# CIS 5600 - Information Security Management

## Project Proposal

# CRYPTOGRAPHY

**Instructor:** Dr. Jeremy Lanman

**Team 1**

<<Member Names>>

## ABSTRACT:

Cryptography is a method of constructing and examining protocols that overcome the impact of adversaries and which are related to various points in understanding safety comparable to data confidentiality, data integrity, and authentication. The word cryptography is derived from a Greek word which means the hidden secret and is practiced to protect the information from social gathering. Cryptography's goal is to construct schemes or protocols that may nonetheless accomplish exact tasks even in the presence of an adversary. A general challenge in cryptography is to allow users to keep up a correspondence securely over an insecure channel in a technique that guarantees their transmissions' privacy and authenticity. Progression in computing powers and parallelism technology are growing obstruction for credible security mainly in electronic expertise swapping underneath cryptosystems. Various cryptographic schemes persist wherein each has its own affirmative and feeble characteristics. Some schemes lift the usage of lengthy bits key and a few help using small key. Functional cryptosystems are both symmetric or uneven in nature. In this study, we can see the assessment of modern encryption tactics for satisfied decision of each key and cryptographic scheme. Subsequently this comprehensive survey thrash outs the cutting-edge tendencies and study issues upon cryptographic factors to conclude the upcoming requirements concerning cryptographic key, algorithm constitution and stronger privateness especially in transferring the multimedia understanding.

## KEYWORDS:

Cryptographic problems, Symmetric vs. Asymmetric, Steganography, Digital signature, Hash functions.

## SUMMARY:

Offering privacy and authenticity remains a valuable purpose for cryptographic protocols, but the area has elevated to encompass many others, including e-voting, digital coins, and at ease auctions. Cryptographic systems tend to involve each algorithm and a secret worth. The key value is referred to as the key. The reason for having a key furthermore to an algorithm is that it is intricate to hold devising new algorithms in an effort to allow reversible scrambling of understanding.

Cryptography additionally depends on encryption strategies equivalent to symmetric and asymmetric to encode the exact text message like plain textual content with the usage of secret code referred to as key. The process of encoding or encrypting the undeniable textual content is referred as enciphering or encryption and the vise versed system is referred to as decoding or decryption. Symmetric encryption requires a single shared secret code referred to as confidential key and uneven encryption is headquartered on two keys known as confidential key and public key. Personal key stays secret and public secret's publically available. In asymmetric encryption, public key's used to encrypt the message and confidential key's used to decrypt the same message. Safety is the essential controlled factor now days ordinarily issues with big understanding alternate procedure like internet. More commonly customers demand at ease verbal exchange above all in case organizational linkage, Governmental conversation and banking transactions. Cryptographic algorithms are dependable phenomena in this situation.

## MOTIVATION OF THE PROPOSED PROBLEM:

Cryptography plays a valuable role in networks and information confidentiality. Security protocols that aid to achieve distinctive security offerings make use of cryptography. Cryptography is a technology that may play fundamental roles in addressing precise varieties of expertise vulnerability. Cryptography enables individuals to preserve confidence within the digital world the place humans can do their trade on electric channel without stressful of deceit and deception.

In recent times, Confidentiality is seen because the central hindrance within the area of expertise security and cozy verbal exchange is the easy use of cryptography. The development of public-key cryptography creates a large-scale network of men and women who can verbal exchange securely with one another despite the fact that that they had never communicated earlier than. Typically, without cryptography money machines would now not be viable, because the machines would now not be ready to reliably keep in touch with the bank computers. Without cryptography, even the thought of electronic voting would not be viable. Cryptographic ideas may also be used in making message easier to decode. In an group, knowledge is the principal asset after human assets and cryptography plays a principal function in securing the expertise. Thus cryptography is principal in day-to-day life.

## MAJOR ISSUES:

In this part, we are able to see the several motives and challenges faced via cryptography. Principal hassle is the changing environment and chance items wherein cryptology will likely be deployed. When you consider that we're evolving closer to ambient intelligence, pervasive networking or ubiquitous computing, which have fully new traits, this would be a major problem. The next hindrance will also be the gradual erosion of the computational difficulty of the mathematical problems on which cryptology is based. This erosion is created partially by means of developments in and partially through progress in cryptanalytic algorithms. Additionally, the standards of recent applications and cryptographic implementations together with the dearth of physical safety in devices will also be acknowledged as an main quandary faced by cryptography.

## Types of Cryptography:

There are two main frameworks in cryptography known as:

- Secret key encryption
- Public key encryption

Secret key encryption makes use of a single key to both encrypt and decrypt messages. As such it need to be reward at both the supply and vacation spot of transmission to allow the message to be transmitted securely and recovered upon receipt on the correct vacation spot. The key ought to be kept secret by way of all events concerned within the communication. If the key falls into the fingers of an attacker, they would then be in a position to intercept and decrypt messages, therefore thwarting the try to obtain at ease communications by way of this process of encryption.

Public key encryption use a pair of keys, every of which is able to decrypt the messages encrypted by using the opposite. Furnished this kind of keys corresponding to exclusive key's kept secret, any verbal exchange encrypted utilizing the corresponding public key may also be regarded comfortable as the one person able to decrypt it holds the corresponding confidential key. The algorithmic houses of the encryption and decryption methods make it infeasible to derive a exclusive key from a public key, an encrypted message, or a blend of each.

Both the secret-key and public-key ways of cryptology have distinctive flaws. The challenge with public-key cryptology is that it's situated on the remarkable measurement of the numbers created with the aid of the combination of the key and the algorithm used to encode the message. These numbers can reach incredible proportions. The manager predicament with Secret Key algorithm is how the two customers agree on what secret key to use. The drawback with secret-key cryptology is that there's mostly a place for an unwanted third party to hear in and acquire know-how the customers do not need that character to have. This is identified in cryptology as the important thing distribution situation. It is among the quality challenges of cryptography.

In the recent decade, using high computing processors are creating a assorted situation for a symmetric encryption which are stylish on small length of key for the reason that dispensed computing can brake small key with no trouble at the same time it also faces issues as a result of at ease key alternate. Without secret and secure key exchange, the symmetric key trade turns into unconfident. The large problems which might be confronted are foundation authentication and crew founded comfy alternate. There is not any assurance that during the time of exchanging secret key, the acquired key is just not falsely modified by a hacker and sent from the professional sender.

The asymmetric scheme is hundred times slower then symmetric ones, on account that it offers with tremendous keys and involves third get together which might be risky for communication between two countries as a result of spy attacks and political reasons. Issuing and renewing of certification requires time and will have to be cost mighty. When big information is involved, it is not feasible because of laziness of encrypting system that requires lot of Random access memory (RAM) and electric energy.

## Digital Signature:

With the aid of digital signature, origin authentication can be archived which is quintessential for protection however the required minimum key size is 1024 bit for digital signature which is the greatest hurdle in processing velocity .The hash services are quick in processing but hash operate do not provide origin authentication. Message authentication codes are fast and are based on symmetric key. For that reason it requires to share and agree on single key as a prerequisite for encryption.

Reliable signature scheme for authentication and integration shouldn't be offered by way of quantum cryptography where it neighbors the likelihood of denial of provider and man in core assault. Signature verification is gradual in elliptical curve cryptography than symmetric encryption.

### Steganography:

Steganography itself is only a process of hiding know-how nevertheless it cannot provide required protection objectives and concealing method with image results the gigantic measurement of message. The primary difficulty with steganography is the implementation of Statistical and Radiofrequency methods like size and Signature intelligence (MASINT) used to fully grasp the inter–bit delays for cracking the expertise.

### Excessive Efficiency:

Excessive efficiency is required for efficient answer in purposes comparable to tough disk and bus encryption requiring encryption in terabit networks. If cryptography seems to be very high-priced without feasibility, it's going to now not be deployed. Taking reference to Gilders legislation which predicts that speed and storage will broaden with a factor of 10,000 for LAN devices and Moore's law which predicts that the computing power for the identical rate will develop with a component of about a hundred, reflecting parallelism is significant in cryptographic operation and highlights the need for high efficiency design.

## JUSTIFICATION ON SOLVING THE PROBLEM:

By tackling the difficulty faced in cryptography, we are able to assure that the customers in each the tip can confidently trade knowledge and preclude any exploitation from 1/3 party. With the emphasis on refinement in the problems confronted in cryptography, an expand in information confidentiality, knowledge integrity, and authentication can also be accomplished. Consequently making it safer for the entities and individual who use the internet for transactions and conversation.

We will be able to be utilizing quite a lot of countermeasures so as to eliminate the maximum quantity of hazard. With probably the most original problems, we can be dealing with each of them in one other technique to curb the problems.

## EXPECTED RESULT:

With an in-depth understanding of cryptography, our workforce believes that the problems confronted may also be overcome with few corrective measures and strategically alterations to the overall body work accompanied with the attention measures from each users.

## REFERENCES:


Workman, Michael; Phelps, Daniel; Gathegi, John. *Information Security for Managers.* Jones & Bartlett Learning, LLC. 2013.

Darshanand, Khusial; McKegney, Ross. *E-Commerce Security: Attacks and Preventive Measures.* April 2005. http://www.ibm.com/developerworks/library/co-0504_mckegney/index.html

Giunipero, Troy. *The Netbeans E-Commerce Tutorial*. 2010. https://netbeans.org/kb/docs/javaee/ecommerce/intro.html "Securing the Application"