Original Article
Bulletin of Pure and Applied Sciences.
Mathematics & Statistics Vol.45 E, No.2.
July-December 2026: P.37-44

Print version ISSN 0970 6577
Online version ISSN 2320 3226
Available online at www.bpasjournals.com

Mathematical Cryptography: From Ancient to Modern Techniques

[1]L. Jyotsna, [2]A. Ashwini, [3]B. Thanu Sri, [4]P. Vishnupriya, [5]S. Yamini

Author Affiliation:
[1-5]Department of Mathematical and Computational Sciences, Sri Sathya Sai University for Human Excellence, Kalaburagi, Karnataka, India

***Corresponding Author:** **L Jyotsna**, Department of Mathematical and Computational Sciences, Sri Sathya Sai University for Human Excellence, Kalaburagi, Karnataka, India
E-mail: jyotsna.l@sssuhe.ac.in

ABSTRACT
This review article delves into the evolution and significance of cryptography, retracing its applications from the ancient times to the digital era. It emphasises the pivotal role of the mathematics in the development of the cryptographic techniques. To show the real-world applicability of classical cryptographic methods, the existing Shift Cipher has been utilised to encrypt and decrypt an Excel document containing data using Python code implementation for practical data security applications.

Keyword: Cryptography, Encryption, Decryption, Symmetric, Asymmetric, Ancient Indian Cryptography.

How to cite this article: Jyotsna L., Ashwini A., Thanu Sri B., Vishnupriya P., Yamini S. Mathematical Cryptography: From Ancient to Modern Techniques. *Bulletin of Pure and Applied Sciences- Math & Stat.*, 2026;45E (1):37-44.

Received on 10.04.2026, Revised on 22.06.2026, Accepted on 19.07.2026

1. INTRODUCTION

Throughout our lives, we often find ourselves concealing certain information from others-whether it's our grades from friends, personal diaries from family, confidential documents, or unique ideas from competitors. We desire to keep this information secure to protect our privacy, maintain trust in our relationships, and safeguard our personal and professional interests.

With the advanced technology, our information has largely shifted to online platforms. We share significant amounts of personal data under the belief that it remains secure. However, these technological advancements have also facilitated the efforts of hackers, who can steal the data and pose cyber threats. However, in certain situations, hacking information can also serve a beneficial purpose, such as in the military, where commanders use the hacking process to rescue the country from terrorists. Thus, the study of secure communication techniques that allow only the sender and not the unintended receiver of a message to read its content is known as "cryptography". The term cryptography comes from the Greek word "Kryptos," which means hidden. It is closely linked to encryption, which is the process of scrambling plain text into ciphertext and then converting it back when it is received; this process is called decryption.

Cryptography has two classes: Symmetric and Asymmetric systems.

Symmetric cryptosystem: This cryptosystem uses one shared key for both enciphering, converting plaintext into ciphertext, and deciphering, converting ciphertext into plaintext. A well-known example is the Data Encryption Standard (DES), an algorithm that was widely used in the past. However, with the development of technology, it became easier for unauthorised persons to crack it, which led to the Advanced Encryption Standard (AES) being widely used because it provides longer keys, making unauthorised access highly difficult.

Asymmetric cryptosystem: This system uses a pair of keys, a public key and a private key. The public key is shared with the populace, and it can be used by anyone for data encryption. The private key is kept confidential by the proprietor and is used to decipher the data back into its original form. Rivest-Shamir-Adleman (RSA) and Secure Hash Algorithm (SHA) are popular algorithms that rely on this principle, applying the public key for encryption and the private key for authentication and decryption.

These cryptosystems are designed to secure the data from unauthorised access. However, there is a practice called cryptoanalysis, which involves decrypting an encrypted message without using the encryption key by unauthorised individuals. This field of study, known as cryptanalysis, is the art of understanding the weakness in ciphertext and finding methods to break it without the enciphering key [1, 7].

2. ROLE OF CRYPTOGRAPHY FROM THE ANCIENT TO THE MODERN ERA

India's history of number systems is truly fascinating. The earliest evidence of a numerical system in India dates back to the Vedic period, where basic mathematical operations were developed for constructing fire altars and for astronomy [2]. Later, during Ashoka's period, archaeologists found numerals on the cave walls and on the coins [4]. These carvings have shown two types of writing: Kharosthi and Brahmi. These two scripts represented numerical systems. These early forms of numerals laid the groundwork for mathematical advancements that followed.

Around the 6th century CE, the KaTaPaYaDi system emerged, using Sanskrit letters to express numbers, making it easier to remember numbers as words or verses. This system was highly flexible [3]. Besides the KaTaPaYaDi system, there were many other cryptosystems such as Aryabhata Akshara Sankhya, Bhutha Sankhya, Ramshalaka, Kautilayama, Muladivaya, and Gudhayojya. Here is a brief introduction to the ancient Indian Cryptosystems.

2.1. Bhūtasaṃkhyā System:

The Bhūtasaṃkhyā System operates on the principle of assigning common words to numerical values. These common words include the following:

1. Physical bodies, including the earth, moon, planets, stars, oceans, mountains, fire, sky, directions, etc.
2. Parts of the human body, such as eyes, ears, jaws, knees, hands, fingers, teeth, etc.
3. Animals such as serpents, horses, elephants, etc. [5].
4. The names of devatas such as Shiva, Indra, Surya, and sometimes historical persons such as Manu, Rama, etc

Thus, the Bhūtasaṃkhyā refers to the collection of things denoted by that number. Hence, our ancestors used these common words in their ślokas or verses to mention the numbers they had in their mind [5]. Some numbers have multiple representations; the common words and their synonyms correspond to the same numerical value.

Numerals, which are represented by various words in the Bhūtasaṃkhyā system, are given below:

- 0 is represented by बिन्दु (point), नभस् (sky), रन्ध्र (hole), ख (space), आकाश (ether), पूर्ण (complete), व्योमन् (sky), अम्बर (sky), जलधर (cloud), शून्य (zero or empty), ब्रह्मन् (Brahman).
- 1 is represented by all that is unique, like भूमि (earth), चन्द्र (moon), sun, वदन (face), वाच् (speech), रूप (form), because everything has only its own shape; it is also used to represent ब्रह्मन् (Brahman), आदि (beginning).
- 2 is represented by the dualities and pairs like (नेत्र)(चक्षुस्)(अक्षीणि) eyes, ears, jaws, (हस्त)(पाणि) hands, यम (pair), dvi, dvandva, युगल (twin). Ashvini devatas, Yama, the word 'पक्ष', which is the moon's waxing and waning periods (krishnapaksha and shulkapaksha).

Application: Five centuries ago, Neelakanta Somayaji, in his commentary on Arya Bhatiya, provided the value of π (pi) up to 13 decimal places using the Bhūtasaṃkhyā system. The verse is as follows.

- विभुधनेत्रगजाहिहुताशनत्रिगुणवेदाभासारनबाहवः।
- नवनीखर्वमिते वृत्तिविस्तरे परिधिमानमिदं जगदुरुभुदः॥

In this verse, the first line represents the numbers 33 (vibhuda), 2 (netra), 8 (gaja), 8 (ahi), 3 (hutasana), 3 (tri), 3 (guna), 4 (veda), 27 (bha), 8 (sarana), and 2 (bahavaha), forming the number 2827433388233. The second line instructs to divide this number by "Navanikharvamm," representing 900,000,000,000, resulting in the value 3.1415926535922.

2.2. KaTaPaYaDi System:

The KaTaPaYaDi System has come from the Kerala school.

Number	1	2	**3**	**4**	5	6	7	8	9	0
Sanskrit letters	क	ख	ग	घ	ङ	च	छ	ज	झ	ञ
	ट	ठ	ड	ढ	ण	त	थ	द	ध	न
	प	फ	ब	भ	म	–	–	–	–	–
	य	र	ल	व	श	ष	स	ह	–	–

Table.2.1

The column, represented by the blue colour in the Table.2.1, gives the name KaTaPaYaDi to the system "कटपयादि", 'ādi' in Sanskrit means etc.

Rules for Encoding and Decoding:

A few simple rules are followed while encoding and decoding the numbers under the Katapayadi system.

अङ्कानां वामतो गतिः। añkānām vämato gatih

This Sanskrit phrase translates to: "The movement of numbers is from left to right." In the context of the Katapayadi system, this indicates that the numerical values encoded in Sanskrit letters are interpreted from left to right, similar to the reading of numbers in modern times. It is a succinct way to remind users of the reading direction for the encoded numerals.

The Sadratnamāla text, written by Śankarauarman, explains further rules for converting numbers into coded forms using the Katapayadi.

- Vowels are represented with zero (śunya).
- The nine integers (1to 9) are represented by the consonant group beginning with the alphabet "ka", "ta" , " pa" , " ya".
- In a conjunct consonant (miśram), only the last of the consonants should be counted, e.g., in स्व, only व is to be used, स is ignored.
- A consonant in its half form is to be ignored.

Example: The name रामा ≡ 25 in the KaTaPaYaDi system but when read the application of this rule Rāmā becomes the encoding for the 52. The best Application for the KaTaPaYaDi system is Melakartha Raga in the Carnatic music. From these ragas, many other derivative (Janya) ragas are formed.

Naming the Ragas:

- The first two syllables of the raga name represent the raga's position in the Melakartha sequence.
  Example:

Ratnāngi Raga:

- The syllables "Ra" and "Na" in "Ratnāngi" represent the number 02.
- This makes Ratnāngi the 2nd Melakartha raga.
- In this context, the letters "Ra" and "Na" are considered, while the half-letter "Ta" is ignored.

This legacy now forms the foundation of modern cryptosystems.

2.3. Modern Application of Cryptography:

In the introduction, modern cryptosystems were briefly discussed. Now, let us dive into the digital world applications, such as WhatsApp, online banking, and e-commerce, where encryption safeguards sensitive data.

Online Banking:

Online banking depends on cryptography to keep financial information secure. It works behind the scenes to encrypt sensitive data such as passwords and account details, ensuring that even if someone intercepts it, they cannot read it.

Example: The figures show the official website of the State Bank of India. The URL of this website, https://onlinesbi.sbi.com, is a good indication that the website is protected using cryptography. Here, a certificate signature algorithm and a certificate signature value are used. The algorithm used is SHA-256, which is a secure asymmetric cryptographic algorithm.

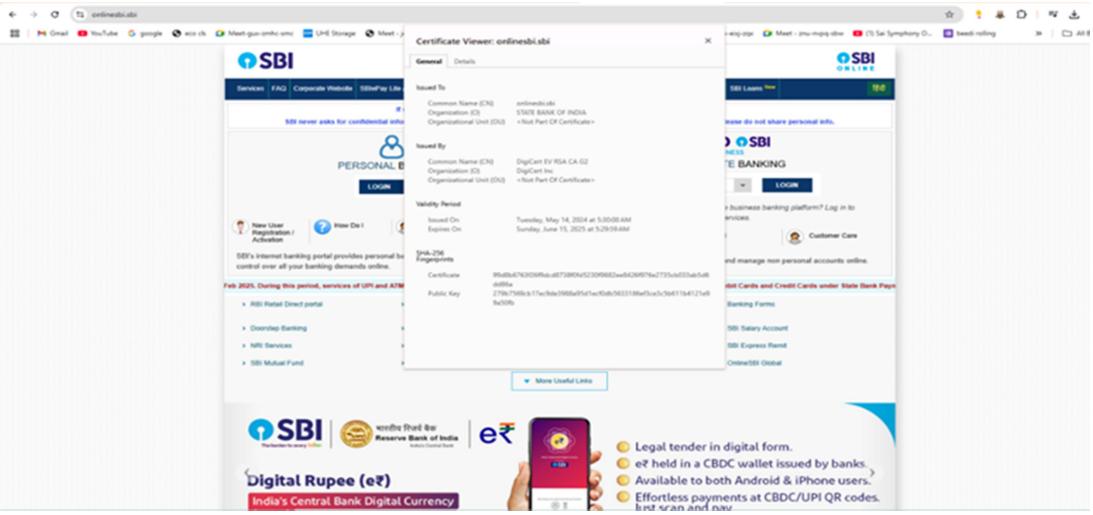


Figure 2.3(a): Online banking

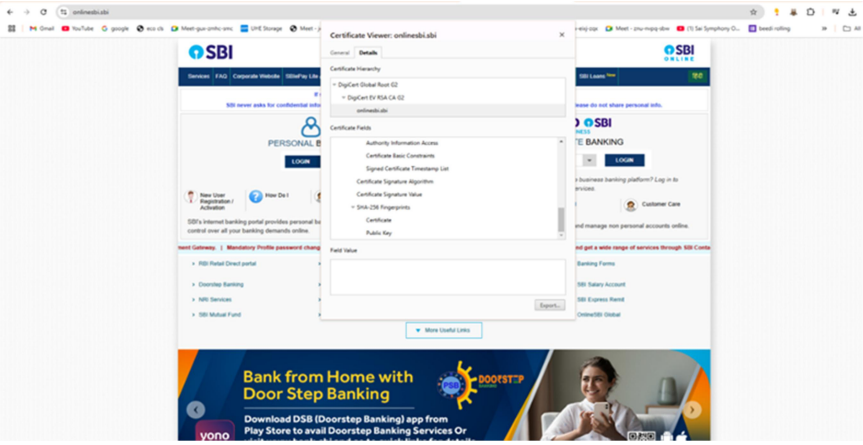


Figure 2.3(b): Online banking

Social Media platforms:

Cryptography is a key tool that keeps social media secure and private for users. It uses end-to-end encryption (E2EE), ensuring that only the sender and the intended recipient can read messages, as the decryption keys are kept solely on their devices. This means that no one else, not even the platform, can access those conversations. Additionally, sensitive data, such as passwords, is protected using hashing, a process that securely scrambles the information so it can't be easily stolen or misused.

Example:

Fig.2.3(c) shows the page used to log in to WhatsApp Web. The URL of this site is https://web.whatsapp.com, which indicates that the site is secured via cryptography. This site employs end-to-end encryption, ensuring that only the sender and the intended recipient can read the messages and not anybody else. Both encryption and decryption are secured on WhatsApp Web, where there is an indication of a secure connection, permissions for this site, and tracking prevention for this site (balanced).

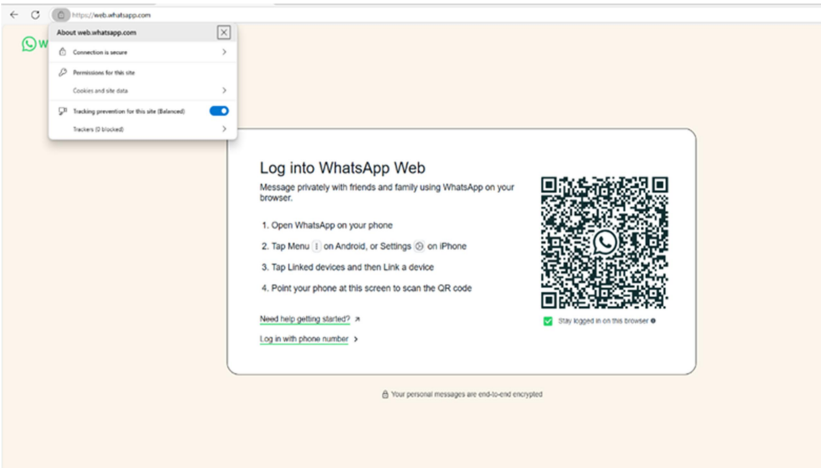


Figure 2.3(c): Social Media Platform.

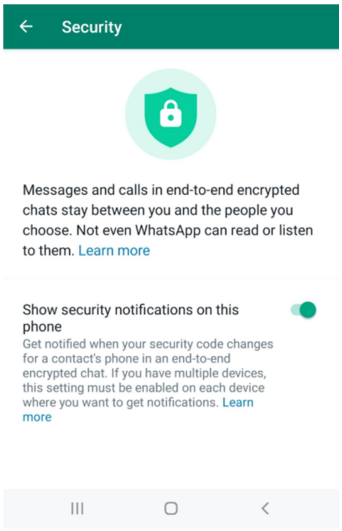


Figure 2.3(d): Social media platforms

3. IMPLEMENTATION OF SHIFT CIPHER FOR ENCRYPTION AND DECRYPTION OF EXCEL DATA

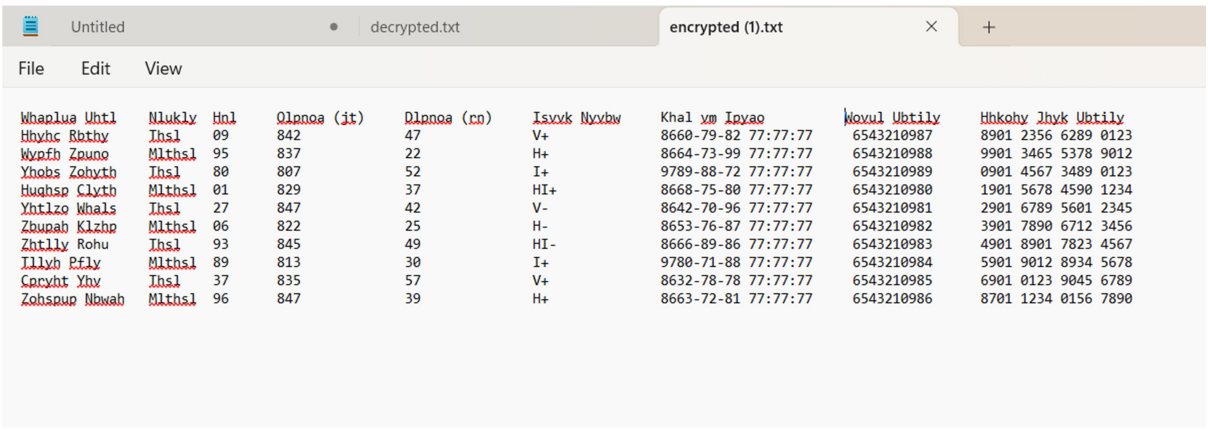
Shift Cipher is a substitution cipher where each character in the plaintext is shifted a specific number of places down the alphabet.
Mathematical representation:
Encryption: $C = (P + K) \, mod \, 26$
Decryption: $P = (C - K) \, mod \, 26$
Where, C represents the ciphertext letter, P represents the plaintext letter, $K$is the shift key (K=3). Below are examples of the encryption and decryption of the Shift cipher:
Encryption:
Plaintext is – "THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG"
Decryption:
Ciphertext is – "WKH TXLFN EURZQIRA MXPSV RYHU WKH ODCB GRJ"
An example of its use is demonstrated through an Excel sheet.
Figure 3.1 shows the data in the Excel file.

J23

	B	C	D	E	F	G	H	I
1	Gender	Age	Height (cm)	Weight (kg)	Blood Group	Date of Birth	Phone Number	Aadhar Card Number
2	Male	32	175	70	O+	15-02-1993	9876543210	1234 5689 9512 3456
3	Female	28	160	55	A+	07-07-2004	9876543211	2234 6798 8601 2345
4	Male	13	130	85	B+	05-11-2012	9876543212	3234 7890 6712 3456
5	Female	34	152	60	AB+	13-08-1991	9876543213	4234 8901 7823 4567
6	Male	50	170	75	O-	29-03-1975	9876543214	5234 9012 8934 5678
7	Female	39	155	58	A-	10-09-1986	9876543215	6234 0123 9045 6789
8	Male	26	178	72	AB-	19-12-1999	9876543216	7234 1234 0156 7890
9	Female	12	146	63	B+	11-04-2013	9876543217	8234 2345 1267 8901
10	Male	60	168	80	O+	01-01-1965	9876543218	9234 3456 2378 9012
11	Female	29	170	62	A+	14-05-1996	9876543219	1034 4567 3489 0123
12								
13								
14								
15								
16								

Figure 3.1: . Data to be encrypted

Using the Shift Cipher algorithm, a user-input Python code [6] was written to encrypt the Excel file. After compiling the code, the user was asked to enter the key (shift value). The key value "7" was entered, and the program generated a file named "encrypted.txt."



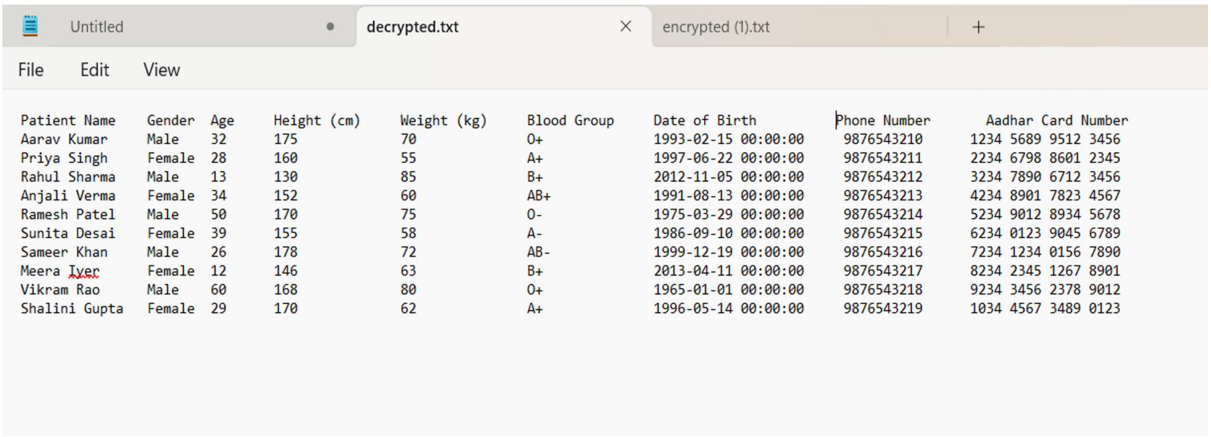
Untitled • decrypted.txt encrypted (1).txt

File Edit View

Whaplua Uhtl	Nlukly	Hnl	Olpnoa (it)	Olpnoa (rn)	Isvvk Nyvbw	Khal vm Ipyao	Wovul Ubtily	Hhkohy Jhyk Ubtily
Hhyhc Rbthy	Ihsl	09	842	47	V+	8660-79-82 77:77:77	6543210987	8901 2356 6289 0123
Wypfh Zpuno	Mlthsl	95	837	22	H+	8664-73-99 77:77:77	6543210988	9901 3465 5378 9012
Yhobs Zohyth	Ihsl	80	807	52	I+	9789-88-72 77:77:77	6543210989	0901 4567 3489 0123
Huqhsp Clyth	Mlthsl	01	829	37	HI+	8668-75-80 77:77:77	6543210980	1901 5678 4590 1234
Yhtlzo Whals	Ihsl	27	847	42	V-	8642-70-96 77:77:77	6543210981	2901 6789 5601 2345
Zbupah Klzhp	Mlthsl	06	822	25	H-	8653-76-87 77:77:77	6543210982	3901 7890 6712 3456
Zhtlly Rohu	Ihsl	93	845	49	HI-	8666-89-86 77:77:77	6543210983	4901 8901 7823 4567
Tllyh Pfly	Mlthsl	89	813	30	I+	9780-71-88 77:77:77	6543210984	5901 9012 8934 5678
Cpryht Yhv	Ihsl	37	835	57	V+	8632-78-78 77:77:77	6543210985	6901 0123 9045 6789
Zohspup Nbwah	Mlthsl	96	847	39	H+	8663-72-81 77:77:77	6543210986	8701 1234 0156 7890

Encrypted.txt

The same parameters used for the encryption code were applied to decrypt the Excel file. A Python code was developed for the decryption process. After compiling the code, the program prompted the user to enter the key (shift value used for encryption). After entering the key value "7", the program saved the decrypted file as "decrypted.txt".



Untitled • decrypted.txt encrypted (1).txt

File Edit View

Patient Name	Gender	Age	Height (cm)	Weight (kg)	Blood Group	Date of Birth	Phone Number	Aadhar Card Number
Aarav Kumar	Male	32	175	70	O+	1993-02-15 00:00:00	9876543210	1234 5689 9512 3456
Priya Singh	Female	28	160	55	A+	1997-06-22 00:00:00	9876543211	2234 6798 8601 2345
Rahul Sharma	Male	13	130	85	B+	2012-11-05 00:00:00	9876543212	3234 7890 6712 3456
Anjali Verma	Female	34	152	60	AB+	1991-08-13 00:00:00	9876543213	4234 8901 7823 4567
Ramesh Patel	Male	50	170	75	O-	1975-03-29 00:00:00	9876543214	5234 9012 8934 5678
Sunita Desai	Female	39	155	58	A-	1986-09-10 00:00:00	9876543215	6234 0123 9045 6789
Sameer Khan	Male	26	178	72	AB-	1999-12-19 00:00:00	9876543216	7234 1234 0156 7890
Meera Iyer	Female	12	146	63	B+	2013-04-11 00:00:00	9876543217	8234 2345 1267 8901
Vikram Rao	Male	60	168	80	O+	1965-01-01 00:00:00	9876543218	9234 3456 2378 9012
Shalini Gupta	Female	29	170	62	A+	1996-05-14 00:00:00	9876543219	1034 4567 3489 0123

Decrypted.txt

Above fig shows the decrypted file which is matching to the original file in the fig (3.1).

4. CONCLUSION

Securing information from unauthorised access is crucial to maintaining privacy and trust. To achieve this, we rely on cryptography, which involves encoding information in such a way that only authorised parties can access it.

We developed a Python code to encrypt and decrypt the Excel file using the Shift Cipher algorithm, which already exists. This journey from ancient to modern cryptography, it highlights the continuous evolution of cryptography.

In this review article, we utilised the Shift Cipher algorithm in Python. Due to its limited key space, the ciphertext is vulnerable to hacking. In the future, we are aiming to develop a new cryptosystem with a more secure system immune to attacks and implement our future work algorithm in Python code.

REFERENCES

1. Adhikari MR, Adhikari A. Introduction to mathematical cryptography. In: *Basic Modern Algebra with Applications*. New Delhi: Springer; 2014. p. 517-584.
2. Dutta AK, Sriram MS. *Mathematics and Astronomy in India before 300 BCE*. New Delhi: National Mission for Manuscripts; 2016.
3. Fleet JF. The Kaṭapayādi notation of the Second Ārya-Siddhānta. J R Asiat Soc. 1912;44(2):459-462.
4. O'Connor JJ, Robertson EF. The history of Indian numerals. In: *MacTutor History of Mathematics Archive*. St Andrews (UK): University of St Andrews.
5. Rangacharya M, editor. *Gaṇita-sāra-saṅgraha of Mahāvīrācārya*. Madras: Government of Madras; 1912.
6. Saha A. *Doing Math with Python: Use Programming to Explore Algebra, Statistics, Calculus, and More!*. San Francisco (CA): No Starch Press; 2015.
7. Vaudenay S. *A Classical Introduction to Cryptography: Applications for Communications Security*. New York: Springer Science & Business Media; 2005.