Cryptography and Associated Aspects

Insha quadir
Pranveer singh institute of technology
Kanpur , India
Yash Tripathi
Pranveer singh institute of technology
Kanpur
Shreya jaiswal
Pranveer singh institute of technology
Kanpur
Yashika Singh
Pranveer singh institute of technology
Kanpur, India

----------ABSTRACT----------

In this fast transforming world finance and money is also transforming on a high note.Digitalized strength and other innovative systems and instruments are creating new platforms for financial traction who rectify and assume your transaction. Crypto is one such platform where transactions are secured and verified trustfully. Here in this paper, we will come to know how mathematics has enhanced the word of cryptography.In this paper we are going to study about role of mathematics in crypto text, encryption, symmetric key, stream, block cypher, asymmetric key and functions along with hash function,.Crypto key management andEfficient implementation. This paper provides a pure knowledge of application of mathematics in cryptography and how mathematics has enhanced in a truly different way.

INTRODUCTION

Cryptography is the particular way to convert a plain text into cypher text and to convert cypher text into plain text [1-9].

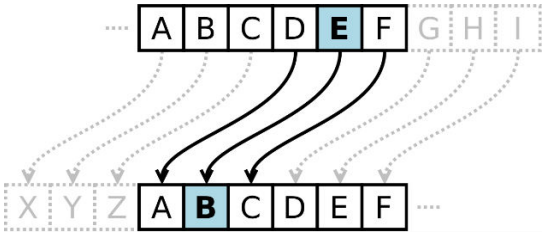
Plain text is a text or message which is present in the simple manner and can be read and understand by anyone easily that whatever is written but the cypher text is the text which is formed by some conversion and anyone can read but cannot understand .to understand it is necessary to change cypher text into plain text.

Basically, we use cryptography to achieve confidentiality. When we talk about network security that there is an important concept of CIAthat is confidentiality, integrity and availability.
Confidentiality is that no one can understand our message. In the network all the devices are connected and it is an unsecure medium of transfer of message and if someone has some knowledge of hacking so it can take our message in an unauthorized way but if itis send with the use of cryptography then it can take the message but cannot understand.
So in cryptography the sender first use the encryption method to change plain text into cypher text by using different algorithms.
As no one can read the message in the cypher text so receiver change the cypher text into plain text for reading and that process is called decryption.
So, the encryption is done by sender and decryption is done by receiver.
The encryption and decryption is done by using the keys.

Cryptography has its unique and extended history.
To describe cryptography in a short way it's Used to implement and safeguard national secrets and Strategies. Very first evolution of cryptography was about 4000 years ago where Egyptians used to transmit Messages written in hieroglyph.
The most salient evolution of cryptography came in the year 1976 when Diffie Hellman published his paper work "New Directions in Cryptography" this content changes radically the concept of cryptography by introducing the igneous method and concept of "Public Key Cryptography" for key exchange, the collateral of which is being based upon discrete logarithmic problem.

*Julius Caesar used the substitution cipher which approximately named *Caesar cipher* today.

*Alphabets are moved by a certain number.
*If the shift is 3 then A becomes D and so on.

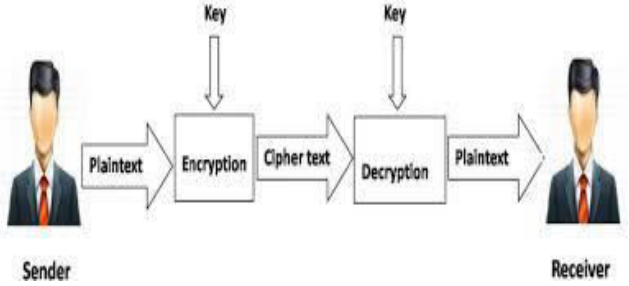


*This method was used by the Roman army to encrypt military and other official messages.
*The enigma machine is the most famous cryptographic cipher device used in ancient history.

*Encryption*is the process of encoding which converts the original representation of the information (plain text) into an unreadable text (cipher) by using an algorithm.

Symmetric key cryptography relies on a single key for encryption and decryption of information. The key needs to be secret and be available with both the sender and receiver.

Strength of algorithm is determined by the size of the key. The longer the key the more difficult it is to crack.
In symmetric key if N people in the world want to use the technique, then there needs to be N(N-1) people thus,each edge must have a unique key for communication.
Thus No. of keys required = No. of edges
Example. Encryption and decryption.



In symmetric key cryptography, there are basically two categories of ciphers that we can employ.

1. Stream ciphers
   These algorithms can encrypt basic information one bit/byte at a time.It is relatively quicks alternative considering the algorithm does not have to deal with blocks of data at a single time.
   Every piece of data that goes into the encryption can needs to be converted into binary format and in this cipher each binary digit is encrypted one after the other.Thebinary data is passed through an encryption key which is randomly generated bit stream upon passing through an encryption key which is randomly generated bit stream upon passing through we receive the ciphertext that can be transferred to the receiver without fear of man in the middle attack.

   BINARY DATA → ALGOTITHM FUNCTION → RANDOM ENCRYPTION KEY

   100101 f(x) 1101011

   DECIMAL/HEXADECIMAL → CIPHER ` TEXT → RECIEVER

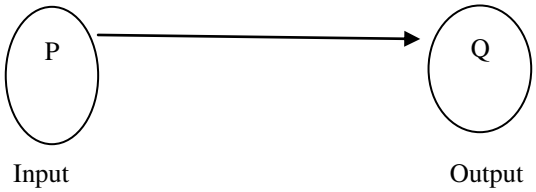
2. Block ciphers
   This dissect the raw information into the chunks of data of fixed size and the size of these blocks depends on the exact cipher being used like 128bit block cipher will break the plain text into →blocks of 128 bit each and encrypt those blocks instead of single digit. Once these blocks are encrypted individually,they are chained together to form a final cipher text.

   Each block Encryption key Encrypted block
   01001 + key 10101 → 10101+01010+00111 → 1010101000111
   01010 + key 00100 → 10101+01010+00111 → 1010101000111
   00111 →cipher text

*Asymmetric key cryptograph*y uses two different keys for encryption and decryption. The key used for encryption is the public key and the key used for decryption is the private key.

In this, public key can be shared via messaging or key serves and the sender encrypt the message using the receiver's public key after which we receive the ciphertext. The ciphertext transmitted to the receiver without any other key on getting the cipher text, the receiver uses his private key to decrypt it and get the plain text back and there is no requirement of any key exchange throughout this process therefore solving the most glaring flow faced in symmetric key algorithm.
For ex. Anyone who has your mailbox address can send you letters without any extra efforts needed from your end. However, nobody other than you can access the contents of the mailbox since only you have the key that can unlock it.
Example. Digital structures for maintaining authenticity of documents.
Background on functions:
Function in a set of p and q in which element p is properly assigned to element q by a rule 'f'.
Functions are also called "mapping" or "transformation".

P Q=f(p)



We can take a function in which we give the input and take output and there is rule f. if we have input in element p so the rule is transform into output that called f(p).
Norm signaling – f:A → B
Example– A={p,q,r}; B={1,2,3,4}
The rule of f forms A to B is:
f(p)=3 f(q)=1 f(r)=2
To show the form of mathematics:

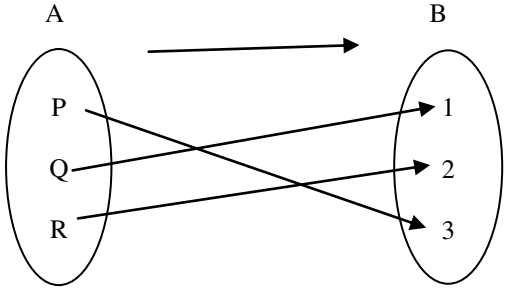


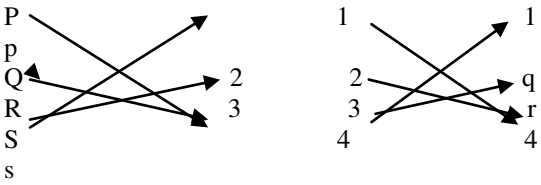
Image are A & B are is $I_m(f)=\{1,2,3\}$

a) 1-1(one-to-one) function:-

- If f(x)=2x+3 is 1-1. A=B=IR
- A transformation is 1-1 if each element in the codomain q is the image of at most one element in the domainp.

Eg-

F Q



- If f in a bijection form P to Q then it is a simple matter to define a bijection g from Q to P as shown in example.

b) One Way functions:

If we know what is twoways function then it will be easy to understand one way function.

A function in which we take input and give output or take output give input is called two ways function.

Example- y=2x+8;

Here y is output and x is input.

Y=32(output) | X=12(input)

One way function in which input is convert to output is easily but in reversing the direction is (output to input) is hard.

Example:

- Modular arithmetic:

37 mod 5 = 2 | 5=2?

7,12,17,-----

Easy | Hard

- Semi prime No:

19*13=242 | what are the factor of 377?

? | (13*29)

Easy | 3,541,789,831---------

Hard

c) Trapdoor one way function:-

It is similar to one way function in which some extra information is given by additional property.

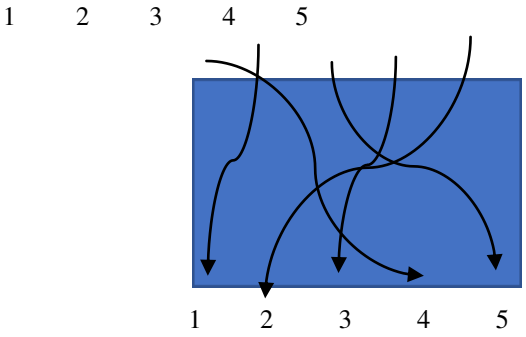
It is difficult but if we have some special information like one of prime no. is given and second one is to be found.

Diffie, Hellman and Markle published the trapdoor function, it become popular in cryptography.

The trapdoor function fulfills the requirements of the public key.

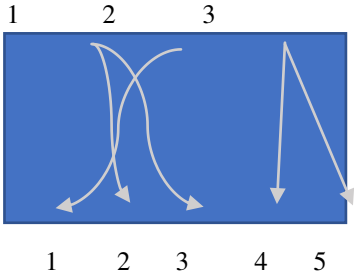
- Easy generation of public-private key pair.
- Encryption can be made even easier by using a public key.
- Decryption can be made even easier by using a private key.
- Infeasible to know P.T. from C.T. public key.

- *Permutation box(p-box)* :- This is a method to shift the bit from one place to another, meaning it changes the location of bits.
- *Block cypher*, they encrypt large plain text into smaller blocks.
- Permutation box is divided into three parts:
- *Straight permutation*---In straight bits, as many bits a as are in the input, the same number of bits will be in the output. Only their places will change.



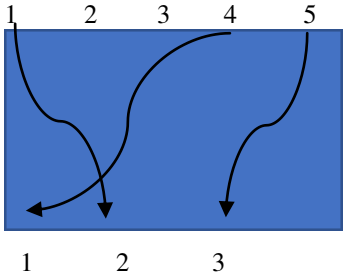
If input has 5 bits, then the output will also have 5 bits.

Expansion permutation: In expansion permutation,the input bits are smaller than the output bits.



- Number 0f bits in input < Number of bits in output.

Compression permutation: In compression permutation, the output bits are smaller than the input bits. We compress the bits in the compression permutations



Number of output bits < Number of input bits.
Generally Permutation boxes are keyless because they already have a definition of which key has to go where.
In this we move bits from one place to another to increase security. When we convert a plain text into a cipher text,It is a long process, in that we move bits from one place to another through the p-box, so that any hooker will have difficulty in decrypting the message.

APPLICATIONS OF NUMBER SYSTEM IN CRYPTOGRAPHY

The division of applied mathematics perturbed with developing schemes and formulas to enhance the privacy of communications with the use of codes is known as Cryptography. These codes are very useful for various wireless communication scenarios [10-15] and network security applications [16-20].

In order to ensure the integrity and conversation of data from tinker cryptology is used at its best.

In this modern era cryptology has also enhanced his methods hence in order to work more efficiently, cryptography systems rely on task of related with advanced mathematics which is termed as "NUBER SYSTEM" thar survey the belongings of some cryptologic systems, encryption is accomplished by prime numbers as the basis for further mathematical operations.

BINARY NUMBERS:

The numbers compute as sequence of zeroes and ones are known as Binary Numbers.

Types of Binary Numbers are:

Natural Binary System: -it reserves only positive numbers

Two's Complement System-it reserve both positive and negative values.

Notation of numbers in NBS:-

In NBS the stored binary digit is having positive values ranging from 0 to 2^n-1.

Definition:

Using natural binary system of the numbers the decimal value of a n digit number is stored as

$$a_{n-1} \dots a_2 a_1 a_0$$

is equal to:

$$2^{n-1}a_{n-1} + \dots + 2^2a_2 + 2^1a1 + 2^0a_0$$

where: ai may be equal to either 0 or 1.

Notation of fractions in NBS

A binary fixpoint numbers can be elaborated using natural binary system.

Definition:

Using the natural binary system of numberthe decimal value of a

(n+p)-digit binary number can be stored as

$$a_{n-1} \dots a_2 a_1 a_0, a_{-1} a_{-2} \dots a_{-m}$$

which is equal to:

$$2^{n-1}a_{n-1} + \dots + 2^2a_2 + 2^1a_1 + 2^0a_0 + 2^{-1}a_{-1} + 2^{-2}a_{-2} + \dots + 2^{-p}a_{-p}$$

where:

: n is a number of integer bits,

: p is a number of fractional bits,

: ai can be equal to either 0 or

Binary addition in NBS

In NBS binary addition of two numbers are presented as simple columnar addition:

	1	1	1	1		
		1	1	1	1	0
	1					
+		0	0	0	1	1
	0					
	1	0	0	0	0	1
	1					

Binary subtraction in NBS

In NBS binary subtraction of two numbers can be presented as simple columnar subtraction. subtraction can be done through exchangeable bits and in need can borrow bits from columns on the left. The borrowed numbers have always values one greater than the base of the system is, so in this case 10 (or 2 in the decimal notation; for convenience the example below uses the latter number).

For example, after subtracting 6 from 19 in NBS, we will have:

```
          1   2
    1     0   0   1   1
-                   1   1   0
          1   1   0   1
```

Binary multiplication in NBS:

Binary multiplication of two numbers in NBS may be presented in the same way as multiplication of decimal numbers. For example, the result of multiplication of 22 and 5 (equal to 110) can be calculated in the following way (all the numbers are written in NSB)

```
1   0   1   1   0
x   1   0   1
1   0   1   1   0
0   0   0   0   0
+1  0   1   1   0
1   1   0   1   1   1   0
```

Binary division in NBS

Using shifting and subtraction binary division of two numbers in NBS can be performed.

The numbers should be written in horizontal line, the dividend over the divisor.If the most significant non-zero bit is located at right under the most significant non-zero bit of the dividend the divisor should be moved left.

Then the dividend should be compared to the divisor. If the dividend is bigger than the divisor, one should subtract the divisor from the dividend and write 1 above the horizontal line in the last position then instead of the dividend we should use the result of subtraction.

No subtraction is performed if the divisor is bigger than the dividend.One should write 0 above the horizontal line in the last position, move the divisor to the right by one position and repeat the process of comparing.

Now we should write 0 above the horizontal line in last position if divisor can't move right.

For example, after dividing 11 by 3 the result will be 3 and the remainder 2:

```
              0   1   1
        1     0   1   1
        1     1
        1     0   1   1
-         1   1
              1   0   1
-                 1   1s
```

After obtaining the remainder, it is possible to continue dividing and receive fractional digits (as during dividing of decimal numbers).

CRYPTO KEY MANAGEMENT

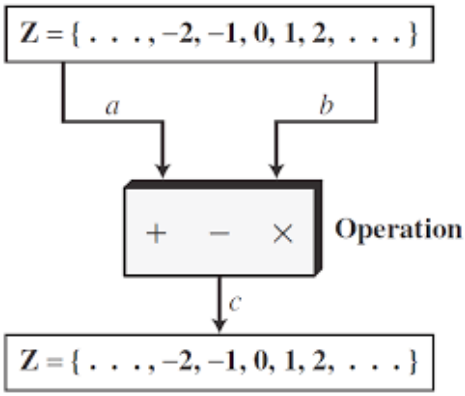
Key management is basically used to secure key generation, secure key storage and use key destruction.
Secure key generation adjust strength of the key:-

Key strength depends upon

: Randomness of key
:Key length
For example:- 7xEDgbj5eplwoXrLoacW23gOuUxt7r1x
This key is the example of 256bit random key we can use for AES 256 block cipher.
It takes almost millions of years to crack this key. Even Quantum computer was not able to crack this key in any of the practical way.
:- Now,one way to protect this key is to store in a Hardware Security Module

HSM strongly protects key and sanction safe storage and rectify of keys
2:- Another way is
Sensitive key management can be done by hardware encrypted USB key or a personal management application or a secret manager.
3:-Another popular method way to secure key is by TMPC(Trusted Platform Module)
Most of popular business computers today have installed TPM for storage and protection of keys.
Some more approaches to secure key are:
. Separation of duties
. Dual control
. Split knowledge

This are basically or we can say strictly used in securing encryption.
Like strong passwords key should be regularly rotated because doing this can help to encrypt overtime
It limits damage of key.

- Efficient implementation:
- Multiple precision integer arithmetic:It is the set of integers denoted by Z and all integers are from negative infinity
- to positive infinity without any fraction.
- Z={--------3,-2,-1,0,1,2,3--------}
- Binary operation: we are more interested in applying the basic operations to set of integers in cryptography .
- ∟Threebasic operations are addition subtraction and multiplication.In these operations we take two input &
- give one output.
- ∟ Both inputs come from the set of integers and output also goes into the set of integers.
- 

- Integer division: if we divide x and y in integer arithmetic , it will have a z and remainder r.
- X=z*y + r
- In this relation x is called dividend; z the quotient; y the divisor;r the remainder.
- Example:
- Assume that x=255 and y=11 we can find z=23 and r=2 using the division algorithm.
- 11)255(23
- 22
- ----------
- 35
- 33
- ---------
- 2
- For our purpose , we inflict the restrictions divisor must be positive and the remainder should be non
- negative .
- Divisibility: if x is non zero and let remainder =0 in the division relation we get:
- X=Z*y;

  So we can say that y divides x.so remainder will be zero and we can write the above relationship as x|y.
- Properties:
- If x|1 then x=+-1;
- If x|a and a|x then x=+-a;
- If x|a and a|b then x|b;

  If x|a and a|b then x|(m*a+n*b) where m and n are arbitrary integers.

Hash function converts different length strings into strings of fixed length which is commonly known as hash values. By the use of hash functions, the output values cannot be reversed to produce the original input.
Examples of hashing algorithms like MDS, SHA-1, HTML.
Examples of hash functions used in the real life also like in password verification. When we use user login website then we enter E-mail and password to confirm that account belongs to me.
Hashing function have advantages over the use of Normal encryption method are as follows:
a) If a hash function produces hash values y, then it will be difficult for anyone to find any input value w that hashes to y and because of to this property it becomes difficult for attacker to find the input if they have hash value.
b)Similarly, if a hash function h for any input y produces hash value h(y) then, it will be difficult to find any value w which will be h(y) = h(w). This all produces the message encryption method.
There are many ways for hashing function encryption:

1.In this method we will achieve both authentication and confidentiality. If the starting hash function will match with the ending hash function, then it shows that our messages are authenticate and the generated (cipher + hash code) message cannot be separated easily it shows the confidentiality.

2.Here, only authentication will be achieved and processing time will be less. This method is useful when there will be no loss if the given information will become public.
Example: If teacher says at 2 pm we will have extra class, there is no loss of anyone if the information given by teacher will be public.

One of the best uses of hashing function is *Digital signatures.*

With the digital signatures, a long message will be hashed and the hash value will be signed and the receiver will hash the received message and verifies that the received signature is correct for this hash value or not.
The signature must use some information unique to the sender to prevent forgery and contradiction.

3.Confidential means a packet which is not meant for everyone and only selected people can see them. So the content or message should be read by only sender and receiver, that means the whole message or content is kept secret from everyone, only two of them knows about it.

Note:
M – Message
H – Hash Function
K_s – A random Session Key created for Symmetric Encryption purpose
DP – Public-Key Decryption Algorithm
EP – Public-Key Encryption Algorithm
DC – Asymmetric Encryption Algorithm
EC – Symmetric Encryption Algorithm
KP_b – A private key of user B used in Public-key encryption process
KP_a – A private key of user A used in Public-key encryption process
PU_a – A public key of user A used in Public-key encryption process
PU_b – A public key of user B used in Public-key encryption process
|| – Concatenation
Z – Compression Function
Z^{-1} – Decompression Function

CONCLUSION:

Cryptocurrency is the most advanced topic in the global financial and transaction system. There is a great excitedness of crypto exchange rates. Crypto has gained huge trust as a result of which they are used on a wide scale. Even some nations have started to issue national cryptocurrency.
Mathematics has enhanced crypto in such a way that crypto is also called as “mathematical money”. Crypto are built only by using of complex mathematics and computational methods. Modern crypto also has an essence of matrices, number theory and many more mathematical applications.

From this research we can conclude that mathematics has entitled the world of crypto on the another level.

REFERENCES

[1].V. Shukla, A. Chaturvedi, N. Srivastava, Nanotechnology and cryptographic protocols: issues and possible solutions, Nanomaterials and energy, volume 8, issue 1, 2019, 1-6,
DOI: 10.1680/jnaen.18.00006

[2]. M.K. Misra, A. Chaturvedi, S.P. Tripathi, V. Shukla, A unique key sharing protocol among three users using non-commutative group for electronic health record system, Journal of discrete mathematical sciences and cryptography, volume 22, issue 8, 2019, 1435–1451,
DOI: 10.1080/09720529.2019.1692450

[3]. A.Chaturvedi, N.Srivastava, V.Shukla, A secure wireless communication protocol using Diffie-Hellman key exchange, International journal of computer applications, volume 126, number 5, 2015, 35-38,
DOI: 10.5120/ijca2015906060

[4]. V. Shukla, A. Chaturvedi, M.K. Misra, On authentication schemes using polynomials over non commutative rings, Wireless personal communications, volume 118, issue 1, 2021, 1-9,
DOI: https://doi.org/10.1007/s11277-020-08008-4

[5]. V. Shukla, A. Mishra, S. Agarwal, A new one time password generation method for financial transactions with randomness analysis, Innovations in electrical and electronic engineering (Part of the lecture notes in electrical engineering book series (LNEE, volume 661)), 2020, 713-720,
DOI: https://doi.org/10.1007/978-981-15-4692-1_54

[6]. V. Shukla, A. Mishra, A. Yadav, An authenticated and secure electronic health record system, IEEE international conference on information and communication technology, 2019, 1-5,
DOI: 10.1109/CICT48419.2019.9066168

[7]. A. Chaturvedi, V. Shukla, M.K. Misra, Three party key sharing protocol using polynomial rings, 5th IEEE Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering (UPCON), 2018, 1-5,
DOI: 10.1109/UPCON.2018.8596905

[8]. V. Shukla, A. Chaturvedi, N. Srivastava, Secure wireless communication protocol: to avoid vulnerabilities in shared authentication, Communications on applied electronics, volume 7, number 6, 2017, 4-7,
DOI: 10.5120/cae2017652680

[9]. V. Shukla, M.K. Misra, A. Chaturvedi, Journey of cryptocurrency in India in view of financial budget 2022-23, Cornell university arxiv, 2022, 1-6,
DOI: https://doi.org/10.48550/arXiv.2203.12606

[10]. V. Shukla, N. Srivastava, A. Chaturvedi, A bit commitment signcryption protocol for wireless transport layer security (wtls), IEEE international conference on electrical, computer and electronics engineering , 2016, 83-86,
DOI: 10.1109/UPCON.2016.7894629

[11]. V.Shukla, A.Chaturvedi, N.Srivastava, A new secure authenticated key agreement scheme for wireless (mobile) communication in an EHR system using cryptography, Communications on applied electronics, volume 3, number 3, 2015, 16-21,
DOI: 10.5120/cae2015651903

[12]. A. Chaturvedi, N. Srivastava, V. Shukla, S.P. Tripathi, M.K. Misra, A secure zero knowledge authentication protocol for wireless (mobile) ad-hoc networks, International journal of computer applications, volume 128, number 2, 2015, 36-39,
DOI: 10.5120/ijca2015906437

[13]. V. Shukla, A. Chaturvedi, N. Srivastava, Authentication aspects of dynamic routing protocols: associated problem & proposed solution, International journal of recent technology and engineering, volume 8, issue 2, 2019, 412-419,
DOI: 10.35940/ijrte.B1503.078219

[14]. V. Shukla, A. Kushwaha, S.S. Parihar, S. Srivastava, V. P. Singh, Authenticated wireless information display system using GSM module, Communications on applied electronics, volume 5, number 3, 2016, 7-11,
DOI: 10.5120/cae2016652251

[15]. V. Shukla, A. Chaturvedi, N. Srivastava, Double layer cryptographic protocol for mobile ad-hoc networks (MANETs) by commitment scheme, Communications on applied electronics, volume 7, number 9, 2017, 32-36,
DOI: 10.5120/cae2017652716

[16]. V. Shukla, A. Chaturvedi, N. Srivastava, A secure stop and wait communication protocol for disturbed networks, Wireless personal communications, volume 110, 861-872, 2019,
DOI: https://doi.org/10.1007/s11277-019-06760-w

[17]. V. Shukla, A.Mishra, A new sequential coding method for secure data communication, IEEE international conference on computing, power and communication technologies, 2020, 529-533,
DOI: 10.1109/GUCON48875.2020.9231252

[18]. A. Chaturvedi, V. Shukla, M.K. Misra, A random encoding method for secure data communication: an extension of sequential coding, Journal of discrete mathematical sciences and cryptography, volume 24, issue 5, 2021, 1189-1204,
DOI: https://doi.org/10.1080/09720529.2021.1932902

[19]. V. Shukla, A. Chaturvedi, N. Srivastava, A new one time password mechanism for client-server applications, Journal of discrete mathematical sciences and cryptography, volume 22, 2019, 1393-1406,
DOI: 10.1080/09720529.2019.1692447

[20]. V. Shukla, M.K. Misra, A. Chaturvedi, A new authentication procedure for client-server applications using HMAC, Journal of discrete mathematical sciences and cryptography, volume 24, issue 5, 2021, 1241-1256,
DOI: https://doi.org/10.1080/09720529.2021.1932908