ADV MATH SCI JOURNAL
Advances in Mathematics: Scientific Journal **10** (2021), no.9, 3063–3092
ISSN: 1857-8365 (printed); 1857-8438 (electronic)
https://doi.org/10.37418/amsj.10.9.1

A MATHEMATICAL PROPOSED MODEL FOR PUBLIC KEY ENCRYPTION ALGORITHMS IN CYBERSECURITY

Heba Ahmad Saif[1], Gharib Musa Ibrahim Gharib, and Mohammad Rasmi AL-Mousa

ABSTRACT. Information security is a very important science, especially after the continuous increase in cybercrime of all kinds, which caused very large financial, economic and political losses, so it was necessary to find a solution to protect the data and keep it secret. Data encryption is one of the most important solutions to preserve data and reduce cybercrime. The encryption process means converting the plain text using a private key into symbols and numbers that make this text incomprehensible to others. There are many algorithms that are used for encryption, and the public key algorithms are the strongest in the encryption process because they depend on two keys, the public key and the private key. One of the most important problems facing this type of algorithm is the lack of a clear mathematical model that facilitates understanding and how to deal with these keys. In this thesis, a mathematical model has been proposed in which two functions are defined, the public key and the function of the private key, based on the concepts and specific characteristics of the function. A general mathematical model was constructed by defining two functions, one for the public key and the other for the private key, using the properties of a function in mathematics, to produce strong keys used in the public key algorithm, to protect data and keep it secret, and this model was applied to the RSA and ELGamal algorithms. The most important result was that in the case of applying the mathematical model, it is easy to understand and deal with the public key and the private key mathematically.

[1]*corresponding author*

2020 *Mathematics Subject Classification.* 94A60.

Key words and phrases. public key, encryption, algorithm, cybersecurity.

Submitted: 02.08.2021; *Accepted:* 18.08.2021; *Published:* 01.09.2021.

1. INTRODUCTION

Information security is a collection of activities aimed at keeping data safe from unauthorized access or alterations, either while stored and when transferred from one computer or physical location to another. Information security includes several methods and techniques developed and implemented to protect print, digital, or any form of highly classified, personal, confidential information or unauthorized access, utilize, misuse, disclosure, destruction, alteration or disruption. Considering that knowledge has become one of the most important assets of the 21st century.

Because information technology has become the accepted corporate buzz phrase which basically means "computers and related things." Sometimes there is a lack of understanding about information security and cybersecurity [1].

Cybersecurity is the general task of protecting information technology assets from threats, and cybersecurity is a particular activity under the umbrella of information security. Network protection and application security are associated information security activities [2].

The primary components of information security are often summarized by the CIA which are: confidentiality, integrity, and availability. In a perfect scenario, the data must always be kept confidential, in its correct state, and available [3].

Mathematics is one of the most important pillars on which data security is based, due to the use of precision mathematical equations are used to create complex algorithms that are used already to encrypt data and thus protect data confidentiality.

These equations are considered difficult and accurate as their primary task is to complicate any possible penetration of an electronic network. Public key infrastructure relies on the use of modern, scientifically proven digital coding and signature systems to protect information security, which have been developed using highly advanced mathematical algorithms and encryption functions that are difficult to decode or analyze [4].

The main objective of this thesis is to use mathematics to build a mathematical model of public key cryptographic algorithms in cybersecurity that aims to protect data confidentiality.

A mathematical model is a description of a structure that utilizes mathematical theorems and expression. It represents a structure by consists of a range of

variables and a set of equations that determine relationships among variables. Variables could be of many forms; real or integer numbers, Boolean values, or strings. The main aim of the mathematical model system is to study the effects of different components and make behavioral predictions [5].

Mathematical models allow scientists to represent complicated processes in the form of descriptive formulas. The data used in the models are usually linked to a particular number of variables chosen for the question at hand. There is currently no general model for all purposes. Mathematical models are used in the fields of sciences, engineering, computer science, and social sciences [6].

Mathematical models are usually made up of relationships and variables. Relationships can be defined by operators, like algebraic operators, functions, differential operators, etc. Variables are abstractions of system parameters of interest, which can be quantified.

Mathematical models aim to investigate behavior and the relationship between problem components as well as looking at all possibilities and evaluating alternatives and exclusion in order to make substantive decisions [7]. The Figure 1 shows how to simplify the representation of certain aspects of the real system.

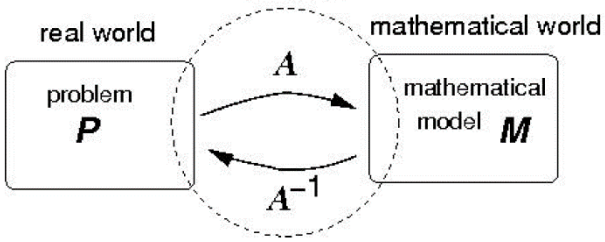

FIGURE 1. Mathematical models[8]

Recently, cybercrime has spread widely around the world, and has caused great material and political damage in addition to moral damage such as disclosure of data privacy and theft of information, etc [29-31].

Because of the increase in these crimes, it was necessary to find effective security methods to protect data from the risks and attacks that may befall them, and researchers began to pay attention to finding have to maintain the security of data and information. Encryption is beginning to gain special importance due to its ability to make stolen data useless for anyone who is not authorized

to access it. Encryption keys are necessary to decode data and give full control to the people who are authorized to access it, allowing companies and customers to maintain the privacy of their data. The public key algorithm is one of the most powerful algorithms used in encryption. Unfortunately, after looking at the encryption algorithms, this thesis found that there is no clear mathematical model that shows how to handle public encryption keys.

One solution proposed is to build a mathematical model to demonstrate the functioning of the public key in public key cryptographic algorithms.

The primary contribution of this thesis is building a general mathematical model by defining two functions: one for public key and the other for private key using function properties in mathematics, to produce strong keys used in the public key algorithm, to protect data and to keep it confidential.

2. BACKGROUND

In this section, much current research related to cybersecurity has been studied. It also includes the importance of encryption to keep data confidential through encryption algorithms. In addition, this section highlights several electronic crimes that the computer may be exposed to by cybercriminals, as these crimes penetrate the privacy of information and lead to the separation of user's connection to the network and the blocking of services that can be provided to users.

Cybercrimes are electronic activities that are committed with a criminal aim to cause material or moral harm to a person or entity, directly or indirectly. Cybercrime includes any criminal activity that takes place through computers or networks such as hacking and piracy, or via the Internet and mobile phones [9].

Definitely, cybercrime is a criminal act and is punishable by statute. Cybercriminals are inventing various techniques and applications to target computers and networks. As technology develops, internet users face greater risk and through cyber-attacks are continually discovering new methods of export [10]. Cybercrime can victimize people and computers in different ways, including:

- Unpleasant private messages with bad content.
- Virus infection
- Unauthorized access to e-mail, social network or any other account via the Internet

- Abusive or hostile private messages
- Spread rumors or misinformation on the Internet
- A victim of online fraud
- Files encoded with ransomware
- Misuse of a credit card
- Unauthorized access to the online bank account

Prislan et al. [10] presented an important statistical study, which showed that the percentage of females who were subjected to cybercrime is: 54.7% are females while 36.8% are males. Most participants with this statistic used the Internet to search for information (31.4%), followed by communicating with friends (27.1%), and working (19.4%).

Cybersecurity is the protection afforded to an information system in order to achieve the established goals of maintaining (the integrity, availability, and confidentiality) of the information system's resources. It is relates to protection from potential dangers through external sources, especially the Internet [11].

Cybersecurity professionals work to protect computers from any kind of attacks, breaches, and threats, in addition to ensuring that no unauthorized person is allowed to enter and access information, modify or copy it, where it is concentrated Cybersecurity protects the whole computer from external sources [12].

Cybersecurity concerns with the understanding of surrounding issues of diverse cyber-attacks and devising defense strategies that preserve confidentiality integrity and availability of any digital and information technologies. There are several objectives that should be achieved to ensure the privacy of data, these objectives are [13]:

- Confidentiality: Ensures that the information in the computer is accessed only by authorized parties, not by anyone else.
- Integrity: Ensure that the information and programs are modified or deleted only by the authorized party in a specified and authorized manner.
- Authentication: The information received by every device must verify the sender's identity to decide if the information comes from an authorized party or is a fraudulent identity.

- Availability: Ensure that the authorized person is able to access information systems whenever needed and accessibility should not be prevented.
- Accountability: The security objective that creates the obligation for an individual's behavior to be linked to that individual in a specific manner.

Ensuring cybersecurity is a very complex task, it dependent on two factors: domain knowledge and requiring high cognitive capabilities to identify potential threats of network data. Ensuring cybersecurity need different measurements to deter, prevent, detect and correct the security violations affecting data transmission [14].

The threats countered by cyber-security are three-fold [15]:

- Cybercrime includes single entities or groups that aim to cause damage to the financial benefit processes.
- Cyber-attack often involves comparing understanding of politics.
- Cyberterrorism aims at blocking computer networks which lead to confusion or fear.

The importance of studying cybersecurity comes from an important perspective, which is that the more knowledge in cybersecurity enabled the correct detection of malicious events and reduced the incorrect classification as malicious of benign events. While knowledge of cybersecurity helps detect malicious events, in order to make accurate detection decisions, situated knowledge regarding a specific network at hand is required.

Cybersecurity is important as it includes anything related to the protection of confidential data, personal information, intellectual property, apps, and fraud and harm attempted by criminals and opponents of business and government information systems [16].

According to the enormous technological development of information systems, the information and communications technology field received huge amounts of data every day, stored on computers or transmitted through computers, the importance of ensuring this information was not exposed to hacking or modification became necessary, and information security became more important in the storage and transmission of data. Encryption is beginning to become particularly important because of its ability to make stolen information useless for anyone who is not allowed to access it [17].

The following figure shows how the encryption process takes place [18]:

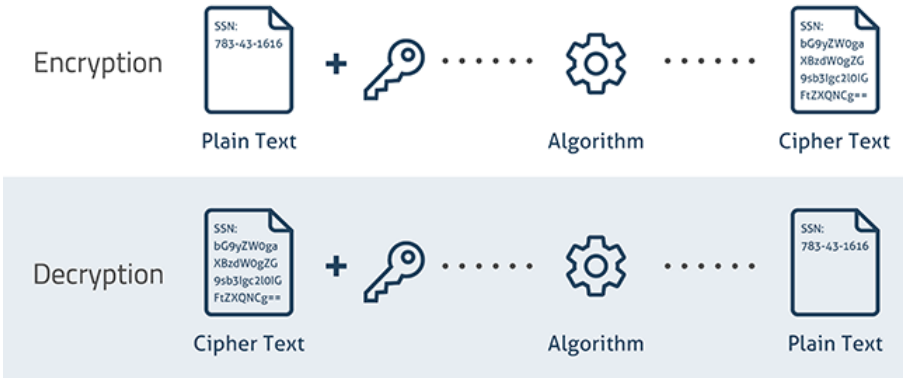

FIGURE 2. Encryption process

Encryption is a process to convert plain text to cipher text. The encryption process provides a way to secure information, by encoding a message and makes only the intended person who can read the message.

Cryptography utilizes the technique of encryption to send sensitive messages over an unreliable channel. This process requires two major things: a key and an encryption algorithm. An encryption algorithm indicates the technique used in the encryption process. Encryption occurs at the sender-side [13].

Decryption is the opposite encryption process. It is a process where cipher text is converted into plain text. Cryptography utilizes the receiver-side decryption algorithm to get the original message from the cipher text. The decryption process needs two things: a key and a decryption algorithm.

There are different terms that are used in cryptography:

- Plain text: The original message.
- Cipher text: The coded message.
- Keys: Used as input for encryption or decryption and determines the transformation.

Cryptography has a range of security objectives to ensure data confidentiality, data non-alteration etc. This is commonly practiced, because of the great security advantages of cryptography [13]. There are various cryptography goals which are:

- Confidentiality: Ensuring the data are transmitted on the device and must only be accessed by the permitted party and not by everyone else.
- Authentication: The data collected by any device will validate the sender's identity as to whether the information is coming from an authorized person or a fake persona.
- Integrity: Ensuring that information and programs are changed or removed only in a declared and permitted way by the authorizing party.
- Non Repudiation: Ensuring that the transmission will not be refused by either the sender or the recipient of the message.
- Access control: The data provided can only be accessed by the approved parties.

3. CATEGORIES OF CRYPTOGRAPHY

'Cryptographic systems are classified along three independent dimensions [19]:

- The type of operations used for transforming plaintext to ciphertext: Substitution, transposition.
- The way in which the plaintext is processed:Block ciphers, stream cipher.
- The numbervb of keys used: Symmetric key, asymmetric key.

3.1. **Type of operations.** There are two types of Operation used to transform plaintext into cipher text which are: Substitution cipher and transposition cipher. The first type is substitution cipher. It is a method of encryption where the plaintext letters are replaced by other letters either by numbers or symbols. The method of substitution cipher is very easy, and can be easily understood. There are several types of substitution of cipher such as: Caesar Cipher, Monoalphabetic Cipher, and Homophonic Cipher [19].

In Caesar cipher method, the cipher text can be produced by replacing each letter of the alphabet with the standing letter k at the bottom of the alphabet, the alphabetic wrapped in a manner that the next letter Z is A. In order to encrypt a text in English which consists of 26 letters, the following equation must be follow:

ciphertext : $E\ (k, p) = (p + k) \bmod (26)$

The decryption algorithm is:

plaintext: $E\ (k, c) = (c - k) \bmod (26)$

If the attacker knows that a specific ciphertext is a Caesar cipher, then it is simple to perform a brute force attack, simply try all the 25 possible keys. But if the plaintext language is unknown then plaintext production cannot be recognizable. In addition, the input plaintext may be compressed in some way, making it again difficult to recognize [20].

The second type is transposition cipher, which is a method of encryption in which the positions occupied by plaintext letters are changed by a regular system, as the ciphertext contains a plaintext permutation, which means: the plaintext is re-ordered [19].

Mathematically a "Bijective function" is being used to encrypt and an "Inverse function" to decrypt on the positions of the letters. This method is very simple and easy to understand. There are several types of transposition cipher such as: Rail Fence Cipher, Scytale, Route Cipher, Row Transposition Cipher and Columnar Transposition [21].

In Row Transposition Cipher, the message can encrypt by writing the content of this message in a rectangle, row by row, and read the message off, column by column, but permute the order of the columns [19]. The column order is' then the key to the algorithm; a pure transposition cipher is simple to recognize because it has the same letter frequencies as a plaintext message. To decrypt it, a receiver will work out the lengths of the column by dividing the length of the message by the length of the key. The following figure shows how to encrypt this message (attack postponed until two am).

```
Key:          4 3 1 2 5 6 7
Plaintext:    a t t a c k p
              o s t p o n e
              d u n t i l t
              w o a m x y z
Ciphertext:   TTNAAPTMTSUOAODWCOIXKNLYPETZ
```

FIGURE 3. Row Transposition Cipher[22]

A drawback of transposition is the high demand for memory and also ciphertext letters are still in the same proportion as English letters, as the letters are not modified by the cipher, so the ciphertext is vulnerable to brute force attack [22].

3.2. **The processing way.** There are two ways in which the plaintext is processed which: Block ciphers and stream cipher. The first way is a block cipher, which block of plaintext is handled as a whole and had to create an equal-length ciphertext block [19].

It is a function which maps n-bit plaintext blocks to n-bit ciphertext blocks; n is called the length of the blocks. It can be considered as a simple substitution cipher with a character large scale. The function is placed to a K-bit Key Try to take values of any k-bit vector set Vk from a subset K (the key space). It's generally assumed the key is picked. The use of equally sized plaintext and ciphertext blocks prevents data expansion.

Usually, a block size of 64 or 128 bits is used. Majority of network-based cryptographic symmetric applications use block ciphers [23].

The second way is a stream cipher is one that encrypts a digital data stream one bit or one byte at a time. For a stream cipher to be secured its keystream must have a wide period of time and the key or internal state of the cipher must not be retrieved from the keystream. Stream ciphers are mostly used in hardware for their speed and ease of implementation, especially in applications when plaintext comes in unknowable length quantities like a secure wireless link [24].

3.3. **The number of keys used.** A key is a text numbered or alphanumeric, or a symbol of a unique nature. It can be used on the plaintext at the time of encryption, and on the ciphertext at the time of decryption [25]. Selecting keys in encryption is very critical because it directly relies on the reliability of the encryption algorithm. The strength of the encryption algorithm is dependent on the key's secrecy, key length, initialization vector and how all of them work together [19].According to the number of keys used in the encryption process, there are different algorithms can be classified into symmetric key and asymmetric key, The first type is symmetric key cryptography. Symmetric key is a method of cryptosystem where the same key is used for encryption and decryption [26]. The key represents a joint secret between two parties which can be used to establish a private link to information, Symmetric key follows the self-certification method, which means that the key is self-certified, and no additional method is required for key authentication [27].

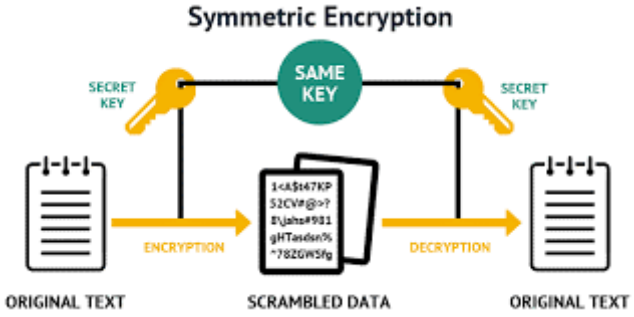

FIGURE 4. Symmetric key[28]

Symmetric key is necessary as it provides faster and easier service without the use of several resources; but there are a several problems with symmetric algorithms [32]:

- The shared secret key is exchanged over unsecured Internet, if a third party accesses a secret key, cipher text messages can be easily decrypted, to solve this problem the key most changed frequently or keep it as safe as possible.
- Difficulty determining whether the data has already been changed or sent by the intended sender, If the hacker has a secret key, the original text will be hacked and changed, to solve this problem, different methods must be used to ensure data integrity and non-repudiation such as digital signatures and Hashing functions.
- The possibility of using symmetric encryption cracking tools, such as using a brute force attack, trying all possible keys, and discovering the properties of the algorithm used for encryption, then knowing the plain text or secret key.

Several algorithms to explain symmetric key cryptography have been developed, such as AES, DES, 3DES, Blowfish [33].

The second type is asymmetric encryption. Asymmetric key is a cryptosystem method which uses two keys; public key is used for encryption by the sender and private key used for decryption by the receiver. And it is also known as public key cryptography. In asymmetric key, the self-certification is absent but digital signatures are used to certify the keys. This approach is more efficient and authenticates better, as privacy remains strong [34].

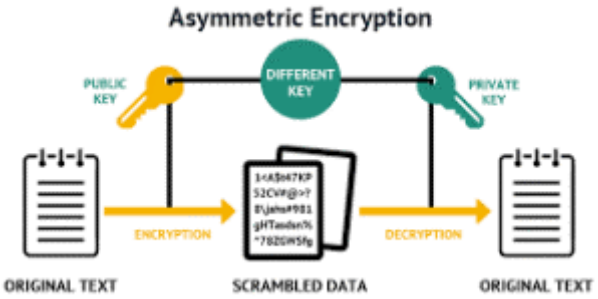

FIGURE 5. Asymmetric encryption[18]

Several algorithms to implement asymmetric key cryptography have been developed, such as Diffie_Hellman and Digital Signature Algorithm [26].

4. PUBLIC KEY ENCRYPTION

Public-key cryptography, or asymmetric cryptography, is an encryption method which uses two, but not similar, mathematically related keys which are: a public key and a private key. Unlike symmetric key algorithms that rely on both encryption and decryption of one key, each key performs a specific function. The public key is used for encryption, and the private key is used for to decryption. The following figure described the public-key cryptography [35].

The primary applications for public key cryptography are:

- Digital signatures: The document is digitally signed with a private key of the person and checked by the public key of the person
- Encrypting: Information is encrypted with the public key of an user and can only be encrypted with the private key of that user.

Calculating the private key, based on the public key, is computationally impractical. Due of this, public keys can be publicly available, allowing users to quickly and efficiently encrypt content and validate digital signatures, and private keys can be kept private, ensuring that information can be decrypted and digital signatures generated by private key owners only [35].

Because public keys have to be shared but are too large to remember effectively, they are kept on digital certificates for secure transportation and distribution. Because private keys are not exchanged, they are easily stored in the software or operating system that are using, or on hardware (e.g. USB token,

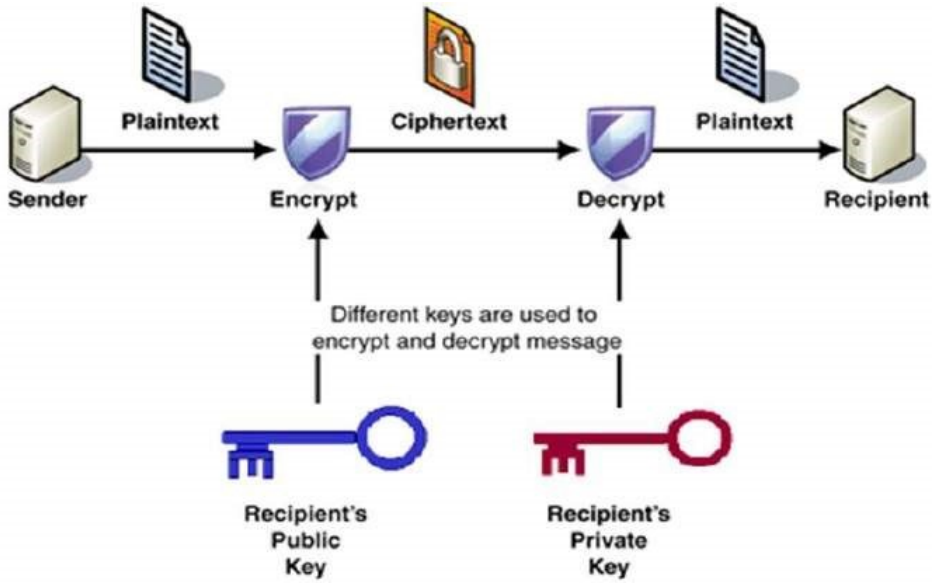

FIGURE 6. Public Key Cryptography

hardware protection module) including drivers that allow the software or operating system to be used with it.

There are several public key algorithms that used such as Rivest-Shamir-Adleman, Digital Signature Algorithm, Diffie-Hellman Key Exchangeand, and the ElGamal Public Key Encryption, each of these algorithms will describe briefly in the following sections.

4.1. **Rivest-shamir-adleman (RSA).** RSA is a public-key cryptographic algorithm for key exchange, digital signatures, or data encryption, developed by Ron Rivest, Adi Shamir, and Leonard Adleman in 1978 [36]. RSA uses a block for encryption of the variable size and a key for variable size. It is a number theory-based asymmetric cryptosystem which is a block cipher system. In RSA, two prime numbers are used to obtain public and private keys based on mathematical formulae, these keys are used for processes of encryption and decryption.

When the sender encrypts the message using the receiver public key and the receiver can decrypt it using his own private key, whether the data has been encrypted with the public key, only the corresponding private key can decrypt the cipher data [35].

RSA can be described in three broad steps; key generation, encryption, and decryption. When selecting the small values of $p\&q$ to construct the key then the encryption method is too weak and the data can decrypted using random probability theory and side channel attacks. If large $p\&q$ lengths are selected then more time is spent and the efficiency is reduced compared to DES. In addition, for $p\&q$, RSA often needs similar lengths; technically these are very difficult requirements to satisfy [37]. For encryption in the RSA algorithm, the following steps should be followed [35].

The first step in encrypting an RSA message is to generate the keys. To do this, two prime $(p\&q)$numbers (and) would be required, which are chosen for the primary test. The Primality Test is an algorithm that systematically identifies prime numbers, like the (Rabin-Miller primality test).The prime e *and n* numbers in the RSA must be very large, but also relatively far apart. The numbers that are small or near together are a lot easier to crack key [38].

Within RSA, the cryptographic keys are made up of the prime number e and n. The number e may be anything between 1 and $\phi(n)$ the value for. As the public key is exchanged publicly, it's not that necessary for e to be a random number. In practice, is e usually set at 65,537, since when even greater numbers are selected randomly, encryption becomes much less effective. The last encrypted value is called ciphertext (c) key [38]. This emerges from the plain text message $(m)$by adding the following rule to the public key: $c = m^e \pmod n$.

In RSA encryption, only private keys from the same key pair may be decrypted after the data or message has been encrypted to ciphertext using a public key. Private keys are mainly composed of d and n . the value of know n, and the following equation must be used to find d: $de \equiv 1 \pmod{\phi(n)}$.

To decrypt the message and restore the original message the following equation is used: $m = c^d \pmod n$.

There are several advantages when using RSA, which is: RSA is a safe and efficient algorithm for its users because it uses complex mathematics. It is also difficult to crack the RSA algorithm, since it involves factorizing prime numbers that are difficult to factories. In addition, the RSA algorithm uses the public key to encrypt data, and everybody knows the key so it's easier to share the public key [38].

The drawbacks include; The RSA algorithm can be quite slow in situations when large data is to be encrypted by the same system. To check the security of

public keys it needs a third party. Through the RSA algorithm, data transmitted could be manipulated by middlemen who could temper with the public key process [39].

4.2. **The elgamal public key encryption algorithm.** ElGamal [40] is a public key cryptography algorithm developed by Tather ElGamal used for digital signature, but later it is modified to be used for encryption and decryption, and it is considered an alternative to the RSA for public-key encryption [41].

Since ElGamal is a public key, it needs use of a different key into a private and a public part. One key aspect of this method is that private part information makes decryption simple. If the private key is unknown, then decrypting the message in an appropriate time is virtually impossible [40, 41].

ElGamal encryption includes three components: The key generator, the encryption algorithm and the decryption algorithm. In each component there are different processes, it will describe in details in this section [41].

At least one key for symmetric algorithms and two keys for asymmetric algorithms is a basic requirement for a cryptographic process, in ElGamal just the receiver should build and distribute a key in advance [41]. The "receiver" should follow the steps to create its key pair:

- Prime and group generation: Firstly, the receiver must generate a large p prime and the generator g of a multiplicative group $\mathbb{Z}_p^*$ of the integers modulo p.
- Private Key selection: Receiver randomly selects the integer b of group $\mathbb{Z}$ and with the constraint $1 \leq b \leq p - 2$. It will be the private exponent.
- Public key assembling: The public key part $g^b \bmod p$ can be computed from this. In the ElGamal cryptosystem, the receiver's public key is the triplet $(p; g; ; g^p)$and his private key is b.
- Public key publishing: The public key has to be distributed using some special key server or other way, therefore the sender can get hold of it.

To encrypt a message M to the receiver, the sender should first extract its public key triplet $(p, g; g^p)$from a key server or receive from it through unencrypted e-mail, this transmission does not involve a security problem, since the only secret part b , is sent in g^b. Since the basic principle of the ElGamal cryptosystem is that generating the discrete logarithm is unfeasible, this is secure [41]. To encrypt the plaintext message *M* , the "sender" should follow these steps:

- Obtain the public key: The sender must obtain the receiver's public key part $(p; g; g^p)$ from a trusted and official key server.
- Prepare the message M for encoding: Write *M* as an integer set $(m_{1,}$ $m_2, \ldots)$ in the $(1, \ldots, p-1)$ range. All integers are encoded one by one time.
- Select random exponent k In this stage, the sender must select a random exponent which takes the place of the private exponent of the second partyin the Diffie_Hellman key exchange. The randomness is a key factor because the probability of guessing the k gives the attacker a sensible amount of information needed to decrypt the message.
- Compute public key: To send the random exponent k to the receiver, the sender must calculate $g^k \pmod p$and link it with the ciphertext to be sent to the receiver.
- Encrypt the plaintext: The sender encrypts the message M into ciphertext C in this phase. The sender iterates through the set generated during the preparing message for encoding, and measures for each of the c_i: $m_i * \left(g^k\right)^b \pmod p$. The cipher text C is the set of all c_i with $0 < i \leq |M|$.

5. A MATHEMATICAL MODEL

This section provides a detailed explanation of the mathematical model framework, which was created by using two functions to define the public key and the other function of private key. And presented a simple introduction to the number theory and definitions used in the mathematical model. In addition, a new functionality has been explained by using an example RSA and ELGamal algorithms case study, to demonstrate how to use the public key cipher algorithem using the proposed mathematical function.

5.1. **Number theory.**

The number theory is the study of the set of positive integers, which is often called the set of natural numbers, and the relationships between these numbers. During the past years, scientists have separated natural numbers into a variety of different types such as: Fibonacci, odd, square, cube, prime, triangular etc. The main goal of number theory is to discover interesting and unexpected relationships between different sorts of numbers and to prove that these relationships are true [42].

5.2. **The division algorithm.** The Division Algorithm, it asserts that an integer a can be "divided" by a positive integer b in such a way that the remainder is smaller than is b . The exact statement of this fact is Theorem 5.1.

Theorem 5.1. *Given integers a and b, with* n < 0*, there exist unique integers q and r satisfying* $a = qb + r \quad 0 \leq r < b,$

The integers q and r are called, respectively, the quotient and remainder in the division of a by [43], for example $a = 21 \;\; b = 2$, then $21 = 2 \times 10 + 1$.

5.3. **The greatest common divisor.** Of special significance is the case in which the remainder in the Division Algorithm turns out to be zero.

Definition 5.1. *An integer b is said to be divisible by an integer $a \neq 0$, in symbols $a \mid b$, if there exists some integer c such that $b = ac$. We write $a \not| b$ to indicate that b is not divisible by a.*

Thus, for example, -12 is divisible by 4, because $-12 = 4(-3)$. However, 10 is not divisible by 3; for there is no integer c that makes the statement $10 = 3c$ true(Burton, 2006).

5.4. **The euclidean algorithm.** The Euclidean Algorithm may be described as follows: Let a and b be two integers whose greatest common divisor is desired. Because $\gcd(|a|, |b|) = \gcd(a, b)$, there is no harm in assuming that $a \geq b > 0$. The first step is to apply the Division Algorithm to a and b to get: $a = q_1 b + r_1$, $0 \leq r_1 < b$.

If it happens that $r_1 = 0$, then $b \mid a$ and $\gcd(a, b) = b$. When $r_1 \neq 0$, divide b by r_1 to produce integers q_2 and r_2 satisfying: $b = q_2 r_1 + r_2$, $0 \leq r_2 < r_1$.

If $r_2 = 0$, then we stop; otherwise, proceed as before to obtain: $r_1 = q_3 r_2 + r_3$, $0 \leq r_3 < r_2$.

This division process continues until some zero remainder appears, say, at the $(n + 1)$ stage where r_{n-1} is divided by r_n (a zero remainder occurs sooner or later because the decreasing sequence $b > r_1 > r_2 > \ldots \geq 0$ cannot contain more than b integers).

The result is the following system of equations:

$a = q_1 b + r_1 \qquad 0 < r_1 < b$

$b = q_2 r_1 + r_2 \qquad 0 < r_2 < r_1$

$r_1 = q_3 r_2 + r_3 \qquad 0 < r_3 < r_2$

$$\vdots$$

$$r_{n-2} = q_n r_{n-1} + r_n \quad 0 < r_n < r_{n-1}$$

$$r_{n-1} = q_{n-1} r_n + 0$$

We argue that r_n, the last nonzero remainder that appears in this manner, is equal to $\gcd(a, b)$ [43].

Example 1. *Let us see how the Euclidean Algorithm works in a concrete case by calculating, say* $\gcd(12378, 3054)$. *The appropriate applications of the Division Algorithm produce the equations:*

$12378 = 4.3054 + 162$
$3054 = 18.162 + 138$
$162 = 1.138 + 24$
$138 = 5.24 + 18$
$24 = 1.18 + 6$
$18 = 3.6 + 0$

Our previous discussion tells us that the last nonzero remainder appearing in these equations, namely, the integer 6, is the greatest common divisor of 12378 and 3054:

$6 = \gcd(12378, 3054)$

To represent 6 as a linear combination of the integers 12378 and 3054, we start with the next-to-last of the displayed equations and successively eliminate the remainders 18, 24, 138, and 162:

$$\begin{aligned} 6 &= 24 - 18 \\ &= 24 - (138 - 5.24) \\ &= 6.24 - 138 \\ &= 6(162 - 138) - 138 \\ &= 6.162 - 7.138 \\ &= 6.162 - 7(3054 - 18.162) \\ &= 132.162 - 7.3054 \\ &= 132(12378 - 4.3054) - 7.3054 \\ &= 132.12378 + (-535)3054 \end{aligned}$$

Thus, we have $6 = \gcd(12378, 3054) = 12378x + 3054y$, *where* $x = 132$ *and* $y = -535$*[43].*

5.5. **Congruence's.** Gauss introduces the concept of congruence (he explain that he was induced to adopt the symbol $\equiv$ because of the close analogy with algebraic equality). According to Gauss, "If a number n measures the difference between two numbers a and b, then a and b are said to be congruent with respect n to ; if not, incongruent." Putting this into the form of a definition, we have Definition 5.2 [43].

Definition 5.2. *Let n be a fixed positive integer. Two integers a and b are said to be congruent modulo n, symbolized by: $a \equiv b(\mathrm{mod}\, n)$, if n divides the difference $a - b$; that is, provided that $a - b = kn$ for some integer k.*

To fix the idea, consider $n = 7$. It is routine to check that: $3 \equiv 24(\mathrm{mod}\, 7) - 31 \equiv 11(\mathrm{mod}\, 7) - 15 \equiv 45(\mathrm{mod}\, 7)$, because $3 - 24 = -(3)7, -31 - 11 - (-6)7$,and $-15 - (-64) = (7)7$. When $n \not| a - b$, we say that a is incongruent to modulo n, and in this case we write $a \not\equiv b(\mathrm{mod}\, n)$. For a simple example: $25 \not\equiv 12(\mathrm{mod}\, 7)$ because 7 fails to divide $25 - 12 = 13$ [43].

Theorem 5.2. *Let $n > 1$ be fixed and a, b, c, d be arbitrary integers. Then the following properties hold:*

(a) $a \equiv a(\mathrm{mod}\, n)$.

(b) If $a \equiv b(\mathrm{mod}\, n)$, *then* $b \equiv a(\mathrm{mod}\, n)$.

(c) If $a \equiv b(\mathrm{mod}\, n)$ *and* $b \equiv c(\mathrm{mod}\, n)$, *then* $a \equiv c(\mathrm{mod}\, n)$.

(d) If $a \equiv b(\mathrm{mod}\, n)$ *and* $c \equiv d(\mathrm{mod}\, n)$, *then* $a + c \equiv b + d(\mathrm{mod}\, n)$ *and* $a\, c \equiv bd(\mathrm{mod}\, n)$.

(e) If $a \equiv b(\mathrm{mod}\, n)$, *then* $a + c \equiv b + c(\mathrm{mod}\, n))$ *and* $a\, c \equiv bc(\mathrm{mod}\, n)$.

(f) If $a \equiv b(\mathrm{mod}\, n)$, *then* $a^k \equiv b^k(\mathrm{mod}\, n)$ *and* $a\, c \equiv bd(\mathrm{mod}\, n)$, *then for any positive integer k (Burton, 2006).*

5.6. **Fermat's theorem.** Let p be a prime and suppose that $p \not| a$. Then $a^{p-1} \equiv 1(\mathrm{mod}\, n)$.

Example 2. $2^{16} \bmod 17$ *by Fermat theorem* $2^{17-1} \equiv 1(\bmod 17)$.

5.7. **Euler's phi-function.** Euler extended Fermat's theorem, which concerns congruence's with prime modulo, to arbitrary modulo. While doing so, he introduced an important number-theoretic function, described in Definition 5.3.

Definition 5.3. *For $n \geq 1$, let $\phi(n)$ denote the number of positive integers not exceeding n that are relatively prime to n.*

As an illustration of the definition, we find that $\phi(30) = 8$; for, among the positive integers that do not exceed 30, there are eight that are relatively prime to 30; specifically $1, 7, 11, 13, 17, 19, 23, 29$

Similarly, for the first few positive integers, the reader may check that:

$$\phi(1) = 1, \phi(2) = 1, \phi(3) = 2, \phi(4) = 2, \phi(5) = 4, \phi(6) = 2, \phi(7) = 6, \ldots.$$

Notice that $\phi(1) = 1$, because $\gcd(1,1) = 1$. In the event $n > 1$, then $\gcd(n,n) = n \neq 1$ so that $\phi(n)$ can be characterized as the number of integers less than n and relatively prime to it. The function ϕ is usually called the Euler phi-function (sometimes, the indicator or totient) after its originator; the functional notation $\phi(n)$, however, is credited to Gauss.

If n is a prime number, then every integer less than n is relatively prime to it; whence,$\phi(n) = n - 1$. On the other hand, if $n > 1$ is composite, then n has a divisor d such that $1 < d < n$. It follows that there are at least two integers among $1, 2, 3, \ldots, n$ that are not relatively prime to n, namely, d and n itself. As a result,$\phi(n) \leq n - 2$. This proves that for $n > 1$, [43], $\phi(n) = n - 1$ if n and only if is prime.

5.8. **Euler's theorem.** The first published proof of Fermat's theorem (namely that $a^{p-1} \equiv 1(\mathrm{mod}\, n)$ if $p \not| a$ was given by Euler in 1736. Somewhat later, in 1760, he succeeded in generalizing Fermat's theorem from the case of a prime p to an arbitrary positive integer n. This landmark result states: If $\gcd(n,n) = 1$, then $a^{\phi(n)} \equiv 1(\mathrm{mod}\, n)$[43].

Theorem 5.3. *If* $n \geq 1$ *and* $\gcd(a,n) = 1$*,then* $a^{\phi(n)} \equiv 1(\mathrm{mod}\, n)$.

For example, putting $n \equiv 30$ and $a = 11$, we have $11^{\phi(30)} \equiv 11^8 \equiv (11^2)^4 \equiv (121)^4 \equiv 1^4 \equiv 1(\mathrm{mod}\, 30)$.

5.9. **Miller-Rabin test for primality.** Primality testing is based on Fermat theorem, this algorithm can be summarized as follows:

- Pick an odd integer $q \geq 3$, then the number $(q-1)$ will be even integer. The even integer $(q-1)$ can be expressed in the form of some power of 2 times an odd number i.e.; $(q-1) = 2^2.s$, where $n > 0$, s is odd.

  Simply, we can say that divide $(q-1)$ by 2 until the results is an odd number.

- Choose at random an integer m i.e $1 < m < q-1$ and compute

  $$m^s \bmod q, m^{2s} \bmod q, \ldots, m^{2(n-1)s} \bmod q, m^{2^n.s} \bmod q \ldots .(1).$$

  By Fermat theorem we know that if q is prime, $m^{q-1} \equiv 1 (\bmod q)$.

  So, if q is prime, then $m^{2^n.s} \bmod q = 1$. This may or not be an earlier element of the sequence (1) that has residue equal to 1.
- Next, if $m^s (\bmod q)$ is equal to ± 1, then q passes the primality test for the integer m.

  Otherwise $m^s (\bmod q) = k \neq \pm 1$, at most $(n-1)$ times replace k by square modulo n, and check if it is ± 1. If it is 1, q is not a prime. If result is -1, then q passes the primality test.

The mathematics of primality testing of an odd random integer q, by Miller – Rabin test is summarized as below:

Step 1: put $(q-1) = 2^n.s$

Step 2: Select a random integer i.e. $1 < m < q-1$.

Step 3: Compute $m^s (\bmod q)$.Either,$m^s (\bmod q) = \pm 1$, (then q may be prime inconclusive), or $m^s (\bmod q) = k \neq \pm 1$, (then go to next step 4).

Step 4 : Compute $k^{2i} (\bmod q), i = 1$ to $n-1$, Either $k^{2i} (\bmod q) = -1$, (then q is prime), or $k^{2i} (\bmod q) = k_1 \neq -1$, (then q is not prime (conclusive) and q is composite integer definitely).

Example 3. *Apply the Miller Rabin test to* $q = 53$.

Solution.

Step1: Here $(q-1) = 2^n.s \rightarrow (53-1) = 2^n.s \rightarrow 52 = 2^2.13; n = 2; s = 13$.

Step 2: Select a random number $m = 2$.

Step 3: Compute $2^{13} (\bmod 53) = 30$.

Step 4: $30^2 (\bmod 53) = (2^{13})^2 (\bmod 53) = 52 (\bmod 53) = -1$*, 53 is prime.*

Example 4. *Apply the Miller Rabin test to* $q = 561$.

Solution.

Step 1 : $(q-1) = 2^n.s \longrightarrow (561-1) = 2^n.s \longrightarrow 560 = 2^4.35; n = 4; s = 35$.

Step 2 : Select a random number $m = 2$.

Step 3 : Compute $2^{35} \bmod 651 = 263$.

Step 4 : $(263)^2 \bmod 561 = (2^{35})^2 \bmod 561 = 166 \longrightarrow$
$(166)^2 \bmod 561 = (2^{35})^4 \bmod 561 = 67 \longrightarrow$
$(67)^2 \bmod 561 = (2^{35})^8 \bmod 561 = 1$*, 561 is composite.*

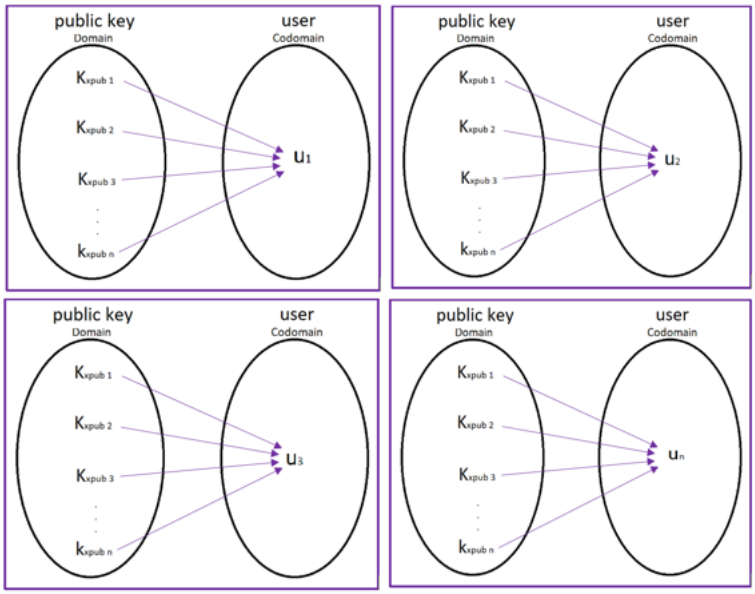

FIGURE 7. The way the public key function process.

5.10. **Public and private key.** The strength of the encryption algorithm depends on the length of the key, and this thesis specializes in the public key that includes two keys; in this section a public key and a private key will be presented and explained in detail.

The public key function can be describe as the following:

- The map of public key $F : Pub \longrightarrow U$, such that $F(K_{Xpub}) = u_n$, for all $n \in \mathbb{Z}$, and the elements $(K_{XpuB1}, K_{Xpub2,}K_{Xpub3,\ldots,}K_{Xpubn})$ are the domain in pub set (the public key) and the element $(u_1, u_{2,}u_3, \ldots, u_n)$ are the codomain in U set (the user).
- In the public key function, all elements in pub set (the public key) is related with the elements in U set (the user).
- The public key is written in the form of an ordered pair $\{K_{xpub}, u_n\}$.

The work of the public key can be described that any declared key will be in the possession of any user, and when the sender wants to send a message to the recipient he converts it to a digital message first, then the sender encrypts the message using the recipient's public key and then sends it over the Internet, and now once the encrypted message reaches the recipient, the recipient must

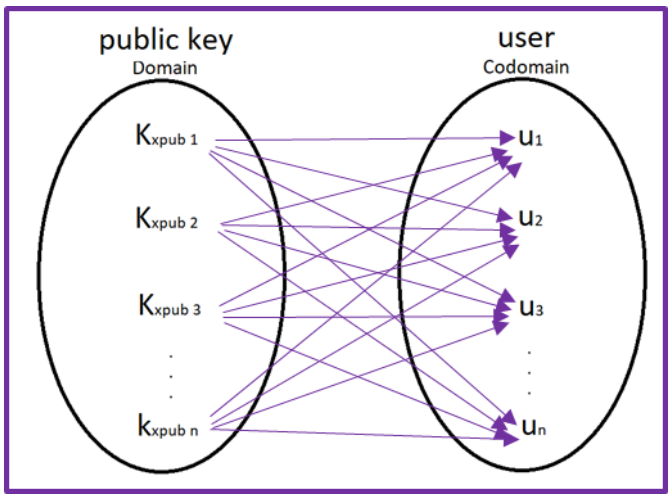

FIGURE 8. Public key works

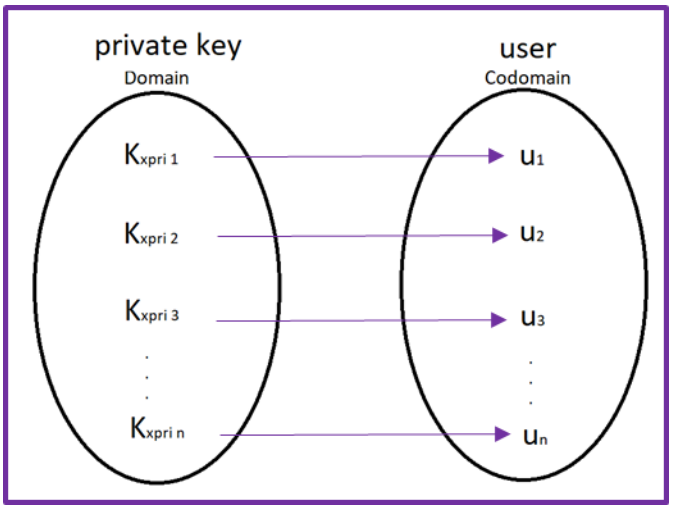

FIGURE 9. The way the private key function process

decrypt the message, although the message is encrypted the key using the public, but can only be decrypted by the recipient's private key and this makes the system safer.

The private key function can be describe as the following:

- The map of private key $F : pri \longrightarrow U$, such that $F(K_{xprin})$, for all $n \in \mathbb{Z}$, and the element $(K_{xpri1,}K_{xpri2,}K_{xpri3,}\ldots K_{xprin})$ are the domain in pri

set (the private key) and the element $(u_1, u_{2,}u_3, \ldots, u_n)$ are the codomain in U set (the user).

- In the private key function, each element in pri is related to only one element in U this means every user has a secret private key that no one knows.
- The privet key is written in the form of an ordered $\{K_{xprin}, u_n\}$.

5.11. **Application of mathematical modeling.** In this section, we will apply RSA and ElGamal algorithms as a mathematical case study to prove the research concepts which are the function of public key and the function private key.

First of all we apply RSA algorithm as a mathematical case study. The steps of the RSA algorithm are as follows:

Generating The Public Key:

Step 1: Choose two different prime random numbers, for example $q = 5$ and $p = 11$.

Step 2: Compute $n = p \times q = 11 \times 5 = 55$.

Step 3: Compute $\phi(n) = (p-1)(q-1) = (11-1)(5-1) = 10 \times 4 = 40$

Step4: Choose a random integer e number provided $1 < e \leq \phi(n)$, where $\gcd(\phi(n), e) = 1$, used like exponent for the public key.

For example pick $e = 7$, $1 < 7 \leq 40$, and $\gcd(40, 7) = 1$.

Generate A Private Key:

Step 5: Compute the d value by $de \equiv 1 \pmod{\phi(n)} \longrightarrow d(7) \equiv 1 (\mathrm{mod}\, 40)$, we will use an Euclidean Algorithm to solve this.

$40 = 5(7) + 5$

$7 = 1(5) + 2$

$5 = 2(2) + 1$

we then use the Extended Euclidean Algorithm.

$1 = 5 - 2(2)$

$1 = 5 - 2(7) - 1(5)$

$1 = 3(5) - 2(7)$

$1 = 3(40 - 5(7)) - 2(7)$

$1 = 3(40 - 15(7)) - 2(7)$

$1 = 3(40) - 17(7)$, but this is negative, we calculate $d = -17 (\mathrm{mod}\, 40) = 23 \bmod 40 \longrightarrow d = 23$, d used like exponent for the private key.

Define public key :$\{e, n\} = K_{xpubn} \longrightarrow \{((e, n), User)\} \rightharpoonup \{((7, 55), User)\}$

Define private key: $\{d, n\} = K_{xprin} \longrightarrow \{((d, n), User)\} \rightharpoonup \{((23, 55), User)\}$.

Encrypting The Message:

Suppose that the sender wants to send a "MATH" word to receiver after converting it to a digital message, he simply looks up her public key and use the equation to encrypt each plaintext letter: $c = m^e (\mathrm{mod}\, n)$

Step 6: Encrypting a "MATH" word.

Encrypting M: let $m = 8$, $c = m^e (\mathrm{mod}\, n) = 8^7 (\mathrm{mod}\, 55) = 2 (\mathrm{mod}\, 55) \longrightarrow c = 2$

Encrypting A:let $m = 7$, $c = m^e (\mathrm{mod}\, n) = 7^7 (\mathrm{mod}\, 55) = 28 (\mathrm{mod}\, 55) \longrightarrow c = 28$

Encrypting T:let $m = 3$, $c = m^e (\mathrm{mod}\, n) = 3^7 (\mathrm{mod}\, 55) = 42 (\mathrm{mod}\, 55) \longrightarrow c = 42$

Encrypting H:let $m = 4$, $c = m^e (\mathrm{mod}\, n) = 4^7 (\mathrm{mod}\, 55) = 49 (\mathrm{mod}\, 55) \longrightarrow c = 49$

Ciphertext : 2, 28, 42, 49.

Decrypting The Message:

Step 7: The recipient decrypts the message with its private key using the equation:

$m = c^d (\mathrm{mod}\, n)$

Decrypting 2: $m = c^d (\mathrm{mod}\, n) = 2^{23} (\mathrm{mod}\, 55) = 8 (\mathrm{mod}\, 55) \longrightarrow M = 8$

Decrypting 28: $m = c^d (\mathrm{mod}\, n) = 28^{23} (\mathrm{mod}\, 55) = 7 (\mathrm{mod}\, 55) \longrightarrow A = 7$

Decrypting 42: $m = c^d (\mathrm{mod}\, n) = 42^{23} (\mathrm{mod}\, 55) = 3 (\mathrm{mod}\, 55) \longrightarrow T = 3$

Decrypting 49: $m = c^d (\mathrm{mod}\, n) = 49^{23} (\mathrm{mod}\, 55) = 4 (\mathrm{mod}\, 55) \longrightarrow H = 4$

now we have a plaintext message " MATH ".

Now we apply ElGamal algorithm as a mathematical case study. The steps of the ELGamal algorithm are as follows:

The Key Generator:

Step1: Prime and group generation: Firstly, the receiver must generate prime P, pick $P = 29$ and the generator $g = 8$.

Step2: Private Key selection: Receiver randomly selects the integer $b = 9$.

Step 3: Public key assembling: The public key part. $m = g^b (\mathrm{mod}\, n) = 8^9 (\mathrm{mod}\, 29) = 15$

Define the public key is : $K_{xpubn} \longrightarrow \{(p, g; g^b), User\} = \{(29, 8; 15), User\}$.

Define private key is: $K_{xprin} \longrightarrow \{(g), User\} = \{9, User\}$.

The Encryption Algorithm:

Step 4: Select random exponent: the sender must select a random exponent $k = 3$.

Step 5: Compute public key: calculate $g^k (\mathrm{mod}\, p) = 8^3 (\mathrm{mod}\, 29) = 19$.

Step 6: Encrypt the plaintext:, to send the message " MATH ", this is the equation to encrypt plaintext letter: $c = m * (g^k)^b (\mathrm{mod}\, p)$

Encrypting M: let $m = 13$, $c = m * (g^k)^b (\mathrm{mod}\, p) = 13 * (8^2)^9 (\mathrm{mod}\, 29) = 13 * (19)^9 (\mathrm{mod}\, 29) \longrightarrow c = 27$

Encrypting A: let $m = 14$, $c = m * (g^k)^b (\mathrm{mod}\, p) = 14 * (8^2)^9 (\mathrm{mod}\, 29) = 14 * (19)^9 (\mathrm{mod}\, 29) \longrightarrow c = 9$

Encrypting T: let $m = 22$, $c = m * (g^k)^b (\mathrm{mod}\, p) = 22 * (8^2)^9 (\mathrm{mod}\, 29) = 22 * (19)^9 (\mathrm{mod}\, 29) \longrightarrow c = 10$.

Encrypting A: let $m = 3, c = m * (g^k)^b (\mathrm{mod}\, p) = 3 * (8^2)^9 (\mathrm{mod}\, 29) = 3 * (19)^9 (\mathrm{mod}\, 29) \longrightarrow c = 4$.

Ciphertext: 27,9,10,4.

The Decryption Algorithm:

Step 7: calculates the plaintext through equation:

$m = c * (g^k)^{-b} (\mathrm{mod}\, p)$

Decrypting 27: $m = c * (g^k)^{-b} (\mathrm{mod}\, p) = 27 * (8^3)^{-9} (\mathrm{mod}\, 29) = 27 * (19)^{-9} (\mathrm{mod}\, 29) \longrightarrow M = 13$.

Decrypting 9: $m = c * (g^k)^{-b} (\mathrm{mod}\, p) = 9 * (8^3)^{-9} (\mathrm{mod}\, 29) = 9 * (19)^{-9} (\mathrm{mod}\, 29) \longrightarrow A = 14$.

Decrypting 10: $m = c * (g^k)^{-b} (\mathrm{mod}\, p) = 10 * (8^3)^{-9} (\mathrm{mod}\, 29) = 10 * (19)^{-9} (\mathrm{mod}\, 29) \longrightarrow T = 22$.

Decrypting 4: $m = c * (g^k)^{-b} (\mathrm{mod}\, p) = 4 * (8^3)^{-9} (\mathrm{mod}\, 29) = 4 * (19)^{-9} (\mathrm{mod}\, 29) \longrightarrow H = 3$.

Now we have a plaintext message " MATH ".

6. Conclusions and future work

In this paper, a general mathematical model was created, through this mathematical model two things are defined: the public key and the function of the private key, based on the concepts and distinct characteristics of the function using the properties of a function in mathematics. To verify the effectiveness of the mathematical model, this model was applied to the RSA and ELGamal algorithms. The results showed that applying the mathematical model facilitates

understanding and dealing with the public key and the private key mathematically, thus data confidentiality can be preserved.

However, suggestions that should be completed for further research. As applied our mathematical model in several public-key encryption algorithms. Also, trying to develop an algorithm consisting of two functions, the input in the first function gives an output, and the output in the first function will be the input of the second function.We will change the function and make it more complex we will make $Z = F(X, Y)$ two variables function and not $Y = F(X)$, and the X values (domain) will be the input and Y (codomain)is the output, the hacker will try to decode from Y not knowing the existence of z, but we will make in Y a second encoding that will be entered into Z, i.e., we will make the output in y to be a input (domain) and the message will exit from output (codomain) Z.

REFERENCES

[1] H. PAANANEN, M. LAPKE, M., M. SIPONEN: *State of the art in information security policy development*. Computers & Security, **88** (2020), art. no.101608.

[2] H. HABIBZADEH, B.H. NUSSBAUM, F. ANJOMSHOA, B. KANTARCI, T. SOYATA: *A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities*, Sustainable Cities and Society, 2019.

[3] V. PACHGHARE: *Cryptography and information security*, PHI Learning Pvt. Ltd., 2019.

[4] M. SNEHAPRIYA, M. DEVI: *Design and Implementation of Secure Cryptographic Algorithm Using Vedic Mathematics. Perspectives in Communication*, Embedded-systems and Signal-processing-PiCES, **3**(2) (2019), 30-32.

[5] A. NOVOKHRESTOV, A. KONEV: *Mathematical model of threats to information systems*, Paper presented at the AIP conference proceedings, 2016.

[6] L.J. LAPADULA, D.E. BELL: *Secure computer systems: A mathematical model*, Citeseer, 1996.

[7] A.B. MUNTEANU, D. FOTACHE: *Enablers of information security culture*, Procedia Economics and Finance, **20** (2015), 414-422.

[8] E.A. BENDER: *An introduction to mathematical modeling: Courier Corporation*, 2012.

[9] R. ANDERSON, C. BARTON, R. BÖHME, R. CLAYTON, M.J. VAN EETEN, M. LEVI, S. SAVAGE: *Measuring the cost of cybercrime The economics of information security and privacy*, Springer, (2013), 265-300.

[10] K. PRISLAN, I. BERNIK, G. MEŠKO, R. HACIN, B. MARKELJ, S.L. VRHOVEC: *Cybercrime victimization and seeking help: A survey of students in Slovenia*, Paper presented at the Proceedings of the Third Central European Cybersecurity Conference, 2019.

[11] J. JANG-JACCARD, S. NEPAL: *A survey of emerging threats in cybersecurity*, Journal of Computer and System Sciences, **80**(5) (2014), 973-993.

[12] H.S. LIN, A.Z. SPECTOR, P.G. NEUMANN, S.E. GOODMAN: *Toward a safer and more secure cyberspace*, Communications of the ACM, **50**(10) (2007), 128-128.

[13] E. THAMBIRAJA, G. RAMESH, D.R. UMARANI: *A survey on various most common encryption techniques*, International journal of advanced research in computer science and software engineering, **2**(7) (2012), 226-233.

[14] T. THOMAS, A.P. VIJAYARAGHAVAN, S. EMMANUEL: *Machine Learning and Cybersecurity Machine Learning Approaches in Cyber Security Analytics*, Springer (2020), 37-47.

[15] W. GHARIBI, M. SHAABI: *Cyber threats in social networking websites*, arXiv:1202.2420.

[16] A.U. REHMAN: *Understanding the Significance Of Cyber Security Threats*, VFAST Transactions on Education and Social Sciences, **3**(2) (2014), 1-6.

[17] G. SINGH, SUPRIYA: *A study of encryption algorithms (RSA, DES, 3DES and AES) for information security*, International Journal of Computer Applications, **67**(19) (2013), 33-38.

[18] B. GUPTA, D.P. AGRAWAL, S. YAMAGUCHI: *Handbook of research on modern cryptographic solutions for computer and cyber security*, IGI global, 2016.

[19] J. LI, Y. HUANG, Y. WEI, S. LV, Z. LIU, C. DONG, W. LOU: *Searchable symmetric encryption with forward search privacy*, IEEE Transactions on Dependable and Secure Computing, 2019.

[20] A. DHAVARE, R.M. LOW, M. STAMP: *Efficient cryptanalysis of homophonic substitution ciphers*, Cryptologia, **37**(3) (2013), 250-281.

[21] M. SOKOUTI, B. SOKOUTI, S. PASHAZADEH: *An approach in improving transposition cipher system*, Indian Journal of Science and Technology, **2**(8) (2009), 9-15.

[22] J. YI: *Cryptanalysis of Homophonic Substitution-Transposition Cipher*, 2014.

[23] C. DE CANNIERE, A. BIRYUKOV, B. PRENEEL : *An introduction to block cipher cryptanalysis*, Proceedings of the IEEE, **94**(2) (2006), 346-356.

[24] Z. LIN, G. WANG, X. WANG, S. YU, J. LÜ: *Security performance analysis of a chaotic stream cipher*, Nonlinear Dynamics, **94**(2) (2018), 1003-1017.

[25] G. SINGH, SUPRIYA: *A study of encryption algorithms (RSA, DES, 3DES and AES) for information security*, International Journal of Computer Applications, **67**(19) (2013), 33-38.

[26] S. CHANDRA, S. PAIRA, S.S. ALAM, G. SANYAL: *A comparative survey of symmetric and asymmetric key cryptography*, Paper presented at the 2014 International Conference on Electronics, Communication and Computational Engineering (ICECCE), 2014.

[27] M. AGRAWAL, P. MISHRA: *A comparative survey on symmetric key encryption techniques*, International Journal on Computer Science and Engineering, **4**(5) (2012), 877-882.

[28] K. ROBINSON: *What is Public Key Cryptography?*, 2018, Retrieved from https://www.twilio.com /blog/what-is-public-key-cryptography

[29] M. RASMI, K.E. AL-QAWASM: *Improving Analysis Phase in Network Forensics by Using Attack Intention Analysis*, International Journal of Security and Its Applications, **10**(5) (2016), 297-308.

[30] M. RASMI, A. AL-QEREM: *PNFEA: A Proposal Approach for Proactive Network Forensics Evidence Analysis to Resolve Cyber Crimes*, International Journal of Computer Network and Information Security, **7**(2) (2015), 25-32.

[31] J.A. NADA, M.R. AL-MOSA: *A Proposed Wireless Intrusion Detection Prevention and Attack System*, In 2018 International Arab Conference on Information Technology (ACIT), IEEE, (2018), 1-5.

[32] A. BHARDWAJ, G. SUBRAHMANYAM, V. AVASTHI, H. SASTRY: *Security algorithms for cloud computing*, Procedia Computer Science, **85** (2016), 535-542.

[33] H. KADER, M. HADHOUD: *Performance evaluation of symmetric encryption algorithms*, Performance Evaluation, (2009), 58-64.

[34] M. AGOYI, D. SERAL: *SMS security: An asymmetric encryption approach*, Paper presented at the 2010 6th International Conference on Wireless and Mobile Communications, 2010.

[35] M. FARAJZADEH: *Asymmetric encryption using RSA encryption algorithm*, Artigence, **1**(1) (2019).

[36] R.L. RIVEST, A. SHAMIR, L. ADLEMAN: *A method for obtaining digital signatures and public-key cryptosystems*, Communications of the ACM, **21**(2) (1978), 120-126.

[37] A. KAKKAR, M. SINGH, P. BANSAL: *Comparison of Various Encryption Algorithms and Techniques for Secured Data Communication*, Paper presented at the in Multinode Network", International Journal of Engineering and Technology Volume, 2012.

[38] C.J. PADMAJA, V. BHAGAVAN, B. SRINIVAS: *RSA encryption using three Mersenne primes*, Int. J. Chem. Sci, **14** (2016), 2273-2278.

[39] P. MAHAJAN, A. SACHDEVA: *A study of encryption algorithms AES, DES and RSA for security*, Global Journal of Computer Science and Technology, **13**(15) (2013), 15-22.

[40] T. ELGAMAL: *A public key cryptosystem and a signature scheme based on discrete logarithms*, IEEE transactions on information theory, **31**(4) (1985), 469-472.

[41] R. SINGH, S. KUMAR: *Elgamal's algorithm in cryptography*, International Journal of Scientific & Engineering Research, **3**(12) (2012), 1-4.

[42] M. ERICKSON, A. VAZZANA: *Introduction to number theory*, Chapman & Hall/CRC, 2007.

[43] D.M. BURTON: *Elementary number theory*, Tata McGraw-Hill Education, 2006.

[44] G.M. GHARIB: *Solutions of nonlinear equations to describe physical models in plasma*, Italian aaaajournal of pure and applied mathematics, **44** (2020), 538-546.

[45] G.M. GHARIB: *Conserved Quantities and Fluxes for Some Nonlinear Evolution Equations*, WSEAS Tansactions on Mathematics, **19** (2020), 481-485.

Department of Mathematics
Zarqa University
Zarqa
Jordan.
Email address: soso_haimour_89@yahoo.com

Department of Mathematics
Zarqa University
Zarqa
Jordan.
Email address: ggharib@zu.edu.jo

Department of Internet Technology
Zarqa University
Zarqa
Jordan.
Email address: mmousa@zu.edu.jo