. So why do you think we should study cryptography? Well it is important for us to study cryptography since we are future programmers and future IT professionals because this would help us a lot especially in securing our programs. It will help us to ensure that the programs that we develop are safe from the hackers around us. It will also help us keep our job, imagine that you are responsible for the security of a system and it is infiltrated by hackers, definitely you will lose your job. Therefore as future programmers we should study and use cryptography wisely because this is very powerful but also dangerous in the hands of the wrong.

Modern cryptography concerns with:

1. **Confidentiality**: the information cannot be understood by anyone for whom it was unintended
2. **Integrity:** the information cannot be altered in storage or transit between sender and intended receiver without the alteration being detected
3. **Non-repudiation:** the creator/sender of the information cannot deny at a later stage his or her intentions in the creation or transmission of the information.
4. **Authentication:** the sender and receiver can confirm each other's identity and the origin/destination of the information.

Need of Cryptography

Everyone needs it like government, Companies, Schools, parents etc. Almost everything you use digitally requires some form of security in order to keep your data safe. Cryptography is arguably one of the most important components in fulfilling that requirement of security. Let me provide you with an example to help you draw some connections. When you log into your email or bank account, you probably see an HTTPS in the URL, followed or proceeded by a lock symbol to indicate a secure connection. HTTPS stands for Hyper Text Transfer Protocol Secure (HTTPS), and your connection to almost every single website you visit is maintained using this protocol. HTTPS uses the Secure Sockets Layer (SSL), which utilizes the RSA cryptographic scheme in order to encrypt packets that are transmitted between you and the destination server.

Extending and Applying Visual Cryptography

The lowest hanging fruit on this new research venue (in our

opinion) would be to start applying and extending the currently known visual cryptography methods. Applications for the more advanced methods have not been reported, but these could be forthcoming in suitable AR applications, for example. Another direction would be to extend the capabilities of visualizable encryption to public key cryptography, authenticated encryption, digital signatures etc. This would require also new definitions and theory for such systems. For this reason, it is probably a much harder and long-term endeavor. The main shortcoming of visual cryptography (and visualizable encryption) is that it requires a certain level of visual capability from the user, which is not available to all humans. For example, the WHO (World Health Organization) states that over 250 million people suffer from impaired vision. Out of these, approximately 36 million are totally blind. Thus, a remarkable number of people (especially elderly people) would be left out from the benefits of human cryptography, if only visual or visualizable cryptography would be available. It is interesting to note that currently CAPTCHA security questions on websites tend to have a button, which provides the visual challenge in an audible form. Having similar functionality for visual and visualizable encryption is most likely very difficult if not completely impossible.

Cryptography for Other Senses

It is peculiar to note that for other senses such as hearing, there are no cryptographic constructions similar to visual cryptography. As sound is formed of waves and with superposition one can achieve e.g. noise cancelling, it is entirely possible to think that at least similar secret sharing schemes as in visual cryptography could be fairly easy to construct. This could be formed from two or more sounds that in themselves are "random noise", but in some specific conditions cancel out to form an understandable sound of some sort. Thus, not only visual, but also auditory cryptography could be achieved. This could be another way to start expanding cryptography to human senses. After all, signification (the use of non-speech audio to convey information) is already being tested in network monitoring and situation awareness contexts. Of course, there are also other senses available for human users. The sense of smell is interesting and less applied and studied in the digital context than vision and hearing. There are some ideas on how this could be utilised in the digital world, for example in user authentication. Also synthetic odours can be realised and utilized. Whether or not scents can work as an effective method for human cryptography is an open question. The sense of smell is quite different from vision and hearing, as it is based on detecting different kinds of molecules while the other two are based on detecting electromagnetic or pressure waves. A simple way to convert a visual cryptography scheme to a scent-based scheme is probably not possible.

Cryptography concerns

Attackers can circumvent cryptography, hack into computers that are responsible for data encryption and decryption, and exploit weak implementations, such as the use of default keys. However, cryptography makes it harder for attackers to access messages and data protected by encryption algorithms.

Growing concerns about the processing power of quantum computing to break current cryptography encryption standards led the National Institute of Standards and Technology to put out a call for papers among the mathematical and science community in 2016 for new public key cryptography standards. Unlike today's computer systems, quantum computing uses quantum bits (qubits) that can represent both 0s and 1s and therefore perform two calculations at once. While a large-scale quantum computer may not be built in the next decade, the existing infrastructure requires standardization of publicly known and understood algorithms that offer a secure approach, according to National Institute of Standards and Technology. The deadline for submissions was in November 2017, analysis of the proposals is expected to take three to five years.

CONCLUSION

With the sensitive development in the Internet, information security has turned into an unavoidable sympathy toward any association whose interior private system is associated with the Internet. The security for the information has turned out to be extremely vital. Information security of every individual is a focal question over every organisation. With more scientific instruments, cryptographic plans are getting more adaptable and regularly include numerous keys for a solitary application. The paper displayed different plans which are utilized as a part of cryptography for Network security reason. Encode message with firmly secure key which is known just by sending and recipient end, is a vast point of view to procure powerful security in cloud. The safe trade of key amongst sender and receiver is an imperative task.

REFERENCES:-

1. https://www.studymode.com/essays/Cryptography
2. https://searchsecurity.techtarget.com/cryptography