A Proposed Encryption and Decryption Model

Bivek Panthi

Insight Research Club

panthibivek14@gmail.com

Rohit Bhattarai

Insight Research Club

bhattarai0rohit49@gmail.com

Sampanna Bhatta

Insight Research Club

sampannab556@gmail.com

Supervised by:

Dr. Binod Adhikari

St. Xavier’s College

binod.adhikari@sxc.edu.np

ABSTRACT

The total cost of cybercrime committed worldwide has added to a 100 billion dollars. Only 38 percent of global organizations claim they are prepared to handle a sophisticated cyber-attack. Juniper Research suggests that the average cost of a data breach will exceed $150 million by 2020, and by 2019, cybercrime will cost businesses over $2 trillion-showing an exponential increase from previous years.[1]Failed data encryption is to account for a majority of this unprofitability.

In light of this, this paper aimed to theoretically devise a function to make the data encryption process impregnable.

Standard data values to characters were assigned; cryptography, functional algebra, and modular arithmetic were employed; and, elements of randomness and data compression were utilized to formulate the cipher-text. In turn, the cipher-text is now indecipherable. At a minimum, it will turn out to be a highly feasible alternative in lieu of current encryption technologies.

1. Background

In the security of the network, cryptography has a long history of providing a way to store confidential information and transmit it through insecure networks (i.e., Internet), so that nobody can read it, except the intended recipient. The encryption system is a set of combined algorithms with keys to convert the original message (plain text) into an encrypted message (encrypted text) and convert it again on the side of the desired recipient to the original message (plain text) [2]. The main problem in designing any encryption and decryption algorithm is to improve the level of security. Therefore, this document aims to propose a modified mechanism to enhance the level of security and increase performance by minimizing a significant delay to maintain security and conduct a comparative study.

In computer systems, the algorithm constitutes of complex mathematical formulas that prescribe the rules of the process of converting simple text to encrypted text and vice versa combined with the key. However, identical keys are employed by some of the encryption and decryption algorithms that are, for both the sender and the receiver). And in other encryption and decryption algorithms, they use separate keys, but these keys must be related. During the last decades, information security has become a major problem — encryption and decryption of data. Recently they have been researched and developed widely because there is a demand for stronger encryption and deciphered that is very difficult to interpret. Cryptography plays important roles in meeting these demands. Today, many of the researchers have proposed many of the encryption and decryption algorithms, such as AES, DES, RSA, and others. But most of the proposed algorithms found some problems such as the lack of robustness and a significant amount of time added to the package delay to maintain security in the Communication channel between the terminals. In this document, the security objectives were improved to through "An Approach for Encryption and Decryption" that maintains security in the channels of communication, which makes it difficult for the attacker to preach a pattern as well as the speed of the encryption/decryption scheme.

Encryption is the most efficient way to protect data. The encryption process hides the content of a message so that the original information is retrieved only through a decryption process. Encryption is to prevent unauthorized persons from viewing or modifying the data [3]. Encryption occurs when the data is passed through some substitution technique, displacement technique, table references or mathematical operations. All these processes generate a different form of that data. The unencrypted information is called plain text, and the data is encrypted as an encrypted text, which is a representation of the original data in the form of difference [4]. Key-based algorithms employ an encryption key to encrypt the message. Two broad groups for key-based encryption are present: symmetric encryption using a single key to encrypt and decrypt the message and asymmetric encryption using two different keys public key to encrypt the message and a private key to decrypt it. Currently, there are several types of encryption algorithms based on keys, such as DES, RSA, PGP, elliptic curve and others, but everyone these algorithms depend on high mathematical manipulations [5, 6].

An original message is known as simple text, while the encoded message is called an encrypted text. The process of converting simple text to encrypted text is known as encryption or encryption; the restoration of the plaintext from the encrypted text is to decipher or decipher. The many schemes used for encryption constitute the study area known as cryptography. This scheme is known as a cryptographic or encrypted system. The techniques used to decrypt a message without any knowledge of the encryption details are included in the cryptanalysis area. A cryptographic analysis is what the layman calls "breaking the code". The areas of cryptanalysis and cryptography together are called cryptology.

Symmetric encryption is a form of cryptosystem in which encryption and decryption are made using the same key. It is also known as conventional encryption. Symmetric encryption transforms plain text into encrypted text using a secret key and an encryption algorithm. Using the identical key plus a decryption algorithm, the plain text is retrieved from the encrypted text. The two types of attack in an encryption algorithm are cryptography analysis, based on the properties of the encryption algorithm, and brute force, which involves testing all possible keys. Traditional (pre-computer) Symmetric ciphers use substitution and/or transposition techniques. Substitution techniques assign elements of the simple text (characters, bits) to elements of the encrypted text. Transposition systems orderly transpose the positions of the plaintext elements. Steganography is a technique to hide a secret message within a larger one in such a way that others cannot discern the presence or content of the hidden message.

2. Conventional cryptosystem model:

The traditional cryptosystem model encompasses the symmetric cipher model.

2.1. Symmetric cipher model

Asymmetric encryption scheme has five components (Figure 2.1):

Plain text: This is the original intelligible data or message that is entered into the algorithm as input.

Encryption algorithm: The encryption algorithm makes several substitutions and transformations in the plain text.

Secret key: The secret key is also entered into the encryption algorithm. The key is a value independent of the simple text and the algorithm. The algorithm will produce different output depending on the specific key used at that moment. The exact substitutions and transformations made by the algorithm depend on the key.

Cipher-text: This is the encoded message produced as output. It depends on the secret key and the plain-text. For a given message, two different keys will create two different encrypted texts. Encrypted text is a random data stream, and in its current form, it is unintelligible.

Decryption Algorithm: This is essentially the encryption algorithm executed in reverse. Take the encrypted text and the secret key and produce the original plain text.

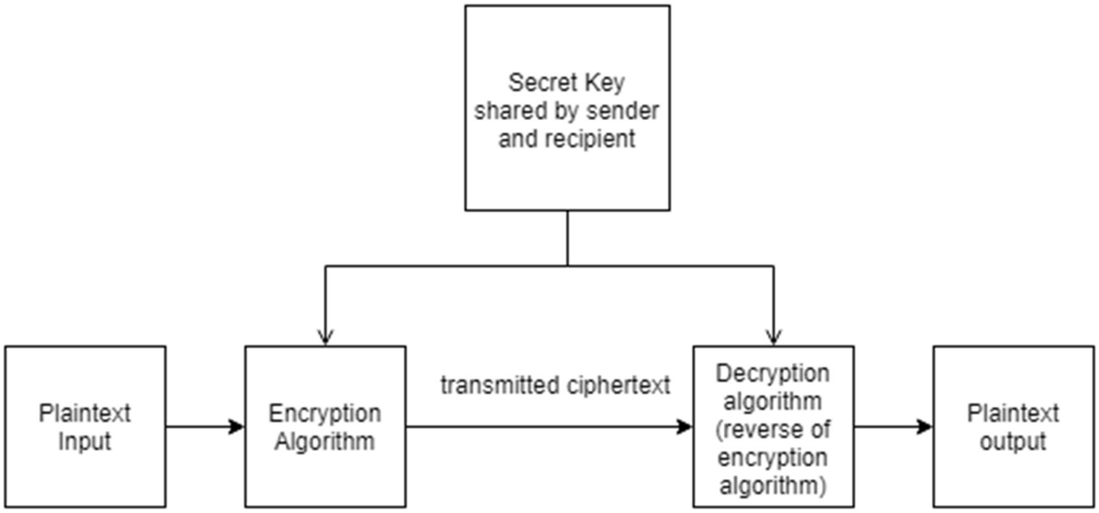

Secret Key shared by sender and recipient
Plaintext Input
Encryption Algorithm
transmitted ciphertext
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

Fig. 2.1 **Symmetric cipher model**

There are two requirements for the safe use of conventional encryption: 1. We require a powerful encryption algorithm. At least, we would like the algorithm to be such that an adversary who knows the algorithm and has access to one or more encrypted texts cannot decipher the encrypted text or decipher the key. This requirement is usually established in a stronger form: the opponent must not be able to interpret the encrypted text or discover the key, even if he or she is in possession of a series of encrypted texts along with the simple text that each ciphertext produced. The sender and the recipient must have obtained copies of the secret key securely and must keep the key secure. If someone can discover the key and know the algorithm, you can read all the communication using this key.

We assume that decrypting a message is not practical by encrypted text plus an understanding of the encryption/decryption algorithm. That is to say: we do not need to keep the algorithm secret; We need to keep the key alone secretly. This characteristic of symmetric encryption is what makes it possible for widespread use — the fact that the algorithm should not be kept secret means that manufacturers can and have developed implementations of low-cost chip data encryption algorithms. These chips are widely available and incorporated in a series of products. With the use of symmetric encryption, the main security problem is maintaining the secret of the key. Let's look more closely at the essential elements of a symmetric encryption scheme, using Figure 2.2. A source produces a message in plain text, X = [X1, X2, ..., XM]. The elements M of X are letters in some finite alphabet. In the past, the alphabet usually consisted of the 26 uppercase letters. Now, the binary alphabet {0, 1} is generally used. A key of the form K = [K1, K2, ..., KJ] is generated for encryption. If the key is generated at the origin of the message, it must also be provided to the destination through some secure channel. Instead, a third party could generate the key and deliver it securely to both the origin and the destination.

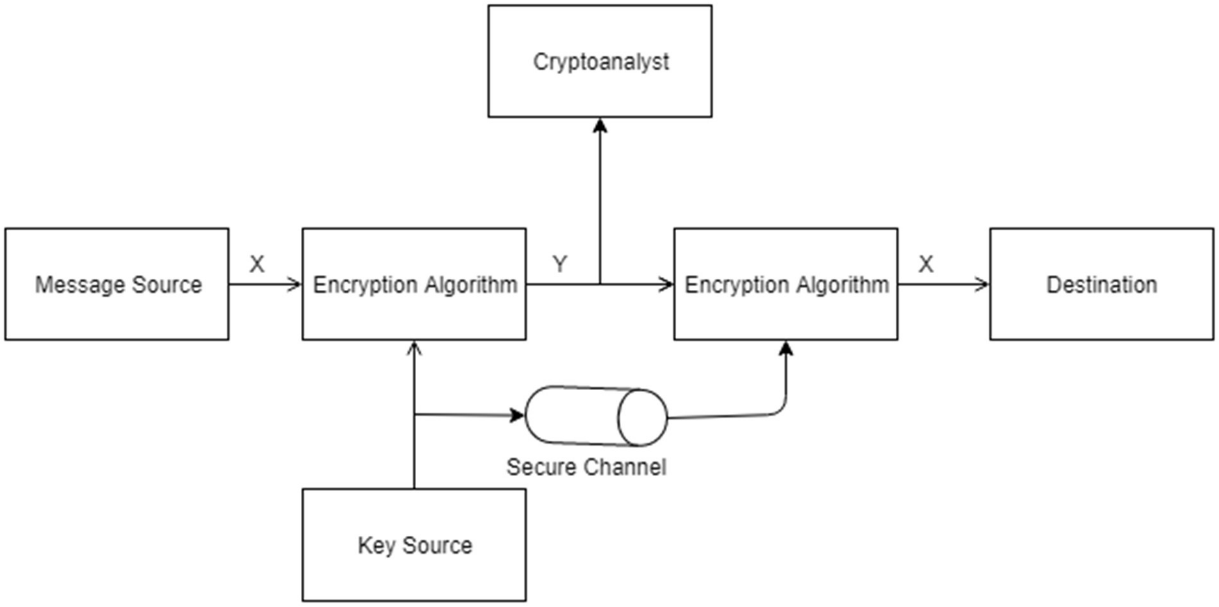


Fig 1.2. Symmetric Model Pathway

Cryptography Cryptographic systems are characterized by three independent dimensions:

1. The type of operations used to transform plain text into encrypted text. All encryption algorithms are based on two principles: substitution, in which each element of the plain-text(bit, letter, group of bits or letters) is assigned to another element, and transposition, in which the plain text elements. The fundamental requirement is that information is not lost (that is, that all operations are reversible). Most systems, called product systems, involve multiple stages of substitutions and transpositions.

2. The number of keys used. If both the sender and the receiver use the same key, the system is regarded as symmetric, single-key, secret-key or conventional encryption. And if the sender and receiver use different keys, the system is referred to as asymmetric, two-key, or public-key encryption.

3. The way in which the plain-text is processed, a block cipher processes the input one block of elements at a single time, producing an output block for each input block. A flow cipher processes the input elements continuously, producing the output one element at a time, as it progresses.

2.2 Cryptanalysis

Usually, the objective of attacking an encryption system is to recover the key in use instead of retrieving the plaintext from a single cipher-text. [7] There are two general approaches to attacking a conventional encryption scheme.

Cryptanalysis analysis: Cryptanalysis attacks are based on the nature of the algorithm and, perhaps, a certain knowledge of the general characteristics of plain text or even some sample plaintext cipher-text pairs. This type of attack exploits the features of the algorithm to get the text until an intelligible translation in plain text.

Brute Force attack: The attacker tries every possible key of a piece of encryption: on average, one should try half of all possible keys to achieving success. If either type of attack succeeds in deducting the key, the effect is catastrophic: all past and future messages encrypted with that key are compromised. First, we consider cryptanalysis, and then we discuss brute force attacks.

2.3 True random number generators

A true random number generator (TRNG) employs a non-deterministic source to create randomness. Most operate by measuring unpredictable natural processes, such as impulse detectors for ionizing radiation events, gas discharge tubes, and leaking condensers. Intel has developed a commercially available chip that takes samples of thermal noise by amplifying the measured voltage through non-driven resistors. A Bell Labs group has developed a technique that uses variations in the response time of raw read requests for a disk sector of a hard disk.LavaRnd is an open source project to create truly random numbers using inexpensive cameras, open source code, and low-cost hardware. The system uses a saturated CCD in a light-tight can as a chaotic source to produce the seed. The software processes the result in truly random numbers in a variety of formats. There are problems with both the randomness and accuracy of these numbers, not to mention the awkward requirement to connect one of these devices to each system in an internal network. Another alternative is to immerse yourself in a published collection of good quality random numbers. However, these collections provide a minimal number source compared to the potential requirements of a large network security application. Also, although the numbers in these books do show a randomness statistic, they are predictable, because an opponent who knows that the book is in use can get a copy. [8]

2. 4. Principles of public key cryptosystems

The notion of public-key cryptography resulted from an attempt to attack two of the most complex problems associated with symmetric encryption. The first problem is the distribution of keys. As we know, the distribution of keys under symmetric encryption requires (1) that two communicators already share a key, which is somehow he has distributed them; or (2) the application of a key distribution center. Whitfield Diffie, one of the discoverers of the public-key encryption (along with Martin Hellman), argued that this other requirement nullified the very essence of cryptography: the ability to keep total secrecy about your communication. As Diffie put it [9], "what good would it be, after all, to develop impenetrable cryptosystems, if your users were forced to share their passwords with a KDC that could be compromised by theft or citation?"

The second problem that Diffie considered, and one that was not related to the first, was that of "digital signatures." If the use of cryptography were generalized, not only in military situations but also for commercial and private purposes, electronic messages and documents would need the equivalent of the signatures used in paper documents. That is, could a system be devised that stipulates, to the satisfaction of all parties, that a digital message has been sent by a person?

Diffie and Hellman made an amazing breakthrough in 1976 [10, 11] find a method that addressed both problems and that was radically different from all previous approaches to cryptography, and dates back more than four millennia. [10] Diffie and Hellman publicly introduced the concepts of public-key cryptography in 1976. However, this is not the real beginning. Admiral Bobby Inman, while the director of the National Security Agency (NSA), claimed that public-key cryptography had been discovered at the NSA in the mid-1960s [12]. The first documented introduction of these concepts occurred in 1970, from Communications-Electronics Security Group, the British counterpart of the NSA, in a classified report by James Ellis [13]. Ellis refers to the technique as not -secret coding and describes the discovery in [14]. In the next subsection, we look at the general framework for public-key cryptography. We then examine the requirements for the encryption/decryption algorithm that is at the heart of the scheme.

Public key cryptosystems Asymmetric algorithms are based on a key for encryption and a different but similar key for decryption. These algorithms have some important features: ● It is computationally impossible to determine the decryption key, given the unique facts of the cryptographic algorithm and the encryption key.

Also, some algorithms, such as RSA, also present the following feature: ● Either of the two related keys can be used for encryption, and the other is used for decryption. A public-key encryption scheme has six ingredients. ● Simple text: This is the message or data legible that are entered into the algorithm as input. ● Encryption algorithm: the encryption algorithm performs several transformations in the plain text. ● Public and private keys: these are a pair of keys that were selected so that if one of them is used for decryption, the other is used for encryption. The precise transformations performed by the algorithm depend on the private or public key that is provided as input. ● Encrypted text: this is the encoded message produced as output depends on the plaintext and the key so that for a given message, two different keys will create two different encrypted texts. ● Decryption algorithm: this algorithm accepts the encrypted text and the corresponding key and produces the original plain text.

3. Proposed model:

For encryption and decryption, we need to convert the text that could contain alphabets, numbers, special characters, etc. in mathematical form: numbers.

3.1 Characteristics:

3.1.1. A significant increase in data security.

3.1.2. Does not require reverse engineering.
Decryptor can decipher, similarly to how cipher Encrypt the data. However, hackers would employ reverse engineering that would be practically indecipherable

3.1.3. It does not imply prime numbers, so its approach is quite unorthodox.

3.1.4. Only the numbers of two digits they replace the characters, so it is feasible to transport data in large volumes. Also, the initial assignment of characters to numbers does not have to correspond to the proposed model.

3.1.5. In the same way, the function used can easily be modified by the person or institution that uses the proposed model.

3.1.6. In the same way, the function used can easily be modified by the person or institution that uses the proposed cipher model.

3.1.7. This proliferates the security level to even greater heights.

3.1.8. The delay time is minimal.

3.1.9. Everything is public. There is no channel safe, but the information cannot be filtered through the channel, which decreases the possibilities of deciphering.

3.2 Transaction number:

Modular arithmetic has been employed for the secure transmission of numbers. The process is described below:

Device 1 chooses a random number, say ‘A’, and using public prime ‘P’ calculates ‘i1’. Similarly, device 2 chooses another number, say ‘B’, and using the public prime ‘P’ calculates ‘i2’. The so formed numbers i1 and i2 are shared between devices. Then using i1, i2, and A, device 1 calculates ‘Z1’ and using i1, i2, and B, device 1 calculates ‘Z2’. The numbers Z1andZ2 are shared. Now using Z2 and A, device 1 calculates S which is the same number obtained by device 2 by using Z1 and B. Hence, a number S is transmitted without being sent. An eavesdropper cannot calculate the number without knowing A or B, which are entirely random numbers.

Calculate mod sends it via secure transmission and receives another random number ‘B’. Now device 1 calculates selects its own secret number, suppose A, and for device 2, B. (A and B are not shared to anyone not even between Device 1 and 2)

Now a random public number P is released, known to all. **Processes for Device 1:**

Processes for Device 1:

$A \equiv i_1 \pmod P$ $B \equiv i_2 \pmod P$

(i_1 and i_2 are shared between Device 1 and Device2.)

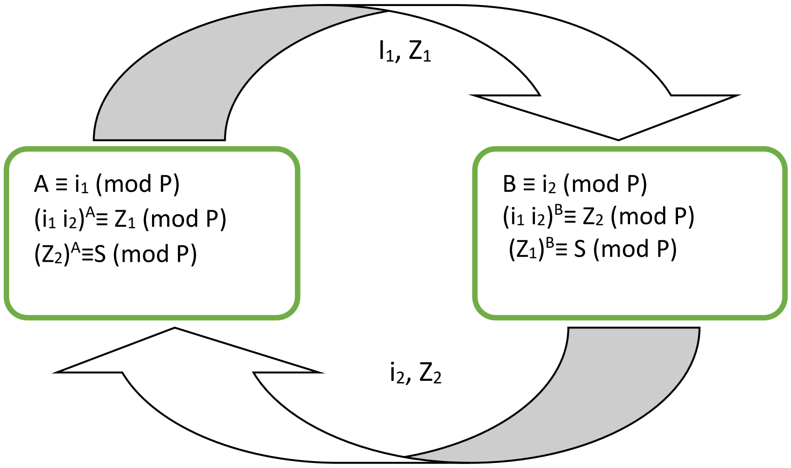
$(i_1\, i_2)^A \equiv Z_1 \pmod P$ $(i_1\, i_2)^B \equiv Z_2 \pmod P$

(Z_1 and Z_2 are shared between Device1 and Device2.)

$(Z_2)^A \equiv S \pmod P$ $(Z_1)^B \equiv S \pmod P$

Hence a number S is transacted safely. There is no problem if anyone in between get track of P, i_1, i_2,Z_1, and Z_2.

Similarly, other numbers of the function can be safely transected which are used for assigning the standard values.


I_1, Z_1
$A \equiv i_1 \pmod P$
$(i_1\, i_2)^A \equiv Z_1 \pmod P$
$(Z_2)^A \equiv S \pmod P$
$B \equiv i_2 \pmod P$
$(i_1\, i_2)^B \equiv Z_2 \pmod P$
$(Z_1)^B \equiv S \pmod P$
i_2, Z_2

3.3 Definition of standard values

For the conversion into numbers, we first begin by describing the standard values for all the characters. For example, 'a' = 1, 'b' = 2, and so on. However, there would be ambiguity since the value '12' can represent 'l' or 'ab', to prevent us from assigning 2-digit numbers or 3-digit numbers depending on the number of characters used by the text that is to be encrypted and protected.When doing so, every two digits would represent a character.

So, now, let's define our standard values for alphabets according to the following table:

a = 11	b = 12	c = 13	d = 14	e = 15	f = 16
g = 17	h = 18	i = 19	j = 20	k = 21	l = 22
m = 23	n = 24	o = 25	p = 26	q = 27	r = 28
s = 29	t = 30	u = 31	v = 32	w = 33	x = 34
y = 35	z = 36				

3.4 Changing Variable Assumption

Now, each of the above standard values serves as a value for a function which results in different two-digit numbers.

Consider a function: $f(S_1, S_2) = {S_1}^{SV} + {S_2}^{SV}$, where ‘SV’ is standard value of a character.

Where 'S_1' and 'S_2' are secret numbers which are sent by the process described above.

And 'S' is the standard value for a given character as defined in the table above, i.e. for 'a', SV=11, for ‘b’, SV=12, for 'p', SV=29.

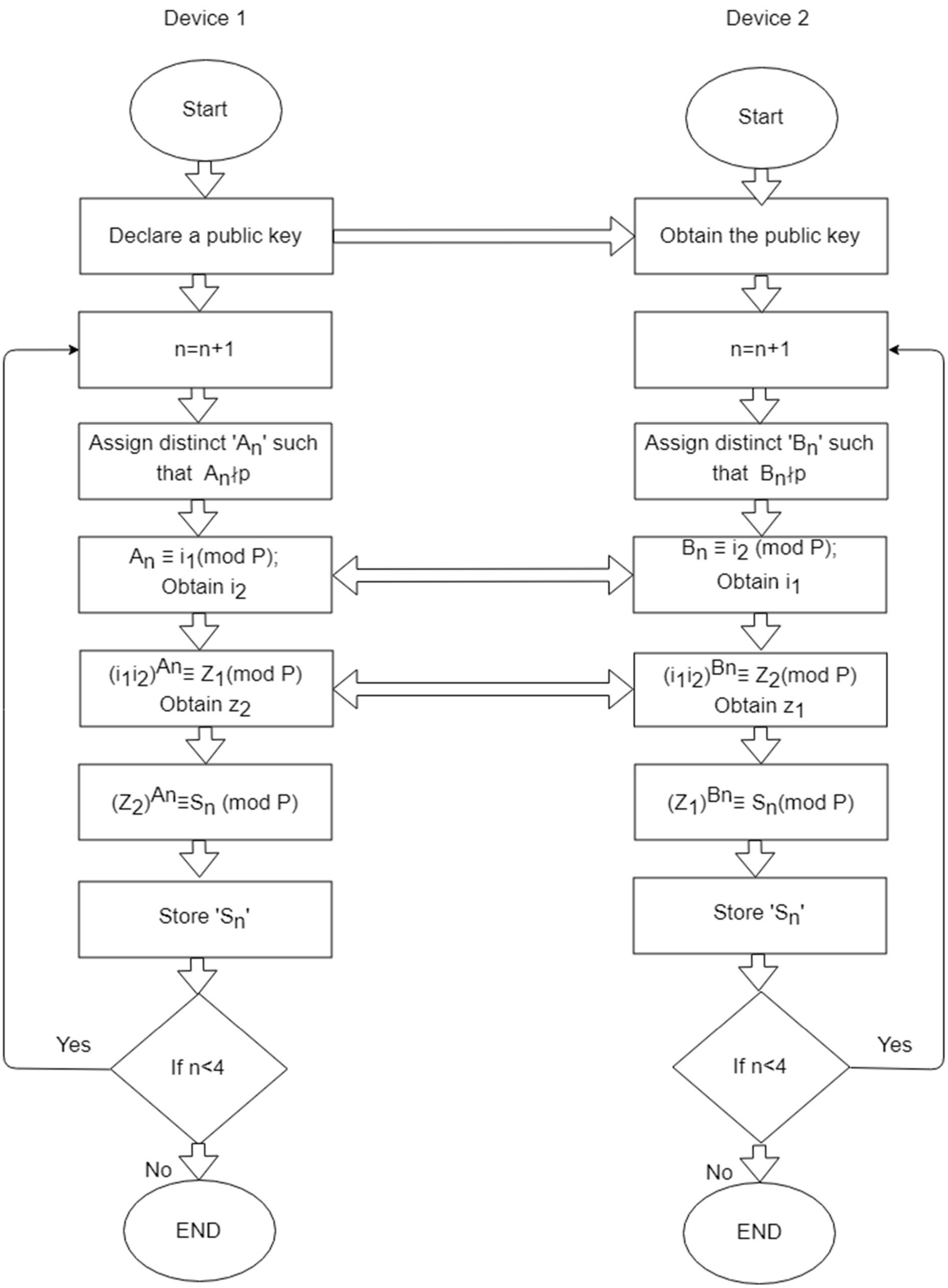
As we can see, a function should have a pair of values which are variablesbut can be assigned as secret numbers: 'S_1' and 'S_2'. After assigning secret numbers to the function, we will run the function for all the standard values. For each standard value, the function will generate a unique number. Now, we shall take the first two digits of the result as the actual value of the character whose standard value was used.

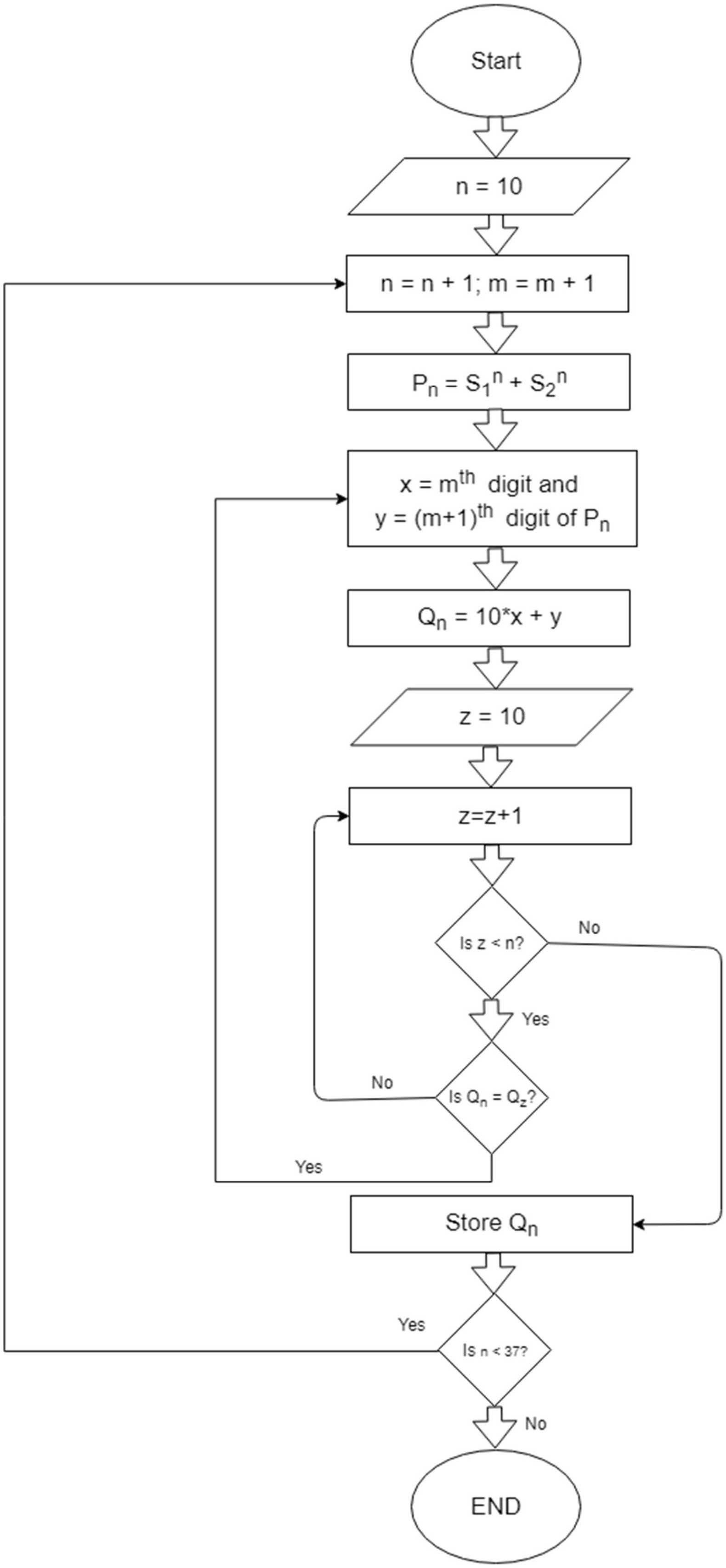
For example, say the secret pair is (4,5), after running the function for standard value 'SV'=20, we get the result of the function as 1458796321, then the value for 'j'=14. The standard value should run in ascending order. In cases when the first two digits of the result are same for two characters, the latter one should take first and third digit as the actual value and so on.

Similarly, $f_{13}(2,3) = 2^{13} + 3^{13}$=1602515. The first two digits are 16, so the actual value of 'c'=16.

In this way, all the characters are provided with a unique two-digit number.

Both devices use the process for encryption and decryption.


Device 1
Device 2
Start
Start
Declare a public key
Obtain the public key
n=n+1
n=n+1
Assign distinct 'A_n' such that $A_n \nmid p$
Assign distinct 'B_n' such that $B_n \nmid p$
$A_n \equiv i_1 (\mathrm{mod}\ P)$; Obtain i_2
$B_n \equiv i_2\ (\mathrm{mod}\ P)$; Obtain i_1
$(i_1 i_2)^{An} \equiv Z_1 (\mathrm{mod}\ P)$ Obtain z_2
$(i_1 i_2)^{Bn} \equiv Z_2 (\mathrm{mod}\ P)$ Obtain z_1
$(Z_2)^{An} \equiv S_n\ (\mathrm{mod}\ P)$
$(Z_1)^{Bn} \equiv S_n (\mathrm{mod}\ P)$
Store 'S_n'
Store 'S_n'
Yes
If n<4
If n<4
Yes
No
No
END
END


Start
n = 10
n = n + 1; m = m + 1
$P_n = S_1^n + S_2^n$
x = m^{th} digit and
y = $(m+1)^{th}$ digit of P_n
$Q_n = 10*x + y$
z = 10
z=z+1
Is z < n?
No
Yes
Is $Q_n = Q_z$?
No
Yes
Store Q_n
Yes
Is n < 37?
No
END

3.5 Conversion of "text" into "numbers":

After obtaining all the values of characters, each character in the text is replaced with its corresponding number. Then we shall have a large number with an even number of digits if we have chosen a two-digit number for each character.

3.6 Inserting a random number after every ‘S_3’ digits

So, to avoid the reverse process for unauthorized access, we shall insert a random number after every S_3th digit, where 'S_3' is also a secret number.-

3.7 Decryption

For decryption, the authorized person (Device 2) would have all the secret numbers. So, the person will run the same function with 'S_1' and 'S_2'. On the other hand, he/she would divide the encrypted number obtained from the author by the secret prime 'p'. Then, he/she would remove all those random numbers after each rth digit and convert the result into characters as per the table obtained fromthe function.

Citations:

[1] Banker M.- JUNIPER Research Ltd, 2015

[2] Zimmerman P., "An Introduction to Cryptography", Doubleday & Company, Inc., United State of America, USA, 1999.

[3] Freeman J., Neely R., and Megalo L. “Developing Secure Systems: Issues and Solutions”. IEEE Journal of Computer and Communication, Vol. 89, PP. 36-45. 1998

[4] Agnew G. B., Mullin R. C., Onyszchuk I. M., and Vqanstone S. A. “An Implementation for a Fast Public-Key Cryptosystems”. Journal of Cryptology, Vol.3, No 2, PP. 63-79. 1995.

[5] Beth T. and Gollmann D. “Algorithm Engineering for Public Key Algorithms”. IEEE Journal on Selected Areas in Communications; Vol. 7, No 4, PP. 458-466. 1989

[6] IBM. “The Data Encryption Standard (DES) and its strength against attacks”. IBM Journal of Research and Development, Vol. 38, PP. 243-250. 1994

[6] William S., Cryptography and Network Security (4th Edition), Prentice-Hall, Inc., Upper Saddle River, NJ, 2005

[7] Gardner, M. Codes, Ciphers, and Secret Writing. New York: Dover, 1972

[8] THE INTEL® RANDOM NUMBER GENERATOR CRYPTOGRAPHY RESEARCH, INC. WHITE PAPER PREPARED FOR INTEL CORPORATION Benjamin Jun and Paul Kocher April 22, 1999

[9] Diffie, W. "The First Ten Years of Public-Key Cryptography." Proceedings of the IEEE, May 1988.

[10] Diffie, W., and Hellman, M. "New Directions in Cryptography." Proceedings of the AFIPS National Computer Conference, June 1976.

[11] Diffie, W., and Hellman, M. "Multiuser Cryptographic Techniques." IEEE Transactions on Information Theory, November 1976.

[12] Simmons, G. "Cryptology." Encyclopaedia Britannica, Fifteenth Edition, 1993

[13] Ellis, J. The Possibility of Secure Non-Secret Digital Encryption. CESG Report, January 1970.

[14] Ellis, J. "The History of Non-Secret Encryption." Cryptologia, July 1999