CRYPTOGRAPHY: FROM THE ANCIENT HISTORY TO NOW, IT'S APPLICATIONS AND A NEW COMPLETE NUMERICAL MODEL

Method · July 2021

DOI: 10.13140/RG.2.2.13438.51524

s. M. Naser
Bangladesh University of Engineering and Technology

CRYPTOGRAPHY: FROM THE ANCIENT HISTORY TO NOW, IT'S APPLICATIONS AND A NEW COMPLETE NUMERICAL MODEL

S. M. Naser
Department of Mathematics, Bangladesh University of Engineering and Technology

ABSTRACT: *In this computer and internet based modern era, people have to deal with private information in thousands way. Today's prime concern is to keep secure the information of different channel and medium related to one's and to communicate securely, and to do so cryptography method is the sole key to it. This research paper will briefly lighten on the history of cryptography, basic definitions related to cryptography and some basic theorems to build different types of cryptography models. This research paper will propose few propositions based on solvability equation and will introduce a solvability series. From ancient time to now there are several cryptographic models are invented. This research paper will present a new type of complete model of cryptography with the help of a modified solvability proposition and solvability series, different from others***.**

KEYWORDS: cryptography, cryptography history, cryptography application, solvability equation, cryptography model

INTRODUCTION

The word cryptography comes from the Greek words kryptos- means hidden and graphein- means writing; altogether the word cryptography means hidden and writing [1]. Usually Cryptography is the process of secret message or secret communication between two individuals or two groups to protect the security of secrecy from any others. From the beginning of civilization when people started to live in different tribes or groups, each of them got the idea to be more powerful than others and to rule other tribes. So they feel for a secure and secret communication and thus how the process of primary cryptography was introduced.

History

Recent days, almost everywhere in electronic based world, cryptography has it's applications. Even though the vast uses of cryptography has not started a long time ago, but the classical use of cryptography has a long history back.

Ancient Cryptography

The study dated back to the ancient civilization, historical proof of using cryptography method is found, which links up to the modern electronic cryptography. People used cryptography to communicate in the early civilization at the region of Egypt, Greece and Rome. Nearly 1900 B.C. [1] (2000 B.C. [2]), in ancient Egypt a non standard cryptography was used on secret hieroglyphics carved on stone- the known earliest cryptography; to hide the meanings from others who did not know it, for the amusement. With the improvement of science, language and writing ability a better form of cryptography was used in ancient Greece, namely the “Scytale” of Sparta [2], which is to be claimed to use among the Spartan military. The idea of this cryptography was generated by using wound tape and sticks [1]. One another early substitution cipher was ceaser shift cipher used in ancient Rome- a mono alphabetic cipher, which was introduced by shifting the position of alphabets. “Atbash” is one of the early ciphers in Hebrew language. In ancient India, there were two kinds of ciphers Kauitiliyam and Mulavediya noted in 2000 year old Kamasutra of Vatsyayana. Kautiliyam cipher was built based on phonetic relations, such as interchanging vowel and consonants and Mulavediya cipher was established by using pair of letters and using the reciprocal ones [3]. In Persia, during the reign of Sasanian kings there were two secret scripts named *šāh-dabīrīya-* for the official correspondence and *rāz-saharīya-* to communicate secret messages with other countries, noted by the Muslim author Ibn al-Nadim [4].

Mainly those classical cryptography methods were based on the rearrangement of alphabets or replacement of positions of alphabets or replacements of different alphabets of different languages, which can be said as transposition ciphers. As examples: “HOW ARE YOU?” could be coded as “WHO ERA UOY?”. Again taking “D” as the position of first alphabet or replacing “A” by “D” and in same way replacing all other alphabets sequentially, “How are you?” could be coded as “ERZ DUH BRX?”.

Advance Cryptography

With the advancement of science, cryptographic technology was also evolving very rapidly and the need to use new term was realized. D. Kahn thinks the modern cryptography was originated in Arab. The first use of mathematical terms- permutations and combinations was in the book of Al-Khalil’s “Book of Cryptographic Messages”, to list all possible Arabic words with and without vowels. A manuscript discovered recently reports that, Arab mathematician and polymath Al-Kindi in 9th century used frequency analysis in building cipher text and wrote a book on cryptography entitled “Rislah fi Istikharaj al-Mu’amma”. Those ciphers are still use to make puzzles [5]. First clearly described work on poly alphabetic cipher is found in the work of Al-Qalqashandi based on earlier work of Ibn al-Durayhim, where each plaintext letter is assigned more than one substitute [6].

Cryptographic Device and Device Based Modern Cryptography

The first cipher device was probably invented by Leon Battista Alberti, an automatic cipher device, where he used a wheel. Then the most interesting cipher device, the Vigenere cipher, poly alphabetic cipher, was invented by Blaise de Vigenere, where a modification of ceaser cipher was used [7]. Several sophisticated cipher machine was invented till early 20th century. During the World War II German soldiers used Enigma machine to transfer the crucial data among the Nazi soldiers, was invented by German engineer Arthur Scherbius at the end of World War I in a view to protect commercial, diplomatic, and military communication. It was one of the finest rotor machines among the others at that time [7].

In modern era, with the revolution of electronic machines such as computer, cryptographic method meets with new mathematical formulas with extensive use of mathematics, including aspects of information theory, computational complexity, statistics, abstract algebra, and finite mathematics generally. Nowadays many computer ciphers are organized by their binary bit sequences. In 1970s decade the introduction of public key cryptography introduced a new type of cryptography using integer modulo n ([8], [9]). The most modern attachment in the field of cryptography is the digital signature. The idea of digital signature was first introduced by Diffie-Hellman in a paper titled "New Directions in Cryptography" [10].

BASIC DEFINITIONS AND THEOREMS

This section will described briefly, all the terms used in cryptography model.

Cryptography

The prefix "crypt-" means "hidden" or "vault" -- and the suffix "-graphy" stands for "writing". Cryptography or cryptology is the practice and study of techniques for secure communication in the presence of "adversaries" (the third parties). More generally, cryptography is about burning the message in such a way that prevents third parties or the public from reading private messages [11]. Cryptography is a method of protecting information and communications through the use of codes, so that only those for whom the information is intended can read and process it.

There are three types of cryptography method.

1. Symmetric
2. Asymmetric
3. Hybrid

Symmetric Key Cryptography

In symmetric key cryptography (also known as private-key cryptography) a secret key may be held by one person or exchanged between the sender and the receiver of a message. If private key cryptography is used to send secret messages between two parties, both the sender and receiver must have a copy of the secret key.

Asymmetric Key Cryptography

In the two-key system (also known as the public key system) one key encrypts the information and another, mathematically related key decrypts it. The computer sending an encrypted message uses a chosen private key that is never shared and so is known only to the sender. Using this public-key cryptographic method, the sender and receiver are able to authenticate one another as well as protect the secrecy of the message [16].

Plaintext

In cryptography, plaintext usually means unencrypted information or the original intelligible message or data that someone wishes to another, fed into the algorithm as input [13].

Key

In cryptography, a key is a piece of information (a parameter) that determines the functional output of a cryptographic algorithm. For encryption algorithms, a key specifies the transformation of plaintext into ciphertext, and vice versa depending on the decryption algorithm. Keys also specify transformations in other cryptographic algorithms, such as digital signature schemes and message authentication codes.

Secret Key

The secret key is also input to the encryption algorithm. The key is a value independent of the plaintext and of the algorithm. The algorithm will produce a different output depending on the specific key being used at the time. The exact substitutions and transformations performed by the algorithm depend on the key [12].

Encryption algorithm

The encryption algorithm performs various substitutions and transformations on the plaintext.

Ciphertext

Ciphertext or cyphertext is the encrypted or encoded information because it contains a form of the original plaintext that is unreadable by a human or computer without the proper cipher to decrypt it. This is the scrambled message produced as output. It depends on the plaintext and the secret key.

Decryption Algorithm

This is essentially the encryption algorithm run in receives. It takes the ciphertext and the secret key and produces the original plaintext.

Encryption

A process of converting Plain Text into Cipher Text is called Encryption. Cryptographers use various encryption methods to send confidential messages via an insecure channel. The process of encryption requires two things – an encryption algorithm and a key. An encryption algorithm means the method that has been used to encrypt the data. Encryption happens at the sender's side.

Decryption

The reverse process of encryption is called Decryption. It is the process of converting Cipher Text into Plain Text. Cryptographers use the decryption algorithms at the receiver side to obtain the original message from non readable message i.e. Cipher Text. The process of decryption requires two things – a Decryption algorithm and a key. A Decryption algorithm means the method that has been used in Decryption. Generally the encryption and decryption algorithm are identical but reverse.

Encoder

An encoder is the person that wants to send the message and uses encryption to make the messages secure.

Decoder

A decoder is the person who decrypts the message. This may be the intended recipient of the message or may be an intruder, trying to get access to the secret message.

Public-Key cryptography:

Public-Key cryptography is a form of cryptosystem in which encryption and decryption are performed using the different keys- one a public key and one a private key. These keys are mathematically related although knowledge of one key does not allows someone to easily determine the other key. The sender A uses the public key of receiver B (or some set of rules) to encrypt the plaintext message M and sends the ciphertext C to the receiver. The receiver applies own private key (or rule set) to decrypt the cipher text C and recover the plaintext message M. Because pair of keys is required, this approach is also called asymmetric cryptography. Asymmetric encryption can be used for confidentiality, authentication, or both [14].

Public-key cryptography is used interchangeably with asymmetric cryptography; they both denote exactly the same thing and are used synonymously. Symmetric cryptography has been used for at least 400 years. Public-key cryptography, on the other hand, is quite new. It was publicly introduced by Whitfield Diffie, Martin Hellman and Ralph Merkle in 1976. Much more recently, in 1997 British documents which were declassified revealed that the researchers James Ellis, Clifford Cocks and Graham Williamson from the Uk’s Government Communications Headquarters (GCHQ) discovered and realized the principle of public-key cryptography few years earlier, in 1972. However, it is still being debated whether the government office fully recognized the far-reaching consequences of public key cryptography for commercial security applications [15].

Diffie-Hellman Key Exchange

A simple public-key algorithm is Diffie-Hellman key exchange. This protocol enables two users to establish a secret key using a public-key scheme based on discrete logarithms. The protocol is secure only if the authenticity of the two participants can be established. D-H is used for secret-key key exchange only, and not for authentication or digital signatures.

RSA

The first, and still most common, public key cryptography implementation, named for the three MIT mathematicians, who developed it – Ronald Rivest, Adi Shamir, and Leonard Adleman. RSA today is used in hundreds of software products and can be used for key exchange, digital signatures, or encryption of small blocks of data. RSA uses a variable size encryption block and a variable size key. The key-pair is derived from a very large number n, that is the product of two prime numbers chosen according to special rules; these primes may be 100 or more digits in length each, yielding an n with roughly twice as many digits as the prime factors. RSA has three phases: Key Generation, Encryption, and Decryption.

Cipher

Cipher is the algorithm that is used to transform plaintext to cipher text. This method is called encryption, in other words, it's a mechanism of converting readable and understandable data into "meaningless" data [16].

Rotor Machines

In cryptography, a rotor machine is an electro-mechanical stream cipher device used for encrypting and decrypting messages. In the 1920s, various mechanical encryption devices were invented to automate the process of encryption. Most were based on the concept of a rotor, a mechanical wheel wired to perform a general substitution [17].

Congruence Modulo n

For any given positive integer $n > 1$, two integers a and b is called congruence modulo n, if n is a divisor of the difference of these two integers a and b. Then the congruence modulo is denoted by the equivalence relation as following,

$$a \equiv b(mod\, n).$$

Which means, $a - b$ is divisible by n. i.e., there exist an integer k such that, $a - b = kn$.

As an example, Let, $a = 17$, $b = 3$, $n = 2$.

Then, $a - {}^{b}\!/_{n} = (17 - 3)/2 = 7 = k(suppose)$. Then the whole calculation can be written in the form of congruence modulo n as, $17 \equiv 3(mod\ 2)$.

Reduction Map and Lift

We call the natural reduction map $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, which sends a to $a + n\mathbb{Z}$, reduction modulo n. We also say that a is a lift of $a + n\mathbb{Z}$. Thus, e.g., 7 is a lift of $1\ mod\ 3$, since $7 + 3\mathbb{Z} = 1 + 3\mathbb{Z}$ [8]. Similarly, 13 is a lift of $3\ mod\ 5$, since $13 + 5\mathbb{Z} = 3 + 5\mathbb{Z}$.

Solvability

The equation $ax \equiv b(mod\ n)$ has a solution if and only if $\gcd(a, n)$ divides b.

Euler's $\varphi - function$

For $n \in N$, let

$$\varphi(n) = \#\{a \in N: a \leq n\ and\ \gcd(a, n) = 1\}$$

For example,

$$\varphi(1) = \#\{1\} = 1,$$
$$\varphi(2) = \#\{1\} = 1,$$
$$\varphi(3) = \#\{1,2\} = 2$$
$$\varphi(4) = \#\{1,3\} = 2,$$
$$\varphi(7) = \#\{1,2,3,4,5,6\} = 6$$
$$\varphi(9) = \#\{1,2,4,5,7,8\} = 6,$$

Also, if p is any prime number then

$$\varphi(p) = \#\{1,2, \ldots, p - 1\} = p - 1$$

Using Euler's $\varphi - function$ it is simple to find out the number of relatively prime number of a given natural number and if the natural number is a prime number p then the number of relatively prime number less than p is $p-1$ [8].

Euler's Theorem
If $\gcd(x, n) = 1$, then $x^{\varphi(n)} \equiv 1\ (mod\ n)$.

Chinese Remainder Theorem
Let $a, b \in \mathbb{Z}$ and $n, m\ \in \mathbb{N}$ such that $\gcd(n\ , m\ ) = 1$. Then there exists $x \in \mathbb{Z}$ such that

$$x \equiv a\ (mod\ m\ ),$$
$$x \equiv b\ (mod\ n\ )$$

Moreover x is unique modulo [8].

Extended Euclidean Representation
Suppose $a, b \in \mathbb{Z}$ and let $g = \gcd(a, b)$. Then there exists $x, y \in \mathbb{Z}$ such that

$$ax + by = g\ .$$

Example
Suppose $a = 9$ and $b = 13$. Then $\gcd(9{,}13)$ can be calculated as follows:

$$\begin{aligned} 13 &= 1.9 + 4 & so\ , 4 &= 13 - 9 \\ 9 &= 2.4 + 1 & so, 1 &= 9 - 2.4 \\ & & or, 1 &= 9 - 2.(13 - 9) \\ & & or, 1 &= 3.9 - 2.13 \end{aligned}$$

Pseudoprimality
An integer $p > 1$ is prime if and only if for every $a \not\equiv 0(mod\ p)$,

$$a^{p-1} \equiv 1(mod\ p)$$

Wilson's Theorem
An integer $p > 1$ is prime if and only if

$$(p-1)! \equiv -1(mod\ p).$$

For example, if $p = 7$, then

$$(p-1)! = 6! = 720 \equiv -1(mod\ 7).$$

But if $p = 6$, then

$$(p-1)! = 5! = 120 \equiv 1(mod\ 7)$$

So 6 is a composite number.

Wilson's theorem, from a computational point of view, probably one of the world's least efficient primality tests since computing $(n-1)!$ takes so many steps [8].

APPLICATIONS

In this section few applications of cryptography and cryptographic goals will be described in brief.

Applications of Cryptography

There are thousands of applications of cryptography in everyday life. In this modern era of computer and internet based life, to keep secrecy of private data and for secure communication cryptography is the major key.

Computer Security

By cryptography a collection of tools designed to protect any data from hackers, theft, corruption or natural disaster while allowing these data to be available to the users at the same time. The example of these tools is the antivirus program.

Network Security

Network security refers to any activity designed to protect the usability, integrity, reliability and safety of data during their transmission on a network. Network security deals with hardware and software.

Internet Security

Internet security is measures and procedures used to protect data during their transmission over a collection of interconnected networks, while information security is about how to prevent attacks and to detect attacks on information-based systems [19].

Secrecy in Transmission

In any type of transmission of data it is the simple and secured way to use a private key to keep the secrecy of data, meaning with reasonable assurance and low overhead.

Secrecy in Storage

To maintain the secrecy of information storage a one-key system can be used where the key is known by the user and to read the information meaningfully, that is encryption and decryption process can only be performed by using the key. The problem of this storage process is if the key is forgotten then it never can be read or if the key is stolen by hacker then the secrecy could be revealed.

Integrity in Transmission

In some case integrity of transmission is more important than secrecy of transmission. As an example, the electronic funds transfer amount of a bank could be known by the public. But if the transferred checksums information is known by the third party, then it could be transfer to wrong receiver. In this case, Cryptographic techniques are widely used to encrypt the checksums information and to send the receiver and again by decryption and comparing the information of receiver checksums, the integrity of transmission is assured.

Integrity in Storage

The major mean of assuring integrity of stored information has historically been access control, where access control includes system of locks and keys, guards and other mechanisms of a physical or logical nature.

Authentication of Identity

Where previous time authentication of identity was provided by the simple password system, now the modern strong cryptographic transforms are providing highly reliability and authentication of identity.

Credentialing Systems

In electronic credit card cryptography is used to store secret information.

Electronic Signatures

Electronic signatures are a means of providing a legally binding transaction between two or more parties which is hard to forge and easy to use.

Electronic Cash

There are patents under force throughout the world today to allow electronic information to replace cash money for financial transactions between individuals. Such a system involves using cryptography to keep the assets of nations in electronic form.

Threshold systems

Thresholding systems are systems where a minimal number of individuals are allowed from the total number of individuals. For example, in a nuclear arms situation, one might want a system wherein three out of five members of the joint chief of staff agree. Most threshold systems are based on encryption with keys which are distributed in parts.

Systems Using Changing Keys

Regular change of keys increases the safety of the system from any kind of outside attack which can be organized by using cryptography [20].

Cryptography Goals

Cryptography has many goals to achieve. These goals can be either all achieved at the same time in one application, or only one of them. These goals are:

Confidentiality: It is the most important goal, that ensures that nobody can understand the received message except the one who has the decipher key.

Authentication: It is the process of providing the identity that assures the communicating entity is the one that it claimed to be. This means that the user or the system can prove their own identities to other parties who don’t have personal knowledge of their identities.

Data Integrity: It ensures that the received messages have not been changed in any way from its original form. The data may get modified by an unauthorized entity intentionally or accidentally. Integrity service confirms that whether data is intact or not since it was last created, transmitted, or stored by an authorized user. This can be achieved by using hashing at both sides the sender and the recipient in order to create a unique message digest and compare it with the one that received.

Non-Repudiation: It is mechanism used to prove that the sender really sent this message, and the message was received by the specified party, so the recipient cannot claim that the message was not sent. For example, once an order is placed electronically, a purchaser cannot deny the purchase order, if non-repudiation service was enabled in this transaction.

Access Control: It is the process of preventing an unauthorized use of resources. This goal controls who can have access to the resources. If one can access, under which restrictions and conditions the access can be occurred, and what is the permission level of a given access ([16], [18]).

METHODOLOGY

First this paper will introduce modified solvability with brief illustration on modified solvability and for the solvability equation a solvable series will be proposed. Then based on solvable series a method of encryption and decryption will be described. The whole method is given below step by step:

Step-1: Cryptographic key

The encoder and the decoder secretly choose a solvable equation $ax \equiv b(mod\, n)$ which is known to both of them. Then both of them will compute the value of $a^{'}, b^{'}$ and $n^{'}$as following,

$$a^{'} = \frac{\mathrm{a}}{gcd(a,n)}, \qquad b^{'} = \frac{b}{gcd(a,n)} \quad and \quad n^{'} = \frac{n}{gcd(a,n)}$$

The solvable equation is the key equation of this model.

Then the difference of any two consecutive solutions is $d = n^{'} = 5$.

Step-2: Plain text

First the encoder will select a plain text. Then comparing with the alphabet-numerical table, the encoder will find out the numerical value of each letter of the word and will put it in an array. Each letter will be separated into the array by a comma. Each word will be separated into different array by a comma between two arrays.

Step-3: Encryption

The encryption key is $E_m(x) = x_m$, where m is the alphabetic position of the letter. The encryption equation can be written as,

$$k = x = \frac{yn^{'} + b^{'}}{a^{'}}$$

$k = x_1$ is the first integer solution of x for a certain value of y.
The difference between two consecutive solutions is $d = n^{'}$.
Then, putting the value of k and d in the general solvability series as following,

$$x_m = k + (m - 1)d,$$

the encoder will obtain solution series.
Putting the value of $m = 1, 2, \dots ,26$ in the above equation the encoder will build the encryption table, where the value of $E_m(x)$ will be found for the value of m.
Then replacing the value of m by $E_m(x)$ from the array, the new array will be the cipher text of this model. Then the encoder will send the cipher text to the receiver who is the decoder.

Step-4: Decryption
The receiver will get the cipher text.
The decryption key is $= D_m(y) = y_m$
The decryption equation can be written as

$$f = y = \frac{a^{'}x - b^{'}}{n^{'}}$$

$f = y_1$ is the first integer solution of this equation for a certain value of y.
Then, the second value $f = y_2$ will be obtained for a certain value of x.
The difference between two consecutive solutions of f is $d_y = y_{n+1} - y_n$.
Then the decryption table can be found by putting $m = 1,2, \dots ,26$ in the following equation,

$$y_m = f + (m - 1)d_y$$

Now, consider the given encrypted cipher.
Putting all those values of x_m from the cipher array in the equation $y = \frac{a^{'}x-b^{'}}{n^{'}}$ the value of $D_m(y) = y_m$ will be obtained and comparing those values with the value of decryption table, the value of m will be obtained. Then replacing x_m by m from the array the numeric value of the plain text will be found. From the numeric value of alphabet, the plain text is written.

RESULTS

In this section justification of solvability is shown by the numerical value. Three modified solvability propositions based on solvability proposition will be described with example and a solvability series will be proposed.

Justification of solvability by numerical value:

To justify this proposition (Solvability) numerically, we will put the values of the integer a, n and b.

First, we will put such values of a, n and b in such a way that $gcd(a, n)$ does not divide b. Let, $a = 8, n = 6$ and $b = 5$. Then $gcd(a, n) = \text{gcd}(8, 6) = 2$ and $2 \nmid 5\ (= b)$. Then comparing with solvability equation, we can write $8x \equiv 5(mod\ 6)$.

Here, for any value of $x, 8x$ can be written as $2.4x$, which has a 2 as a factor. So, it is always an even number whereas 5 is an odd number. Then if we subtract an odd number from an even number it is always an odd number, does not contain 2 as a factor. So, $8x - 5$ is an odd integer. We have, $6 = 2.3$, which has an even factor 2 and is an even integer. An even integer never can divide an odd integer. Therefore, $6 \nmid 8x - 5$.

Hence, the equation $8x \equiv 5(mod\ 6)$ has no solution.

Again, we will put such values of a, n and b in a way that $gcd(a, n)$ divides b

Let, $= 8, n = 6\ and\ b = 4 = 2.2$. Then $gcd(a, n) = \text{gcd}(8, 6) = 2$ and $2|4\ (= b)$.

Then by the solvability equation, $8x \equiv 4(mod\ 6)$.

For the value of $x = 2$, we have, $8.2 \equiv 4(mod\ 6)$.

Then, $8.2 - 4 = 12$ and $6|12$.

Therefore, $8x \equiv 4(mod\ 6)$ has a solution for $x = 2$.

Hence, the equation $ax \equiv b(mod\ n)$ has a solution if and only if $gcd(a, n)$ divides b.

Proposition

Modified solvability-1

The equation $ax \equiv b(mod\ n)$ has infinitely many solutions for the infinite number of different positive integer values of x if $\text{gcd}(a, n)$ divides b and all the consecutive solution maintain a certain difference d.

Solvability Series

For the equation $ax \equiv b(mod\ n)$ by the *modified solvability-1* proposition, it has a set of solutions, if $gcd(a, n)$ divides b. Now, let $gcd(a, n)$ divides b. Then, putting $x = 1,2,3, \ldots$ we will find a solution for $x = k$, which we can say the first solution. Similarly, again putting $x = k + 1, k + 2, \ldots$ we will find out another solution which is $x = k + d$. In this way, we can obtain a series of solutions such as,

$$x = k, k + d, k + 2d, k + 3d, \ldots$$

For the convenience, we can call this series as solvability series. In general, the solvability series is,

$$x_m = k + (m - 1)d \qquad ;\text{where } m = 1,2, \ldots$$

Method of finding k, d and the general solvability series

Consider the equation $ax \equiv b(mod\ n)$, where $gcd(a, n)|b$.

Then let,

$$a' = \frac{\text{a}}{gcd(a, n)}, b' = \frac{b}{gcd(a, n)}\ and\ n' = \frac{n}{gcd(a, n)}$$

Then the difference of the any two consecutive solutions $d = n' = \frac{n}{gcd(a,n)}$

The solution equation for the equation $ax \equiv b(mod\ n)$, can be written as,

$$a^{'}k - b = yn^{'} \text{ ; where, x} = k$$
$$= \text{the first solution,}$$
$$\text{y}$$
$$= \text{integer value for which the first integer value of } k \text{ is found}$$

Then,

$$k = \frac{yn^{'} + b^{'}}{a^{'}}$$

Putting, $y = 1,2,3, \ldots$ the first integer value is taken as the value of k.

Then putting the value of k and d in the general solvability series we can found the general *solvability series* for the value of m,

$$x_m = k + (m - 1)d \quad \text{; where } m = 1,2, \ldots$$

Note: If, in any case $k > d$, then k is not the first solution of the *solvability series*. Then the first solution of solvability series is $k - d$ and the general solvability series is,

$$x_m = (k - d) + (m - 1)d \quad \text{; where } m = 1,2, \ldots$$

Illustration

Consider the equation $77x \equiv 33(mod\ 55)$.

Comparing the equation with the equation $ax \equiv b(mod\ n)$ we have, $a = 77$, $n = 55$ and $b = 33$.

Then, $gcd(a, n) = \text{gcd}(77, 55) = 11$ and $55 = 5.11$. So, $gcd(77, 55) = 11$ divides $b = 55$. Then by the modified solvability-I, $77x \equiv 33(mod\ 55)$ has infinitely many solutions.

Now,

$$a^{'} = \frac{77}{11} = 7, \qquad b^{'} = \frac{33}{11} = 3 \quad \text{and} \quad n^{'} = \frac{55}{11} = 5$$

Then the difference of the any two consecutive solutions $d = n^{'} = 5$.

And,

$$k = \frac{yn^{'} + b^{'}}{a^{'}}$$

$$= \frac{5y + 3}{7}.$$

Now, putting $y = 5$, we got the integer value of k,

$$k = \frac{5.5 + 3}{7}$$

$$= \frac{28}{7}$$

$$= 4$$

Now, putting the value of k and d in the general *solvability series*, we got,

$$x_m = 4 + (m - 1)5$$

For $m = 1, 2, \ldots, 6$, the above equation becomes,

$$x_{1,2,\ldots,6} = 4, 9, 14, 19, 24, 29.$$

Proposition
Modified Solvability-2:
The equation $ax \equiv b(mod\ n)$ has a solution for each and every positive integer values of x iff $gcd(a, n) = b$ and n is a factor of a, where x is any positive integer.

Illustration
Consider the equation $18x \equiv 6(mod\ 6)$.
Comparing the equation with the equation $ax \equiv b(mod\ n)$ we have, $a = 18$, $n = 6$ and $b = 6$.
Now, $gcd(a, n) = \text{gcd}(18,6) = 6$ and $b = 6$.
Then by *solvability-2*, $18x \equiv 6(mod\ 12)$ has a solution for each and every positive values of x.
Putting $x = 1,2,3, \ldots$ we have

$$18.1 - 6 = 12 \ \ and \ \frac{12}{6} = 2,$$

$$18.2 - 6 = 30 \ \ and \ \frac{30}{6} = 5$$

$$18.3 - 6 = 48 \ \ and \ \ \frac{48}{6} = 8$$

:Proposition
Modified Solvability-3:
If the equation $ax \equiv b(mod\ n)$ satisfies the modify *solvability-1* and the first solution is k, the consecutive difference of the two solutions is d and the last value of x is r, then the number of solution upto r is exactly $\left\lfloor \frac{r-k}{d} \right\rfloor + 1$, where '$\lfloor\ \rfloor$' is the floor function which converts a real number to the nearest integer less than or equal to that number.

Illustration
Consider the equation $77x \equiv 33(mod\ 55)$.
By solving this equation, we have

$$k = 4\ and\ d = 5$$

For $x = r = 30$, the number of solutions upto r is,

$$\left\lfloor \frac{r-k}{d} \right\rfloor + 1 = \left\lfloor \frac{30-4}{5} \right\rfloor + 1$$

$$= \lfloor 5.2 \rfloor + 1$$

$$= 5 + 1$$

$$= 6$$

From the solution series we have,

$$x_{1,2,\dots,6} = 4, 9, 14, 19, 24, 29.$$

Here, there are 6 solution upto $r = 30$.

Which, satisfies the modified *solvability-3.*

Cryptography Model

Using modified *solvability-1* and solvability series a new type of cryptographic model will be described here.

Cryptographic key

We will use a solvable equation as the key equation of our model.
Let, $77x \equiv 33(mod\ 55)$ be the key equation. Now solve equation to find out the encryption key and decryption key.
Comparing the equation with $ax \equiv b(mod\ n)$, $a = 77, n = 55$ and $b = 33$.
Then, $gcd(a, n) = \text{gcd}(77, 55) = 11$.
Hence,

$$a^{'} = \frac{77}{11} = 7, \qquad b^{'} = \frac{33}{11} = 3 \quad and \quad n^{'} = \frac{55}{11} = 5$$

Then the difference of the any two consecutive solutions $d = n^{'} = 5$.

Plain text
"HELLO WORLD"
Alphabetic position of each letter is given in the following alphabet-numerical table,

Letter	A	B	C	D	E	F	G	H	I	J	K	L	M
m	1	2	3	4	5	6	7	8	9	10	11	12	13
Letter	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
m	14	15	16	17	18	19	20	21	22	23	24	25	26

Tble-1: Alphabet-Numeric table

Here, $m = 1,2, \dots ,26$ represents the alphabets numerically.
Then the alphabetic number for "HELLO WORLD" is:
[8, 5, 12, 12, 15], [23, 15, 18, 12, 4]

Encryption

The encryption key $= E_m(x) = x_m$, where m is the alphabetic position of the letter.
The encryption equation can be written as,

$$k = \frac{yn^{\prime} + b^{\prime}}{a^{\prime}}$$

$$= \frac{5y + 3}{7}.$$

Now, putting $y = 5$, we got the integer value of k,

$$k = \frac{5.5 + 3}{7}$$

$$= \frac{28}{7}$$

$$= 4$$

The difference between two consecutive solutions is $d = n^{\prime} = 5$.
Here, $k < d$. So the first solution is $x_1 = k = 4$,
Now, putting the value of k and d in the general *solvability series*, we got,

$$x_m = 4 + (m - 1)5$$

Putting the value of $m = 1, 2, \dots, 26$ in the above equation the encryption table can be given as following,

m	1	2	3	4	5	6	7	8	9	10	11	12	13
$E_m(x)$	4	9	14	19	24	29	34	39	44	49	54	59	64
m	14	15	16	17	18	19	20	21	22	23	24	25	26
$E_m(x)$	69	74	79	84	89	94	99	104	109	114	119	124	129

Table-2: Encryption table

Then the numeric value $[8, 5, 12, 12, 15], [23, 15, 18, 12, 4]$ of the plain text "HELLO WORLD" can be coded into the cipher text as following:

$$[39, 24, 59, 59, 74], [114, 74, 89, 59, 19]$$

Decryption

The decryption key is $= D_m(y) = y_m$
The decryption equation can be written as

$$y = f = \frac{a^{\prime} x - b^{\prime}}{n^{\prime}}$$

$$f = \frac{7x - 3}{5}$$

For $x = 4$, we get the first integer value of y,

$$f = y_1 = \frac{7.4 - 3}{5}$$

$$= 5$$

For $x = 9$, we get the second integer value of y,

$$y_2 = \frac{7.9 - 3}{5}$$

$$= 12$$

So, the consecutive difference of two y value is,

$$\begin{aligned} d_y &= y_{n+1} - y_n \\ &= y_2 - y_1 \\ &= 12 - 5 \\ &= 7 \end{aligned}$$

Then the decryption table can be found by putting $m = 1,2, \ldots ,26$ in the following equation,

$$y_m = f + (m - 1)d_y$$

The decryption table is given as following,

m	1	2	3	4	5	6	7	8	9	10	11	12	13
$D_m(y)$	5	12	19	26	33	40	47	54	61	68	75	82	89
m	14	15	16	17	18	19	20	21	22	23	24	25	26
$D_m(y)$	96	103	110	117	124	131	138	145	152	159	166	173	180

Table-3: Decryption table

Now, the given encrypted cipher,

$$[39, 24, 59, 59, 74], [114, 74, 89, 59, 19]$$

Now putting all those values of x_m in the equation $y = \frac{7x-3}{5}$ we get,

$$y = \frac{7.39 - 3}{5} = \frac{273 - 3}{5} = 54,$$

$$y = \frac{7.24 - 3}{5} = \frac{168 - 3}{5} = 33,$$

$$y = \frac{7.59 - 3}{5} = \frac{413 - 3}{5} = 82,$$

$$y = \frac{7.59 - 3}{5} = \frac{413 - 3}{5} = 82,$$

$$y = \frac{7.74 - 3}{5} = \frac{518 - 3}{5} = 103,$$

$$y = \frac{7.114 - 3}{5} = \frac{798 - 3}{5} = 159,$$

$$y = \frac{7.74 - 3}{5} = \frac{518 - 3}{5} = 103,$$

$$y = \frac{7.89 - 3}{5} = \frac{623 - 3}{5} = 124,$$

$$y = \frac{7.59 - 3}{5} = \frac{413 - 3}{5} = 82,$$

$$y = \frac{7.19 - 3}{5} = \frac{133 - 3}{5} = 26,$$

Now comparing the values of y with the values from the decryption table, we will find the value of m i.e., the numerical value of position of an alphabet.
Hence the numerical value of the received cipher code is,

$$[8, 5, 12, 12, 15], [23, 15, 18, 12, 4]$$

Comparing with the alphabet-numerical value table we get the plain text,
“HELLO WORLD”

CONCLUSION AND FUTURE RESEARCH

Now-a-days in the computer and internet based world people’s first demand is the security of their private information. Cryptography is the modern security protocol to protect the information from the outsiders and to communicate securely without the involvement of third parties. In this research paper a short history of cryptography, cryptography related definitions and few theorems to illustrate different types of cryptographic models are described. This paper proposed few modified solvability proposition and introduced a general method of solvability series for a solvable equation. A new basic numerical model of cryptography is described based on solvability series and the organization of the model is illustrated with an example in this research paper.

Future Research

Future research on cryptography, extension of this research paper demands to find out a suitable cryptographic model based on a suitable equation and strong key, with the change of times. Use of prime factorization and matrices in cryptography got a great passion in cryptographic field. With the advance of modern times and advent of technology, to keep pace with the ever-changing world we always needed new type of technology. To meet the demand, further research will present more secured cryptographic model applicable to the real life.

References

[1] Damico, T. M. (2009) *A Brief History of Cryptography*, INQUIRES, 1(11), .

[2] C. Paar, C. and Pelzl J. (2010) Understanding Cryptography: A Textbook for Students and
Practitioners, Springer, Hedelberg Dordrecht London New York.

[3] Kahn, D. (1967) THE CODEBREAKERS: The Story of Secret Writing, SCRIBNER, Ney York.

[4] Bosworth, C. E. (1992) CODES- Encyclopaedia Iranica.
https://iranicaonline.org/articles/codes-romuz-sg

[5] Broemeling L. D. (2011) *An Account of Early Statistical Inference in Arab Cryptology*, The
American Statistician, 65(4), pp. 255-257.
DOI: https://doi.org/10.1198/tas.2011.10191

[6] B. Lennon (2018) Passwords: Philology, Security, Authentication, Harvard University Press,
Cambridge, pp. 21.

[7] Bruen A. A. and Forcinito M. A. (2004) CRYPTOGRAPHY, INFORMATION THEORY, AND
ERROR CORRECTION: A Handbook for the 21st Century, John Wiley & Sons Inc., New
Jerseypp. 21.

[8] Stein, W. (2017) Elementary Number Theory: Primes, Congruences and Secrets, Springer, New
York.

[9] Stinson, D. R. (2005) Cryptography: Theory and Practice Third Edition (Discrete Mathematics and
its Applications), Chapman and Hall/CRC, London.

[10] Qadir A. M. and Varol N. (2019) *A Review Paper on Cryptography*, In Proceedings of 2019th
International Symposium on Digital Forensics Security (ISDFS), IEEE, Barcelos, Portugal.
DOI: 10.1109/ISDFS.2019.8757514

[11] Aparajita and Rana, A. (2003) *Steneography- The Art of Hiding Information: A comparison from*
Cryptography, International Journal of Innovative Research in Science, Engineering and
Technology, 2(5), 1308-1312.

[12] Stallings, W. (2011) *Cryptography and Network Security Principles and Practice*, Pearson Education, Inc., New York.

[13] Singh, P. Shende, P. (2014) *Symmetric Key Cryptography: Current Trends*, International Journal of Computer Science and Information Technology, 3(12), 410-415.

[14] Kumar, S. N. (2015) *Review on Network Security and Cryptography*, International Transaction of Electrical and Computer Engineer's System, 3(1), 1-11.

[15] Paar, C. and Pelzl, J. (2010) *Understanding Cryptography*, Springer, Verlag Berlin, Heidelberg.

[16] Kumari, S. (2017) *A Research Paper on Cryptography Encryption and Compression Techniques*, International Journal of Engineering and Computer Science, 6(4), 20915-20919.

[17] Schneier, B. (1996) Applied Cryptography, Second Edition: Protocols, Algorithms, and Source Code in C (cloth), John Wiley & Sons, Inc., New Jersey.

[18] Gupta, R. K. (2020) *A Review Paper on Concepts of Cryptography and Cryptographic Hash Function*, European Journal of Molecular & Clinical Medicine, 7(7), 3397-3408.

[19] Kumari, S. (2017) *Cryptography Encryption and Compression Techniques*, International Journal of Engineering and Computer Science, 6(4), 20915-20919.
DOI: 10.18535/ijecs/v6i4.20

[20] http://all.net/edu/curr/ip/Chap2-4.html