# Cryptography essay

Law, Security

# Introduction

Cryptography is a mathematical technique for encrypting and decrypting data. Cryptography enables one to store and transmit sensitive information across public insecure networks so that no one else can access the information apart from the authorized persons, i. e., the sender and the intended recipient (Martin, 2012). Cryptography uses a cryptographic algorithm. A cryptographic algorithm is a mathematical function used during the encryption and decryption process. The algorithm works together with a key to transform plaintext into encrypted text. The security of encrypted information depends on two things: the secrecy of the key used and the strength of the cryptographic algorithm employed (Stallings, 2013).

# Question 1

Various cryptographic techniques can be used to address security threats to information systems. These include classical encryption techniques, public-key encryption techniques, and digital signatures.

Classical encryption techniques involve the replacing of a plaintext by other letters, numbers or symbols. Processes responsible for such transformations include monoalphabetic ciphers, polyalphabetic ciphers, and Vigenere ciphers with the help of a secret word known as key. The process addresses the issue of interception, because even if the adversary accesses the information, it will be tough for them to comprehend the message.

The Public-Key encryption technique addresses the threat to privacy by making the message confidential. This method makes use of private and public keys of the communicating parties whereby the public key of the message recipient is used by the message sender to encrypt a message. The receiver uses a unique private key to decrypt the message. Since the private key is unique, only the intended recipient can decrypt the message, thus ensuring confidentiality.

Digital signatures are equivalent to handwritten the signatures, only that they are electronic. Digital signatures together with public key cryptosystems help address the threats of masquerading, modification and non-repudiation since the sender of the message can be authenticated (Kartalopoulos, 2009). Data integrity is maintained, and the sender or receiver cannot deny performing a transaction. In this process, the public-key cryptosystem is used in reverse. The sender computes a message digest using a hash function in order to sign the message. Next, the sender encrypts the message using own private key before sending it. The receiver first retrieves the message using the sender’s public key. At this point, the sender is authenticated since the private key used is unique, and only its related public key can decrypt the message. Once the message gets to the recipient, the recipient recomputes the message digest using a hash function and compares it with the sender’s message digest. If valid the message recipient concludes that the message has not undergone any modification. Also, non-repudiation is achieved since the sender cannot deny the message after signing it (Stallings, 2013)

## Question 2

Some of the threats that cannot be addressed by cryptographic techniques include hardware failure, software failure, and theft (Martin, 2012). Hardware failure may occur when one or more devices used in the information system fails to perform its function as expected. Installing an extra hardware makes the system more fault-tolerant.

Programs used in computer systems may contain bugs in which case cryptography cannot fix the bugs. Enhancement and constant program updates can help reduce the bugs.

Theft of physical assets or information involves an intruder accessing computer systems and stealing them. Physical security, for example, peripheral walls and use security guards will help eliminate such threats.

## Question 3

Mathematics plays a critical role in cryptographic techniques. In every encryption or decryption mathematical concepts for instance functions and algorithms are employed.

## In classical cipher methods, mathematical algorithms together with keys are used to transform intelligible messages to unintelligible messages.

In Public-Key Encryption technique, arithmetic algorithms are used in generating the private keys and the respective public keys used during encryption and decryption.

In Digital Signature, Mathematics knowledge is used in the transformation of a message to a message digest. In addition, the hash function comprises of mathematical functions.

## References

Kartalopoulos, S. V. (2009). Security of information and communication networks. Hoboken, N. J: Wiley.

Martin, K. M. (2012). Everyday cryptography: Fundamental principles and applications. Oxford: Oxford University Press.

Stallings, W. (2013). Cryptography and network security: Principles and practice. Upper Saddle River, N. J: Prentice Hall.