ISSN (e): 2250 – 3005 || Volume, 15 || Issue, 1|| January. –2025 ||
International Journal of Computational Engineering Research (IJCER)

Exploring the Role of Linear Algebra in Cryptography: Techniques, Applications, and Examples

Dilruba Akter
Department of Applied Mathematics,
GonoBishwabidyalay, Savar, Dhaka, Bangladesh

ABSTRACT
Linear algebra is a main important part of the mathematics. Its value lies in its many applications, from mathematical physics to modern algebra and its usage in the engineering and medical fields such as image processing and analysis. Cryptography is one of the most important applications of linear algebra and number theory where the process is to change important information to another unclear one. The main goal of cryptography is to keep the integrity and security of this information. There are many types of cryptography techniques and we will try to consider one of them in this paper.
KEYWORDS:*Linear algebra; addition; scalar; multiplication; linear equations; matrices; determinants, Cipher, plain text, cipher text.*

Date of Submission: 02-01-2025 Date of acceptance: 13-01-2025

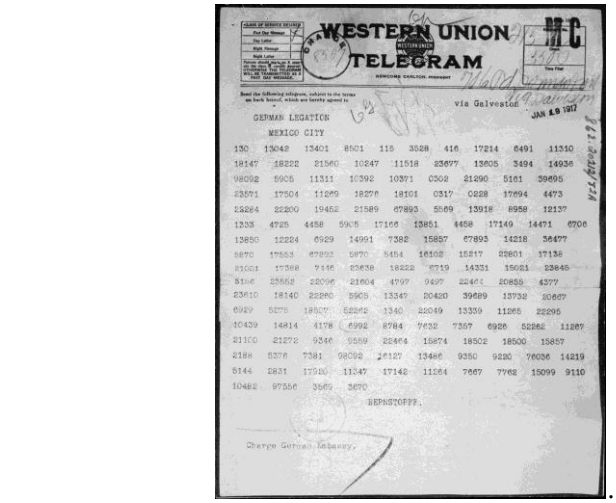
I. INTRODUCTION

Nowadays the application of linear algebra is widespread in engineering.The most popular ones include network security, engineering economics, chemical equation balancing, and network solving. These days, with the progress of technology, we prefer to converse over networks. Applications that need the transmission and reception of data without vulnerability to hacking include text messaging, voice notes, and online banking. Retrieving the information being sent between the sender and the recipient is the aim of hacking. Messages are encrypted or encoded using various encoding algorithms to prevent hackers. Cryptography is among them.. Two ways are available to maintain information confidentiality: concealing its existence or rendering it incomprehensible. Cryptography is the art and science of encrypting data to protect it from unauthorized access. On the other hand, decrypting data through cryptanalysis is both an art and a science. Cryptology is the area of mathematics which includes both cryptography and cryptanalysis. Sophisticated mathematical formulas, or algorithms, and private keys are used in modern cryptography to encrypt and decrypt data.Encoding and decoding secret signals is the study of cryptography. ones that are coded are referred to as cipher text, while ones that are uncoded are called plaintext. Emulation, often known as encoding, is the process of transforming plaintext into cipher text while decoding is the process of translating a cipher text to plaintext. [5] [7][9] [17][6]A message can be encrypted using a matrix as a cipher.To be used in decrypting, the matrix needs to be reversible. A 3x3 matrix made up of random integers can serve as a cipher matrix. Every character in the plaintext needs to be assigned a numerical value and organized into a matrix in order to encrypt it. o The values of these numerals can vary, but as an illustration, let's say that 1-26 stands for A to Z and 27 for a space. The cipher text message is then contained in a new matrix that is created by multiplying this matrix by the cipher matrix.To create secret codes, modern cryptography mostly uses electrical engineering and mathematics. The internet is used by everyone in today's society for a variety of reasons, including business, which deals with personal information that you would like to keep private, secure, and protected. Our daily lives involve cryptography in the form of ATM cards, computer passwords, and other things. The secret to these security codes is the use of encryption, which changes important data into a hidden format. The hidden form is converted back into the original message during decryption. There is very confidential information that goes into the system in order to encrypt and decrypt messages.

II. History

The study of deciphering messages encoded in a secret code is known as cryptography. Although cryptography is necessary for secure communications, it is not sufficient on its own. People's concern of having no security on the internet is the driving force behind the demand for encryption. Although secret codes have been used for years, World War 1 saw a rise in their use. The majority of the warring nations employed a

particular branch of the armed forces known as "signals intelligence." When Germany tried to incite the Mexican government to attack the United States by sending a message to the German embassy in Mexico City, this became extremely significant. Fortunately, Room 20 was able to interpret the telegram and crack the cipher, stopping the Mexican


WESTERN UNION
TELEGRAM

via Galveston

JAN 19 1917

GERMAN LEGATION
MEXICO CITY

130 13042 13401 8501 115 3028 416 17214 6491 11310
18147 18222 21560 10247 11518 23677 13605 3494 14936
98092 5905 11311 10392 10371 0302 21290 5161 39695
23571 17504 11269 18276 18101 0317 0228 17694 4473
23284 22200 19482 21589 67893 5569 13918 8958 12137
1333 4725 4458 5905 17166 13851 4458 17149 14471 6706
13850 12224 6929 14991 7382 15857 67893 14218 36477
6870 17553 67893 5870 5454 16102 15217 22801 17138
21001 17366 7116 23630 18222 6719 14331 15081 23645
3114 25552 22096 21604 4797 9497 22401 20855 4377
23610 18140 22280 5905 13347 20420 39689 13732 20667
6929 5275 18007 52262 1340 22049 13339 11265 22295
10439 14814 4178 6992 8784 7632 7357 6928 52262 11267
21100 21272 9346 9559 22464 15874 18502 18500 15857
2188 5376 7381 98092 16127 13486 9350 9220 76036 14219
5144 2831 17920 11347 17142 11264 7667 7762 15099 9110
10482 97556 3569 5870

BERNSTORFF.

Charge German Embassy.

Figure 1

III. Different ways of coding:

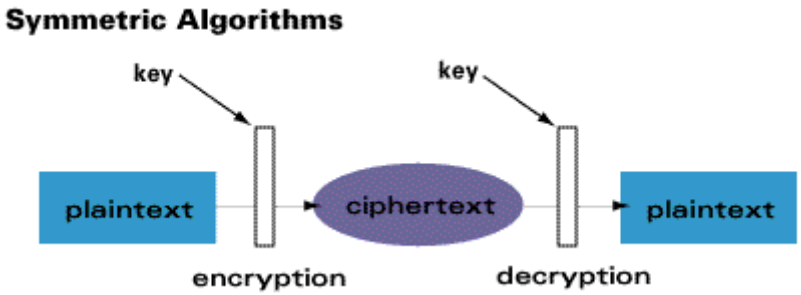
As there are many different versions of cryptography such as symmetric key, asymmetric key, and hash function, there are also many different ways to develop a cipher. We will focus on Hill cipher which is a polygraphic cipher. The Hill cipher transforms plain text into cipher text by matrix multiplication. Lester Hill was able to make an application of linear algebra to polygraphic ciphers. In 1929 and 1931 Lester Hill wrote articles on simple linear transformation in matrices. [8]

Well how do you encrypt a message? Cryptographers use matrices as ciphers to encrypt a message. In order to decrypt the message, the same matrix needs to be inverted. An example of creating a secret message, you first must create a cipher matrix composed of random complex integers. The cipher is the matrix that will change your message into the secret message. Next you would create a message, have 1-26 represents letter A-Z, respectively with 27 meaning a space and place the numerical value into the matrix. Take the cipher matrix and multiply the matrix with the message. This will create the cipher text that the receiver will receive. In order for the receiver to decode the message, they would have to take the cipher text and multiply by the inverted cipher created. The message will be revealed. This is one specific way of making a cipher text; there are many different ways to create the pattern for denotation of letter to numbers. [12] [9][15]

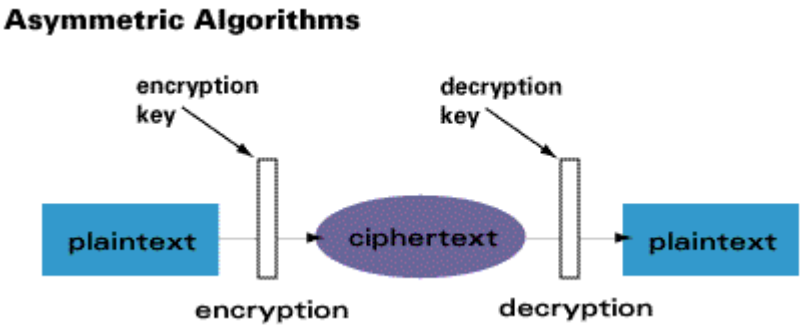
Symmetric and Asymmetric Algorithms

There are two types of key-based encryption, symmetric (or secret-key) and asymmetric (or public-key) algorithms. Symmetric algorithms use the same key for encryption and decryption (or the decryption key is easily derived from the encryption key), while asymmetric algorithms use a different key for encryption and decryption, and the decryption key cannot be derived from the encryption key. [5]

Symmetric algorithms can be divided into stream ciphers and block ciphers. Stream ciphers can encrypt a single bit of plaintext at a time, whereas block ciphers take a number of bits (typically 64 bits in modern ciphers), and encrypt them as a single unit. An example of a symmetric algorithm is DES.



Asymmetric ciphers (also called public-key cryptography) make a public key universally available, while only one individual possesses the private key. When data is encrypted with the public key, it can only be decrypted with the private key, and vice versa. Public key cryptography adds a very significant benefit - it can serve to authenticate a source (e.g. a digital signature). Public key cryptography was invented by Whitfield Diffie and Martin Hellman in 1975. An example of an asymmetric algorithm is RSA. [11]



In general, symmetric algorithms execute much faster than asymmetric ones. In real applications, they are often used together, with a public-key algorithm encrypting a randomly generated encryption key, while the random key encrypts the actual message using a symmetric algorithm. This combination is commonly referred to as a digital envelope. [16]

Substitution

One way of encryption is to replace each letter of alphabet by a different letter or a number. For example, replace **a** with **m**, and **b** with **k**, and so on. This type of coding is simple and by a number of techniques including analysis of frequency of letters, it is easy to be braked.

Polygraphic System

Another way of encoding is to divide plain text into sets of n-letters, and replace them with n code letters. In this case invertible matrices can be used to provide a better coding, than substitution. [8]

First associate a different number with every letter of alphabet.

For example we may use the following conversion table:

A	B	C	D	E	F	G	H	I	J	K	L	M
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
5	6	7	8	9	10	11	12	13	14	15	16	17

N	O	P	Q	R	S	T	U	V	Z	X	Y	Z
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
18	19	20	21	22	23	24	25	26	27	28	29	30

Suppose$n = 3$; choose a3×3invertible matrix A,

$$A = \begin{bmatrix} 1 & -1 & 1 \\ 2 & -1 & 0 \\ 1 & 0 & 0 \end{bmatrix}$$

Then,

$$A^{-1} = \begin{bmatrix} 0 & 0 & 1 \\ 0 & -1 & 2 \\ 1 & -1 & 1 \end{bmatrix}$$

A	B	C	D	E	F	G	H	I	J	K	L	M
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
5	6	7	8	9	10	11	12	13	14	15	16	17

Both communicating parties should have knowledge of the table which list association of letters to numbers, the matrices A and A^{-1} . The party that wants to send a message, needs to convert it to a string of numbers. As a second step that string of numbers needs to be divided into groups of 3, then multiple each group by the matrix *A* to form new groups and build a new string of numbers. Then, send the resulted string as a string of numbers or letters. The party who is receiving the coded string should divide the string into groups of 3, then multiple by A^{-1} and finally convert it to letters

N	O	P	Q	R	S	T	U	V	Z	X	Y	Z
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
18	19	20	21	22	23	24	25	26	27	28	29	30

Example 1:

Suppose you want to encode and send the following message: "This is confidential"

First, using the conversion table, find the corresponding numbers associate with each letter.

This is confidential

Produces the following string of numbers:24 12 13 23 13 23 7 19 18 10 13 8 9 18 24 13 5 16

Then, divide the number into groups of 3 and write each group in the form of a 3×1 vector.

$$\begin{bmatrix}24\\12\\13\end{bmatrix}\ \begin{bmatrix}23\\13\\23\end{bmatrix}\ \begin{bmatrix}7\\19\\18\end{bmatrix}\ \begin{bmatrix}10\\13\\8\end{bmatrix}\ \begin{bmatrix}9\\18\\24\end{bmatrix}\ \begin{bmatrix}13\\5\\16\end{bmatrix}$$

The next step is to find the product of *A* with any of these vectors:

$$A\begin{bmatrix}24\\12\\13\end{bmatrix}, A\begin{bmatrix}23\\13\\23\end{bmatrix},...$$

Now you have the following vectors:

$$\begin{bmatrix}25\\36\\24\end{bmatrix}\ \begin{bmatrix}33\\33\\23\end{bmatrix}\begin{bmatrix}6\\-5\\7\end{bmatrix}\begin{bmatrix}5\\7\\10\end{bmatrix}\begin{bmatrix}15\\0\\9\end{bmatrix}\begin{bmatrix}24\\21\\13\end{bmatrix}$$

This will provide you with the following string which can be sent.

25 36 24 33 33 23 6 -5 7 5 7 10 15 0 9 24 21 13

The party who receives the message, should divide it into groups of 3 and form (3×1) vectors and then multiplies each vector by A^{-1}

For example, $A^{-1}\begin{bmatrix}25\\36\\24\end{bmatrix}=\begin{bmatrix}0&0&1\\0&-1&2\\1&-1&1\end{bmatrix}\begin{bmatrix}25\\36\\24\end{bmatrix}=\begin{bmatrix}24\\12\\13\end{bmatrix}$

After obtaining a string of numbers, the conversion table can be used to convert the string to letters and obtain the decoded message.

Example 2:

Consider an association of the alphabet with numbers in the following conversion table and given matrices A and A^{-1}.Encode and decode the message "PLEASE DO NOT COME"

A	B	C	D	E	F	G	H	I	J	K	L	M
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
1	3	5	7	9	11	13	15	17	19	21	23	25

N	O	P	Q	R	S	T	U	V	Z	X	Y	Z
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
27	19	31	33	35	37	39	41	43	45	47	49	57

$$A=\begin{bmatrix}2 & 3\\ 3 & 5\end{bmatrix}, A^{-1}=\begin{bmatrix}5 & -3\\ -3 & 2\end{bmatrix}$$

And let.

a) Enoding the message:
First, using the coversion table above, find the corresponding string of numbers associate with this message.

PLEASE DO NOT COME

is equivalent to

31 23 9 1 37 9 7 29 27 29 39 5 29 25 9

Next, divide the string of numbers into pairs and group them in (2×1) vectors. Notice that the number of the letters in the plaintext is odd and is not divisible by 2, therefore, we add a dummy letter "E" to the end of the code and form eight different (2×1) vectors. The following string of numbers is produced by multiplying the eight (2×1) vectors by A.

131 208 21 32 101 156 101 166 141 226 93 142 133 212 45 72

and it is the message that should be transmitted.

b) **Decode the message:**

Assuming that you have A and A^{-1}, and the conversion table, and received the following message. You want to decode this message.

117 190 93 140 97 150 185 292 205 328

First, divide it into pairs and form five (2×1) vectors. Then, multiplies each of these vectors by A^{-1}, and form the following string of numbers:

15 29 45 1 35 9 49 29 41 41

Finally using the conversion table, find letters of alphabet corresponding to these numbers, as a result, you will get

H O W A R E Y O U

which will read as

HOW ARE YOU

Breaking a code

The coding and decoding techniques that we discussed used invertible matrices which represent linear transformation. The purpose of cryptography is to find a secure ways of transmitting information that prevents unauthorized entities from learning content of the message. So for each specific way of coding one of the main questions needed to be answered is the following: [1]

How much information needed for someone to break the code?

Since we are using linear transformations for coding and decoding when we use matrices, we need to learn about their properties. Recall that any linear transformation $L:V\to W$ is completely determined by the image of a basis for V . So if A is an $n\times m$ matrix, we need to know n-plaintext vectors $P_1,P_2,.....P_n$, and the cipher text (coded) vectors $AP_1,AP_2,....,AP_n$ to break the code. Breaking the code means obtaining the matrix A^{-1}.

To do this we may form a matrix P

$$P=\left[P_1\middle|P_2\middle|...\middle|P_n\right]$$

Whose columns are plaintext vectors

$$P_1,P_2,.....P_n$$

and let,

$$Q=\left[AP_1\middle|AP_2\middle|...\middle|AP_n\right]$$

Hence, $Q=AP$ and $A^{-1}=PQ^{-1}$. This will give us the tool to decode the message. To use row operation to find A^{-1}, you may want to write $A^{-1}=PQ^{-1}$ as $A^{-1}\,A^{-1}Q=P$ or $Q^T(A^{-1})^T=P^T$. To find A^{-1} you need first solve for $(A^{-1})^T$, by row reducing (using Gaussian Elimination) $[Q^T\,|\,P^T]$ to $\left[I\middle|(A^{-1})^T\right]$.

Example 3:

Suppose that you have received the following message from a friend,

L U P O Z M A E A E G I U A B J

Using standard conversion table, it becomes

12 21 16 15 0 13 1 5 1 5 7 9 21 1 2 10,

Which also the same as (due to mod 26),

12 47 16 67 52 65 27 83 79 135 33 113 47 53 80 140.

Unfortunately, you do not recall the matrix A or A^{-1}. But you know that the plaintext of the fifth through eighth letters is GOOD, is it possible that you figure out what is the original message?

The answer is YES. Knowing the word GOOD, you can find the numerical equivalent of those letters. That is 7 15 for GO and 15 4 for OD. You also know the numerical equivalent of the fifth to eight letters in the encoded message are

52 65 for ZM and 27 83 for AE.

Therefore you can form the matrix P and Q.

$$P_1 = \begin{bmatrix} 7 \\ 15 \end{bmatrix} \leftrightarrow C_1 = \begin{bmatrix} 58 \\ 65 \end{bmatrix}$$

$$P_2 = \begin{bmatrix} 15 \\ 4 \end{bmatrix} \leftrightarrow C_1 = \begin{bmatrix} 27 \\ 83 \end{bmatrix}$$

You can construct

$$Q^T = \begin{bmatrix} C_1^T \\ C_2^T \end{bmatrix} = \begin{bmatrix} 52 & 65 \\ 27 & 83 \end{bmatrix}$$

And,

$$P^T = \begin{bmatrix} P_1^T \\ P_2^T \end{bmatrix} = \begin{bmatrix} 7 & 15 \\ 15 & 4 \end{bmatrix}$$

Form the matrix $[Q^T | P^T]$ and use Gaussian Elimination to reduce Q^T to the identity matrix, the matrix $[Q^T | P^T]$ will change to $[I | (A^{-1})^T]$.

$$\begin{bmatrix} 52 & 65 & 7 & 15 \\ 27 & 83 & 15 & 4 \end{bmatrix}$$

Change to

$$\begin{bmatrix} 1 & 0 & \frac{-2}{13} & \frac{5}{13} \\ 0 & 1 & \frac{3}{13} & \frac{-1}{13} \end{bmatrix}$$

Since the matrix $\begin{bmatrix} \frac{-2}{13} & \frac{5}{13} \\ \frac{3}{13} & \frac{-1}{13} \end{bmatrix}$ is the transpose of A^{-1}, your need to find the transpose of it is matrix to get A^{-1}.

Therefore,

$$A^{-1} = \begin{bmatrix} \frac{-2}{13} & \frac{3}{13} \\ \frac{5}{13} & \frac{-1}{13} \end{bmatrix}$$

Multiply the secret message by A^{-1}, you will get

9 1 13 1 7 15 15 4 19 20 21 4 5 14 20 20

Use the conversion table to find the corresponding letters: IAMAG00DSTUDENTT, which will read "I am a good student".

Problems

Problem 1

Decode the message KNOXAOJX given that it is a Hill cipher (based on matrix transformation) with enciphering matrix $\begin{bmatrix} 4 & 1 \\ 3 & 2 \end{bmatrix}$.

Solution of Problem 1

Given $A = \begin{bmatrix} 4 & 1 \\ 3 & 2 \end{bmatrix}$, we can find

$$A^{-1} = (8-3)^{-1} \begin{bmatrix} 2 & -1 \\ -1 & 4 \end{bmatrix} = 5^{-1} \begin{bmatrix} 2 & -1 \\ -3 & 4 \end{bmatrix}$$

But this matrix does not have integer entries, and is not very helpful. Since our conversion table has 26 letters, we may want to use modular arithmetic, with $\mod 26$ mod26. Since $5 \times 21 = 1 \mod 26$, we may replace $\frac{1}{5}$ by 21. Therefore,

$$A^{-1} = 21 \begin{bmatrix} 2 & -1 \\ -3 & 4 \end{bmatrix} = \begin{bmatrix} 42 & -21 \\ -63 & 84 \end{bmatrix} = \begin{bmatrix} 16 & 5 \\ 15 & 6 \end{bmatrix}$$

in the multiplications above modular arithmetic's ($\mod 26$) is used.

To double check, find AA^{-1} which should be equal to the identity matrix.

$$\begin{bmatrix} 4 & 1 \\ 3 & 2 \end{bmatrix}\begin{bmatrix} 16 & 5 \\ 15 & 6 \end{bmatrix} = \begin{bmatrix} 79 & 26 \\ 78 & 27 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I \ .$$

Now, knowing that $A^{-1} = \begin{bmatrix} 16 & 5 \\ 15 & 6 \end{bmatrix}$, we can divide the whole message into pairs, and convert them into their corresponding numerical values.

11 14 15 24 1 15 10 24

Now multiply A^{-1} by each of these encoded vector, the numbers change to

246249360369911052802 94

Using modular arithmetic, $\mod 26$, the numbers become

12 15 22 5 13 1 20 8

Which converts to the following string of letters:

L O V E M A T H

This yields the message,

LOVE MATH

Problem 2

Use the following 3×3 matrix B to encode the message " PROF IS BORING ".

$$B = \begin{bmatrix} 2 & 3 & 2 \\ 1 & 4 & 2 \\ 5 & 2 & 3 \end{bmatrix}$$

Solution of Problem 2

First, convert the message to its corresponding number values,

16 18 15 6 9 19 2 15 18 9 14 7.

Then, divide the string into groups of three, to obtain:

16 18 15 6 9 19 2 15 18 9 14 7.

Form 3×1 vectors and multiply them by B, to obtain the encoded message:

116 118 161 77 80 105 85 98 94 74 79 94.

Problem 3

Decode the following massage using the standard conversion table and the matrix $B=\begin{bmatrix}2 & 3 & 2\\ 1 & 4 & 2\\ 5 & 2 & 3\end{bmatrix}$ given in problem 2.

Solution to Problem 3

First, find the inverse of matrix B, which is $\begin{bmatrix}8 & -5 & -2\\ 7 & -4 & -2\\ -18 & 11 & 5\end{bmatrix}$

Then, divide the incoming numbers into groups of three, form 3×1 vectors, multiply each vector by the inverse of matrix B. You will get the following string of numbers:

16 18 15 6 9 19 2 15 18 9 14 7

Converting these to letters, the message reads

P R O F I S B O R I N G

So the message decodes to "Prof Is Boring."

III. Conclusion

In conclusion, this review highlights the critical role of linear algebra in advancing cryptographic techniques, particularly through applications like the Hill cipher and matrix-based encryption methods. The use of invertible matrices and modular arithmetic showcases the potential for linear transformations to enhance data security and confidentiality in diverse fields, including communication, banking, and online transactions. Despite the robustness of these methods, challenges remain in addressing vulnerabilities to increasingly sophisticated cryptanalysis techniques.

Future work should focus on developing more efficient algorithms for key generation and matrix inversion, as well as integrating advanced machine learning models to detect and counter potential security breaches. Additionally, exploring the combination of linear algebra with emerging technologies such as quantum computing could pave the way for more secure and scalable cryptographic systems. These advancements will further solidify the role of linear algebra in ensuring secure communication in an increasingly digital and interconnected world

REFERENCES

[1]. Anton, H., &Rorres, C. (1994). Elementary Linear Algebra: Applications Version (7th ed.). New York: John Wiley & Sons.
[2]. Kolman, B. (1997). Introductory Linear Algebra with Applications. New Jersey: Prentice Hall.
[3]. Abraham, S. (1966). Elementary Cryptanalysis: A Mathematical Approach. Mathematical Association of America.
[4]. Konheim, A. G. (1981). Cryptography: A Primer. New York: Wiley-Interscience.
[5]. Stallings, W. (2005). Cryptography and Network Security: Principles and Practices (4th ed.). Prentice Hall.
[6]. Schneier, B. (1996). Applied Cryptography: Protocols, Algorithms, and Source Code in C. Wiley.
[7]. Diffie, W., & Hellman, M. (1976). New Directions in Cryptography. IEEE Transactions on Information Theory, 22(6), 644–654.
[8]. Hill, L. S. (1929). Cryptography in an Algebraic Alphabet. The American Mathematical Monthly, 36(6), 306–312.
[9]. Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (1996). Handbook of Applied Cryptography. CRC Press.
[10]. Daemen, J., &Rijmen, V. (2002). The Design of Rijndael: AES - The Advanced Encryption Standard. Springer.

[11]. Rivest, R. L., Shamir, A., &Adleman, L. (1978). A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM, 21(2), 120–126.
[12]. Hoffman, K., &Kunze, R. (1971). Linear Algebra (2nd ed.). Prentice Hall.
[13]. Goldreich, O. (2004). Foundations of Cryptography (Vol. 1). Cambridge University Press.
[14]. Koblitz, N. (1994). A Course in Number Theory and Cryptography. Springer.
[15]. Gallian, J. A. (2017). Contemporary Abstract Algebra (9th ed.). Cengage Learning.
[16]. Katz, J., &Lindell, Y. (2007). Introduction to Modern Cryptography. Chapman and Hall/CRC.
[17]. Shannon, C. E. (1949). Communication Theory of Secrecy Systems. Bell System Technical Journal, 28(4), 656–715.
[18]. Blakley, G. R. (1979). Safeguarding Cryptographic Keys. Proceedings of the National Computer Conference, 48, 313–317.
[19]. Bernstein, D. J. (2009). Introduction to Post-Quantum Cryptography. In D. J. Bernstein, J. Buchmann, & E. Dahmen (Eds.), Post-Quantum Cryptography (pp. 1–14). Springer.
[20]. Mitzenmacher, M., &Upfal, E. (2005). Probability and Computing: Randomized Algorithms and Probabilistic Analysis. Cambridge University Press.