Information Security Lab
[15B17CI576]

Client Server
Encryption-Decryption

Submitted to - Somya Jain Ma'am

Khushboo Kumari 19803003
Kanistha 19803008
Kanishka Khullar 19803011
Pranav Gupta 19803021

Table of Contents

Introduction

A very important aspect in the world of software development is the security of data that flows through open communication channels. In our web applications, there is an intensive exchange of data via different protocols ,like http, between client applications which are presented as browser, mobile and desktop applications and server side applications. The importance and confidentiality of data may be different depending on the specifics of the web application, and the possibility of interception by a third party increases with perfection of hacking techniques in the world of IT.

Problem Statement

Implement a three layered encryption decryption algorithm which transforms a key into various ways and encrypts the plain text repetitively.

Client-Server

The Client-server model is a distributed application structure that partitions task or workload between the providers of a resource or service, called servers, and service requesters called clients. In the client-server architecture, when the client computer sends a request for data to the server through the internet, the server accepts the requested process and delivers the data packets requested back to the client. Clients do not share any of their resources. Examples of Client-Server Model are Email, World Wide Web, etc.

Client: When we talk about the word Client, it means to talk of a person or an organization using a particular service. Similarly in the digital world a Client is a computer (Host) i.e. capable of receiving information or using a particular service from the service providers (Servers).

Servers: Similarly, when we talk about the word Servers, It means a person or medium that serves something. Similarly in this digital world a Server is a remote computer which provides information (data) or access to particular services.

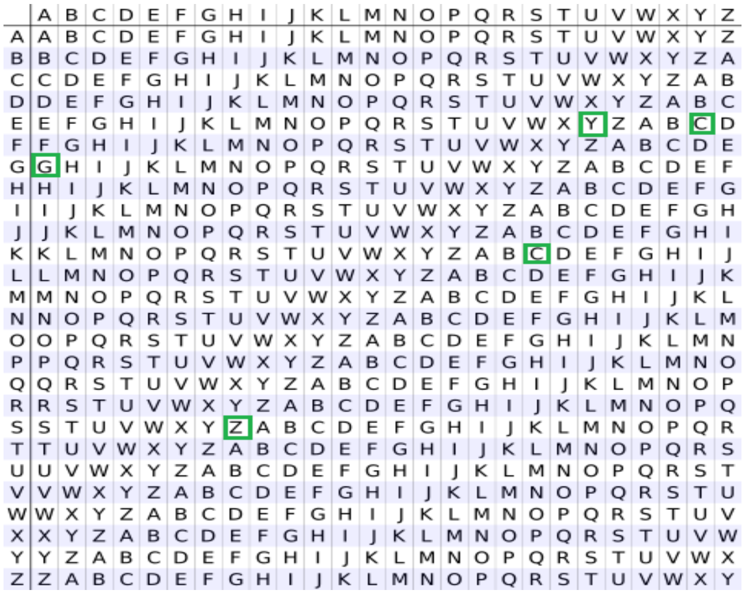
So, it's basically the Client requesting something and the Server serving it as long as it's present in the database.

Encryption-Decryption techniques

Vigenere (Polyalphabetic Cipher)

Vigenere Cipher is a method of encrypting alphabetic text. It uses a simple form of polyalphabetic substitution.A polyalphabetic cipher is any cipher based on substitution, using multiple substitution alphabets. The encryption of the original text is done using the Vigenère square or Vigenère table.

- ➢ The table consists of the alphabets written out 26 times in different rows, each alphabet shifted cyclically to the left compared to the previous alphabet, corresponding to the 26 possible Caesar Ciphers.
- ➢ At different points in the encryption process, the cipher uses a different alphabet from one of the rows.
- ➢ The alphabet used at each point depends on a repeating keyword.



	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

Encryption

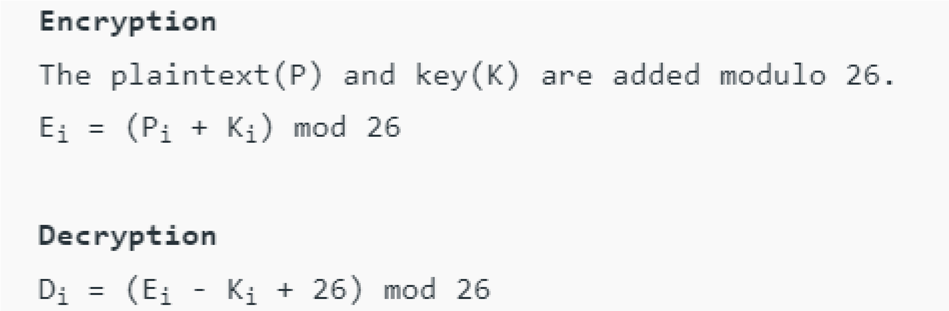
The first letter of the plaintext, G is paired with A, the first letter of the key. So use row G and column A of the Vigenère square, namely G. Similarly, for the second letter of the plaintext, the second letter of the key is used, the letter at row E, and column Y is C. The rest of the plaintext is enciphered in a similar fashion.

Decryption

Decryption is performed by going to the row in the table corresponding to the key, finding the position of the ciphertext letter in this row, and then using the column's label as the plaintext. For example, in row A (from AYUSH), the ciphertext G appears in column G, which is the first plaintext letter. Next, we go to row Y (from AYUSH), locate the ciphertext C which is found in column E, thus E is the second plaintext letter.

Alternative to vigenere table

A more easy implementation could be to visualize Vigenère algebraically by converting [A-Z] into numbers [0–25].



Encryption

The plaintext(P) and key(K) are added modulo 26.

$E_i = (P_i + K_i) \bmod 26$

Decryption

$D_i = (E_i - K_i + 26) \bmod 26$

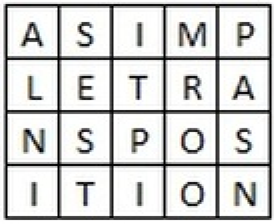
D_i denotes the offset of the i-th character of the plaintext. Like offset of **A** is 0 and of **B** is 1 and so on.

Transposition Cipher

A transposition cipher permutes the characters of the plaintext in fixed chunks of length d. 'f' is a permutation vector of size 'd'. The key for the cipher is given by the pair K = (d,f). Successive blocks of d characters are enciphered by permuting the characters according to f. Suppose that d = 4 and f (2413). This means that the first plaintext character is moved to the third position in the ciphertext, the second plaintext character to the first position, and so forth.

Columnar transposition

The Columnar Transposition Cipher is a form of transposition cipher. Columnar Transposition involves writing the plaintext out in rows, and then reading the ciphertext off in columns one by one. It builds in a keyword to order the way we read the columns, as well as to ascertain how many columns to use.



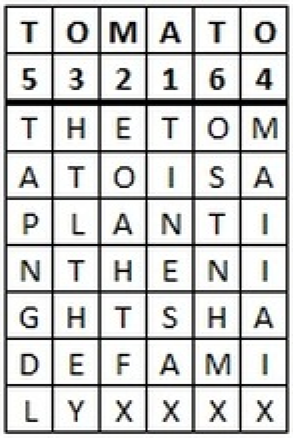
A	S	I	M	P
L	E	T	R	A
N	S	P	O	S
I	T	I	O	N

If we now read down each column we get the ciphertext "ALNISESTITPIMROOPASN"

Encryption

We first pick a keyword for our encryption. We write the plaintext out in a grid where the number of columns is the number of letters in the keyword. We then title each column with the respective letter from the keyword. We take the letters in the keyword in alphabetical order, and read down the columns in this order. If a letter is repeated, we do the one that appears first, then the next and so on.

As an example, let's encrypt the message "The tomato is a plant in the nightshade family" using the keyword tomato. We get the grid given below.



T	O	M	A	T	O
5	3	2	1	6	4
T	H	E	T	O	M
A	T	O	I	S	A
P	L	A	N	T	I
N	T	H	E	N	I
G	H	T	S	H	A
D	E	F	A	M	I
L	Y	X	X	X	X

The plaintext is written in a grid beneath the keyword.

The numbers represent the alphabetical order of the keyword, and so the order in which the columns will be read.

Note that, we have written the keyword above the grid of the plaintext, and also the numbers telling us which order to read the columns in. Notice that the first "O" is 3 and the second "O" is 4, and the same thing for the two "T"s.

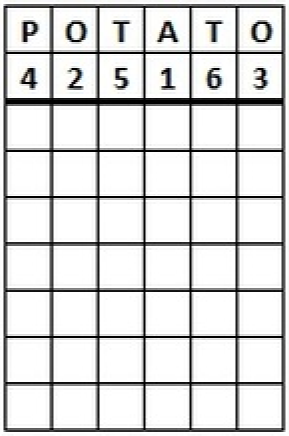
Starting with the column headed by "A", our ciphertext begins "TINESAX" from this column. We now move to the column headed by "M'', and so on through the letters of the keyword in alphabetical order to get the ciphertext “TINESAX / EOAHTFX / HTLTHEY / MAIIAIX / TAPNGDL / OSTNHMX” (where the / tells you where a new column starts). The final ciphertext is thus "TINES AXEOA HTFXH TLTHE YMAII AIXTA PNGDL OSTNH MX ”.

Decryption

The decryption process is significantly easier if nulls have been used to pad out the message in the encryption process.

Firstly, if nulls have been used, then you start by writing out the keyword and the alphabetical order of the letters of the keyword. You must then divide the length of the ciphertext by the length of the keyword. The answer to this is the number of rows you need to add to the grid. You then write the ciphertext down the first column until you reach the last row. The next letter becomes the first letter in the second column (by the alphabetical order of the keyword), and so on.

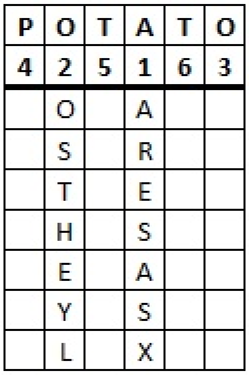
As an example, we shall decrypt the ciphertext "ARESA SXOST HEYLO IIAIE XPENG DLLTA HTFAX TENHM WX" given the keyword potato. We start by writing out the keyword and the order of the letters. There are 42 letters in the ciphertext, and the keyword has six letters, so we need 42 ÷ 6 = 7 rows.



P	O	T	A	T	O
4	2	5	1	6	3

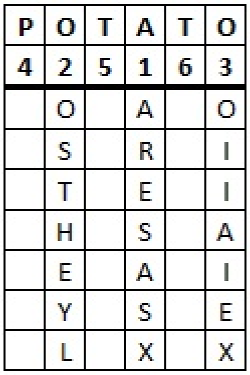
We have the keyword and the order of the letters in the keyword. We also know there are 7 rows.

Now we start by filling in the columns in the order given by the alphabetical order of the keyword, starting with the column headed by "A". After the first column is entered we have the grid shown to the right.We continue to add columns in the order specified by the keyword.



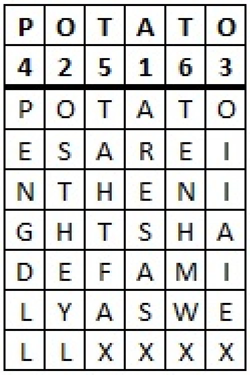
P	O	T	A	T	O
4	2	5	1	6	3
	O		A		
	S		R		
	T		E		
	H		S		
	E		A		
	Y		S		
	L		X		

After inserting the first column



P	O	T	A	T	O
4	2	5	1	6	3
	O		A		O
	S		R		I
	T		E		I
	H		S		A
	E		A		I
	Y		S		E
	L		X		X

After inserting the third column



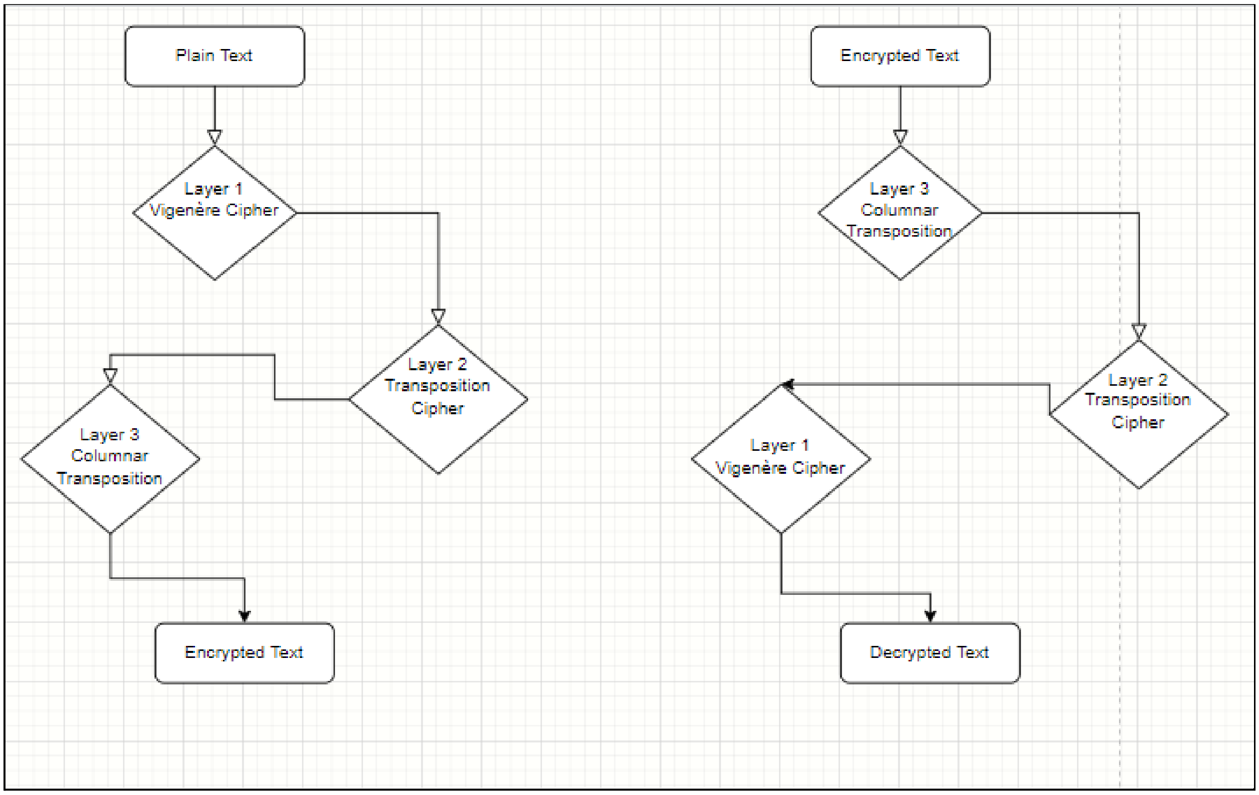
P	O	T	A	T	O
4	2	5	1	6	3
P	O	T	A	T	O
E	S	A	R	E	I
N	T	H	E	N	I
G	H	T	S	H	A
D	E	F	A	M	I
L	Y	A	S	W	E
L	L	X	X	X	X

The completely reconstructed grid

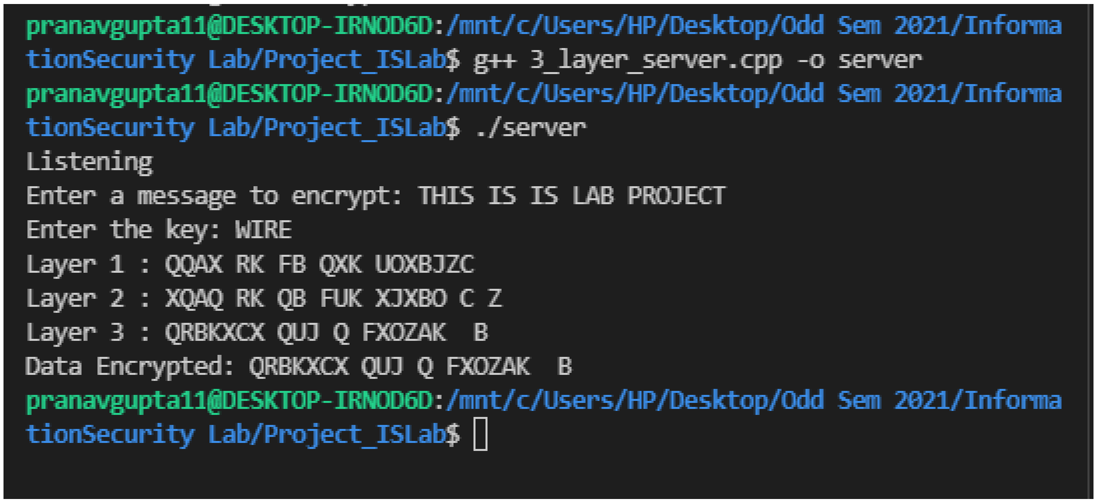
Now we read off the plaintext row at a time to get "potatoes are in the nightshade family as well".

When no nulls have been used we have to do a slightly different calculation. We divide the length of the ciphertext by the length of the keyword, but this is likely to not be a whole number. If this is the case, then we round the answer up to the next whole number. We then multiply this number by the length of the keyword, to find out how many boxes there are in total in the grid. Finally, we take the length of the ciphertext away from this answer. This number (which should be less than the length of the key) is how many nulls there would have been if used, so we need to black out these last few boxes, so we don't put letters in them whilst decrypting.

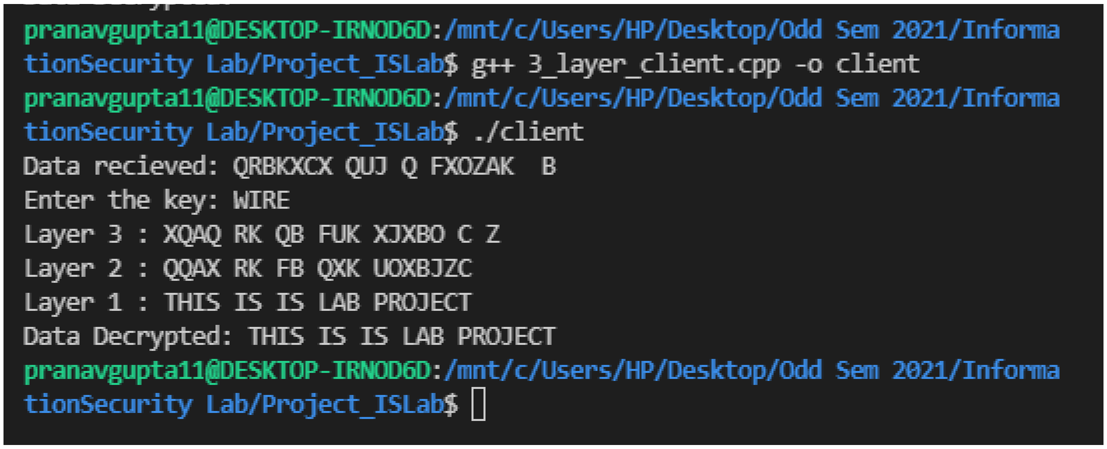
Flowchart


Plain Text
Layer 1 Vigenère Cipher
Layer 2 Transposition Cipher
Layer 3 Columnar Transposition
Encrypted Text
Encrypted Text
Layer 3 Columnar Transposition
Layer 2 Transposition Cipher
Layer 1 Vigenère Cipher
Decrypted Text

Screenshots



```
pranavgupta11@DESKTOP-IRNOD6D:/mnt/c/Users/HP/Desktop/Odd Sem 2021/Informa
tionSecurity Lab/Project_ISLab$ g++ 3_layer_server.cpp -o server
pranavgupta11@DESKTOP-IRNOD6D:/mnt/c/Users/HP/Desktop/Odd Sem 2021/Informa
tionSecurity Lab/Project_ISLab$ ./server
Listening
Enter a message to encrypt: THIS IS IS LAB PROJECT
Enter the key: WIRE
Layer 1 : QQAX RK FB QXK UOXBJZC
Layer 2 : XQAQ RK QB FUK XJXBO C Z
Layer 3 : QRBKXCX QUJ Q FXOZAK  B
Data Encrypted: QRBKXCX QUJ Q FXOZAK  B
pranavgupta11@DESKTOP-IRNOD6D:/mnt/c/Users/HP/Desktop/Odd Sem 2021/Informa
tionSecurity Lab/Project_ISLab$ 
```



```
pranavgupta11@DESKTOP-IRNOD6D:/mnt/c/Users/HP/Desktop/Odd Sem 2021/Informa
tionSecurity Lab/Project_ISLab$ g++ 3_layer_client.cpp -o client
pranavgupta11@DESKTOP-IRNOD6D:/mnt/c/Users/HP/Desktop/Odd Sem 2021/Informa
tionSecurity Lab/Project_ISLab$ ./client
Data recieved: QRBKXCX QUJ Q FXOZAK  B
Enter the key: WIRE
Layer 3 : XQAQ RK QB FUK XJXBO C Z
Layer 2 : QQAX RK FB QXK UOXBJZC
Layer 1 : THIS IS IS LAB PROJECT
Data Decrypted: THIS IS IS LAB PROJECT
pranavgupta11@DESKTOP-IRNOD6D:/mnt/c/Users/HP/Desktop/Odd Sem 2021/Informa
tionSecurity Lab/Project_ISLab$ 
```

Conclusion

Hence we have successfully decoded the plain text using three layers of safety protocols.

References

- Public Key Encryption - GeeksforGeeks
- Cryptography - Wikipedia
- Information security - Wikipedia
- Encrypted client-server communication (protection of privacy and integrity with AES and RSA in details) | by Weblab Technology | Medium
- Columnar Transposition Cipher - GeeksforGeeks