Enhanced Security of Encrypted Text by KDMT: Key-Domain Maximization Technique

Nitin Uniyal, Girish Dobhal, Pradeep Semwal

Abstract: ***Encryption-decryption techniques have been the backbone of network security in the modern era of wireless transmission of data. We present here a more secured encryption-decryption method based on the maximization of key domain in finite field. The proposed technique uses a random primary key to fetch the encryption-decryption key-pair furnished by a unique decomposition. A secondary key taken from a subdomain with specific property is used to add more randomness in the encrypted text structure. A probabilistic comparison of key prediction by hacker is also discussed to justify the added security in the proposed method.***

Keywords: decryption, encryption, isomorphism, permutation.

I. INTRODUCTION

Cryptography is the art of disguising a message mathematically so that the authorized recipient can understand it. It involves two major steps in the process. The first procedure is to disguise the plain text which is known as encryption and the encrypted message is known as cryptogram or cipher text. The authorized recipient knows the inverse process involved so that the cryptogram can be retrieved back to the original message. This is called decryption. Therefore cryptosystem can be considered as five tuple $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ where $\mathcal{P}$ is a finite set of possible plain texts, $\mathcal{C}$ is finite set of possible cypher texts, $\mathcal{K}$ is finite set of possible keys. For each $K \in \mathcal{K}$ there is an encryption rule $E \in \mathcal{E}$ and the corresponding decryption rule $D \in \mathcal{D}$ such that $E: \mathcal{P} \longrightarrow \mathcal{C}$, $D: \mathcal{C} \longrightarrow \mathcal{P}$ are functions such that $D\big(E(x)\big) = x$ for every plaintext element $x \in \mathcal{P}$ [1].

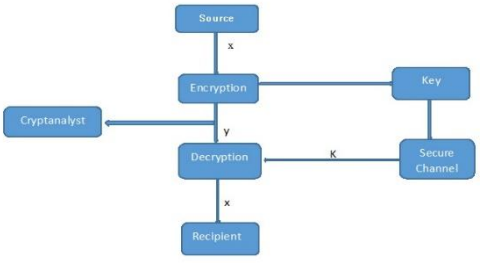

Figure1: Model of conventional cryptosystem

The method of encryption and decryption of the message was there from ancient periods. Encrypted messages were used mostly during the war. In modern era due to digitalization it is necessary to ensure that the information sent through various channels is secured and is difficult to decrypt. Cryptography is derived from the Greek word *Krypto* meaning 'hidden'. Historical evidence of cryptography dates back to 2000 BC, with Egyptian practice of hieroglyphics which consist of pictograms. In ancient India we come across Katapayadi system, *Vararuci* in his book *Chandravakyani* composed the hymns which on interpretation gives the longitudes of Moon at different time interval. *Laghu bhāskarīyavivaraṇa* by *Shankara Narayana* in 869 *CE* and *Grahacāraṇibandhana* by *Haridatta* in 683 *CE* are also the evidences of Katapayadi system. In this system, number 1 is allocated to the letters $Ka\ Ta\ Pa$ and Ya. In this method numerals from 0 to 9 are used. Therefore more than one letter is allocated to a single numeral [2]. The rule was:

ka (क), ṭa (ट), pa (प) and *ya (य)* denote *1*
kha (ख), ṭha (ठ), pha (फ), and *ra (र)* indicate *2*
ga (ग), ḍa (ड), ba (ब) and *la (ल)* stand for *3*
gha (घ), ḍha (ढ), bha (भ) and *va (व)* symbolize *4*
gna (ङ), ṇa (ण), ma (म), and *śha (श)* represent *5*
ca (च), ta (त), and *sha (ष)* stand for *6*
cha (छ), tha (थ), and *sa (स)* means *7*
ja (ज), da (द), and *ha (ह)* stand for *8*
jha (झ) and *dha (ध)* characterize *9*
nya (ञ), na (न) and all vowels means *0*

Figure 2:Rule for Katapayadi system

In west, Julius Caesar around 100 BC created a system in which each character in his message was replaced by a character three position ahead of it in the Roman alphabet. Since then due to advancement of technology various complex methods have developed, during World War I rotor cipher machines were invented and in World War II computers played an important role. The foremost striking development within the history of cryptography came in 1976 when Diffie and Hellman [3] published new directions in cryptography that introduced the revolutionary idea of public- key cryptography. Modern cryptography techniques have become complex and difficult to break as it is based on mathematical theory and computer science. Encryption technology gained importance not only to ensure secure in communications, such as warfare, spies, national security but also in public domain such as in use of ATM, Credit Card, Smart Cards, electronic home systems, RFID tags etc.

Revised Manuscript Received on January 15, 2020
***** Correspondence Author
***Dr. NITIN UNIYAL,** Department of Mathematics, UPES, Dehradun, India. Email: nuniyal@ddn.upes.ac.in
Dr. GIRISH DOBHAL, Department of Mathematics, UPES, Dehradun, India. Email: gdobhal@ddn.upes.ac.in
Mr. PRADEEP SEMWAL, School of Computer Application and Information Technology, SGRR University, Dehradun, India. Email: psemwal22@yahoo.com

Thus, the field of cryptography now deals with the problem of message authentication, digital signatures, protocols for exchanging secret keys, authentication protocols, electronics auctions, digital cash and many more. Modern cryptography can be considered as scientific study of techniques for securing transactions, digital information and distributed computations.

II. TYPES OF CIPHERS

Ciphers can be broadly classified using the following figure.

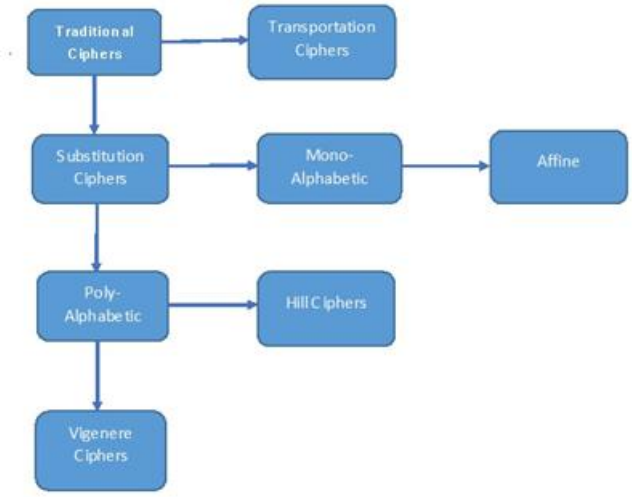

Figure 3:Classification of ciphers

A. Transportation Cipher

In a transposition cipher the plaintext remains the same, but the order of characters is shuffled around. Julius Caesar encrypted by rotating the letters of the alphabet by 3 places. For example, consider the message *Begin the attack now*, with spaces removed would be encrypted as:

EHJLQWKHDWWDFNQRZ

B. Substitution Cipher

In a substitution cipher each character in the plaintext is substituted for another character in the cipher text. The receiver inverts the substitution on the cipher text to recover the plaintext. There are other cases in which each character of the plaintext is replaced with a corresponding character of cipher text, a single character of plaintext can map to one of several characters of cipher text, blocks of characters are encrypted in groups. In general, we have $\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26}$. $\mathcal{K}$ contains all possible permutations of the 26 symbols 0,1,2, ….25 such that for each permutation $\pi \in \mathcal{K}$, define

$$E_\pi(x) = \pi(x) \text{ and } D_\pi(y) = \pi^{-1}(y)$$

where π^{-1} is the inverse permutation of π.

C. Shift Cipher

In the shift cipher, the key K is a number between 0 and 25. For encryption, letters are rotated by K places.

$$\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_{26}.$$

For $0 \le K \le 25$, define

$$E_K(x) = (x + K) mod 26$$
$$D_K(y) = (y - K) mod 26, \quad x, y \in \mathbb{Z}_{26}.$$

If $K = 3$ then it is called Ceaser cipher.

D. Affine Cipher

The Affine cipher is a mono alphabetic substitution cipher in which each letter of an alphabet is mapped to its numeric equivalent. Encryption is performed using a simple mathematical function and is converted back to a letter. The process works on modulo m . Let $\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26}$. $\mathcal{K} = \{(a, b) \in \mathbb{Z}_{26} \times \mathbb{Z}_{26} : \gcd(a, 26) = 1\}$

For $K = (a, b) \in \mathcal{K}$, define

$$E_K(x) = (ax + b) mod 26$$
$$D_K(y) = a^{-1}(y - b) mod 26$$

E. Vigenere Cipher

One of the classic cryptographic algorithms is Vigenere cipher which is included in the category of polyalphabetic substitution and symmetric key cryptographic algorithm. Here, the same key is used for encryption and decryption. Vigenere cipher uses a 26×26 matrix containing alphabets called tabula recta [4].

Let $\mathcal{P} = \mathcal{C} = \mathcal{K} = (\mathbb{Z}_{26})^m$, m being a positive integer. For key $K = (k_1, k_2, \ldots . k_m)$ we have

$$E_k(x_1, x_2 \ldots . x_m) = (x_1 + k_1, x_2 + k_2, \ldots \ldots x_m + k_m)$$
$$D_k(y_1, y_2 \ldots . y_m) = (y_1 - k_1, y_2 - k_2, \ldots \ldots y_m - k_m)$$

where all operations are performed in $\mathbb{Z}_{26}$.

	(Plaintext Letter)																									
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Figure 4: Vignere cipher table

F. Hill Cipher

In Hill ciphers, m successive plaintext letters are substituted by m cipher text letters. The substitution is determined by m, where m is a positive integer therefore we take m linear combinations of the m alphabetic characters in one plaintext element and produce m alphabetic characters in one cipher text element. Hence $m \times m$ $(m \ge 2)$ invertible matrix K is used as a key of the system. Let $\mathcal{P} = \mathcal{C} = (\mathbb{Z}_{26})^m$ and $\mathcal{K} = \{m \times m$ invertible matrices over $\mathbb{Z}_{26}\}$.

For a key K, we have $E_K(x) = xK$, $D_K(y) = yK^{-1}$; all operations are performed in $\mathbb{Z}_{26}$.

III. PROPOSED METHOD: KEY DOMAIN MAXIMIZATION TECHNIQUE (KDMT)

We propose a method in which the plaintext matrix is encrypted to cipher matrix using random key matrices. The crux of the method lies in the simplicity of encryption-decryption key pair in sets $\mathcal{E}$ and $\mathcal{D}$ without much bothering about their existence in either set. The idea is not to restrict the randomness of keys and spend too much efforts in their selection as they are somewhat like temporary co-passengers in the journey of a plaintext. This sort of randomness is also of great significance from the viewpoint of the security of plaintext as it reduces the probability of key-prediction by a hacker. The reason being the added freeness to the existence of key in a mathematical structure. Let us take the keys in form of real matrices $K, \sigma \in M_n(\mathbb{Z}_{37})$, the space of all $n \times n$ matrices with entries belonging to the finite field $\mathbb{Z}_{37}$. Moreover, $M_n(\mathbb{Z}_{37})$ is a vector space in its own regard where the underlying field $\mathbb{Z}_{37}$ provides a sort of randomness to its elements. A random member $K \in M_n(\mathbb{Z}_{37})$ can serve well as the first key shared between the sender and receiver. We call K, the primary key and σ the secondary as the latter works on the output given by the former. Further the domain of σ is somewhat squeezed in topological sense due to its unique property of shuffling the raw encrypted text.

We here first show that $K \in M_n(\mathbb{Z}_{37})$ can be uniquely decomposed as sum of symmetric and skew-symmetric matrix in the following way:

$$K = 19(K + K^{'}) + [18(K + K^{'}) + K]$$

$K^{'}$ being the transposed matrix K.

Since $19(K + K^{'}) + [18(K + K^{'}) + K] = 38K + 37K^{'} = K$where the operations have been performed in the field $\mathbb{Z}_{37}$. Also, it is easy to verify the symmetric and skew-symmetric nature of matrices $19(K + K^{'})$ and $18(K + K^{'}) + K$ respectively. Furthermore, using little algebra of matrices one can deduce that the addition of factor $19(K + K^{'})$ at the sender's end compels the addition of factor $18(K + K^{'})$ at the receiver's end.

Suppose T and T_C respectively denote the plaintext and cipher text matrices. The proposed equations for encryption are:

$$T_C = f(T^{**}) \quad (1)$$

$$T^{**} = \sigma\,[T + 19(K + K^{'})]\sigma. \quad (2)$$

For decryption, we use

$$T^{**} = f^{-1}(T_C) \quad (3)$$

$$T = \sigma^{-1}T^{**}\sigma^{-1} + 18(K + K^{'}). \quad (4)$$

Here $f: \mathbb{Z}_{37} \longrightarrow F$ is an isomorphism from $\mathbb{Z}_{37}$ onto some specifically chosen field F of 37 distinct arbitrary symbols; and σ serving as the second key shared between the sender and receiver. We choose $\sigma \in M_n(\mathbb{Z}_{37})$ named as *permutation matrix* containing exactly one unity in every row and every column, while the other entries being zero.

A. Encryption-Decryption Algorithm

The encryption-decryption algorithm for the proposed method is exhibited as follows.

Encryption Algorithm:

1. Input text matrix T, key matrices K and σ; and an isomorphism $f: \mathbb{Z}_{37} \longrightarrow F$ for some chosen F.
2. Compute $T + 19(K + K^{'}) = T^{*}$.
3. Compute $\sigma T^{*}\sigma = T^{**}$.
4. Compute $T_C = f(T^{**})$ as cipher text matrix.

Decryption Algorithm:

1. Input encrypted matrix T_C, key matrices K and σ; and inverse isomorphism $f^{-1}: F \longrightarrow \mathbb{Z}_{37}$.
2. Compute $f^{-1}(T_C) = T^{**}$.
3. Compute $T^{*} = \sigma^{-1}T^{**}\sigma^{-1}$.
4. Retrieve $T = T^{*} + 18(K + K^{'})$ as text matrix.

B. Illustration of KDMT

For instance, consider the text *OH MY GOD*. Over the finite field $\mathbb{Z}_{37} = \{0,1,2, \ldots 36\}$ w.r.t. mod 37, where the first 26 elements represent alphabets in the order, next 10 elements represent ten digits from 0 to 9 and the last element represents the space respectively; the plaintext matrix achieved by arranging the text row wise as

$$T = \begin{pmatrix} 14 & 7 & 36 \\ 12 & 24 & 36 \\ 6 & 14 & 3 \end{pmatrix} \in M_3(\mathbb{Z}_{37})$$

Suppose $K = \begin{pmatrix} 10 & 2 & 11 \\ 12 & 24 & 0 \\ 5 & 9 & 34 \end{pmatrix}$ and $\sigma = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ are the keys shared at both ends. Then

$$T + 19(K + K^{'}) = \begin{pmatrix} 24 & 14 & 7 \\ 19 & 11 & 22 \\ 14 & 0 & 0 \end{pmatrix}$$

Then (2) gives

$$T^{**} = \begin{pmatrix} 11 & 19 & 22 \\ 14 & 24 & 7 \\ 0 & 14 & 0 \end{pmatrix}$$

For some specifically chosen finite field F, define a one-one correspondence map $f: \mathbb{Z}_{37} \longrightarrow F$ to get encrypted matrix

$$T_C = \begin{pmatrix} @ & \# & \$ \\ \% & \wedge & \& \\ \_ & (& \_ \end{pmatrix} (say).$$

The decryption process can be followed using the inverse map $f^{-1}(T_C) = T^{**}$ and

$$18(K + K^{'}) = \begin{pmatrix} 27 & 30 & 29 \\ 30 & 13 & 14 \\ 29 & 14 & 3 \end{pmatrix}.$$

Using (4) gives back the text matrix $T = \begin{pmatrix} 14 & 7 & 36 \\ 12 & 24 & 36 \\ 6 & 14 & 3 \end{pmatrix}$, which on decryption retrieves the text *OH MY GOD*.

IV. RESULT AND DISCUSSION

The merit of the proposed method lies in the freedom of arbitrary selection of primary key $K \neq O$ (Null matrix) as the state of degeneracy of the proposed decomposition is completely removed due to the existence of the factors $19(K + K^{'})$ and $18(K + K^{'})$ for any choice of K in $M_n(\mathbb{Z}_{37})$. The firmness is supplied by the transpose operation which is well-defined for each member of the vector space. Besides this, the choice of the secondary key $\sigma \neq I$ (Identity matrix) ensures the existence of its multiplicative inverse $\sigma^{-1} \in M_n(\mathbb{Z}_{37})$.

The reason might well be understood by observing $\det(\sigma) = \pm 1$ or equivalently, by looking at its form which is nothing but indeed a derangement of columns of the identity matrix I. Furthermore, the handling of σ for computing the products $\sigma T^{*}\sigma$ and $\sigma^{-1}T^{**}\sigma^{-1}$ is far simpler than any other member of vector space. Precisely speaking, the operation $\sigma T^{*}\sigma$ is something like shuffling symmetrically row-wise and column-wise on an n −dimensional Rubik's cube.

Let us show HOW (?) the probability of key prediction by some hacker is drastically reduced by maximizing the sample space $M_n(\mathbb{Z}_{37})$. Particularly for $n = 3$, the probability $P(predicting\ K) = \frac{1}{37^9}$ which is much lesser than the number $\frac{1}{(37^3-1)(37^3-37)(37^3-37^2)}$ i.e. the probability of prediction of K in the case of LU decomposition used earlier by other researchers; the denominator $(37^3 - 1373 - 37373 - 372$ being the number of invertible matrices in $M_3(\mathbb{Z}_{37})$.

Further, for a hacker merely predicting key K correctly will not work as the second key σ comes from a multiplicative subgroup S_3 of 3! permutation matrices in $M_n(\mathbb{Z}_{37})$, so the probability $P(predicting\ \sigma) = \frac{1}{(3!)^2}$. Since the events of prediction of two keys are mutually exclusive hence $P(predicting\ K\ and\ \sigma) = \frac{1}{37^9}.\frac{1}{(3!)^2}$ which is much lesser than expected. For sufficiently large n, this probability approaches close to zero.

Here it is worthwhile to mention the effortless computation of σ^{-1} as follows: For the choice of secondary key matrix $\sigma = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, a very familiar and compact two-liner representation is $\pi = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ called permutation; where each entry in the second row indicates the position of unity in the column of σ from left to right. Observe that the inverse permutation can be obtained by exchanging the rows of π i.e. $\pi^{-1} = \begin{pmatrix} 2 & 1 & 3 \\ 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ which gives inverse matrix $\sigma^{-1} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$.

V. CONCLUSION

Unlike other methods relying on LU −decomposition of the key matrix $K = LU$, where K is majorly restricted to be non-singular and must contain non-zero entry at the first position, the decomposition used in the proposed method is unrestricted in this sense. The reason being the broadening of the key domain to $M_n(\mathbb{Z}_{37})$ rather than $GL_n(\mathbb{Z}_{37})$ (*General linear group of invertible matrices*). Apart from the freeness in key selection it also adds security by reducing the probability of prediction of K by a hacker due to the maximized sample space size for the choice of K.

In nutshell, the proposed method serves better in the probabilistic comparison of data security and also in sense of the complicacy of key sharing. Nonetheless, there is always an open scope of improvement in the proposed method for further research.

REFERENCES

1. D. R. Stinson, *Cryptography theory and Practice*, Taylor and Francis, 2006.
2. J. F. Sweeney, "Rig Veda Magic Squares" unpublished.
3. W. Diffie and M. Hellman, "New Directions in Cryptography", *IEEE Transaction on Information Theory*, Vol. IT-22, no. 6, 1976.
4. A. Subandi, R. Meiyanti, C.L.M. Sandy, R.W. Sembiring, "Three-Pass Protocol Implementation in Vigenere Cipher Classic Cryptography Algorithm with Keystream Generator Modification", *Advances in Science, Technology and Engineering Systems Journal*, Vol. 2, No. 5, 1-5 (2017).
5. N.F. Johnson, " Exploring Steganography: Seeing The Unseen" *IEEE Computer*, Vol. 31, No. 2, 1998.
6. C. Shannon, , "A mathematical theory of communication" *Bell Syst. Tech. J.*, Vol.27, pp. 379-423, 1948.
7. M. Bellare and P.Rogaway, Introduction to Modern Cryptography: Lecture Notes (2003), available at http://www.cs.ucsd.edu/users/mihir/cse207/classnotes.html.
8. H. G. Liddell, George, H., Scoot, Robert, Jones, Stuart, J. H., McKenzie, RoderickA.: "Greek-English Lexicon", Oxford University Press,1984
9. R. L. Rivest, Cryptography Algorithms and Complexity, *Elsevier*, 717-755, 1990.

AUTHORS PROFILE

Dr. NITIN UNIYAL is working as Assistant Professor in the Department of Mathematics, UPES, Dehradun (India). He obtained his Ph.D. in Differential Geometry from HNB Central University in 2012 and has 16 publications in journals of International repute. He has more than 12 years of teaching and research experience. His broad are of research are Differential Geometry, Nature based Optimization and cryptography. He is an active member of IAENG and The Indian Science Congress, Kolkata.

Dr. GIRISH DOBHAL is working as Assistant Professor in the Department of Mathematics, UPES, Dehradun, India. He obtained his Ph.D. in Differential Geometry from HNB Central University in 2010 and has 22 publications in journals of International repute. He has more than 12 years of teaching and research experience.

Mr. PRADEEP SEMWAL is working as Associate Professor in the School of Computer Application and Information Technology, SGRR University, Dehradun (India). He is pursuing Ph.D. on Network and Network Security and is having a total 14 years of teaching and research experience.