RESEARCH ARTICLE OPEN ACCESS

Securing ASP.NET Query String Data Transmission in Web Application Using Hybrid Encryption Technique

Vilas T Mahajan [1], Rajendra B Patil [2]
Department of Information Technology/ Computer Science [1]
VPM's R. Z. Shah College of Arts, Science and Commerce, Mulund (E), Mumbai-81
Department of Information Technology [2]
S. K. Somaiya Degree College of ArtsScience and Commerce, Vidyavihar (E), Mumbai-77
India

ABSTRACT
Cryptography, from the Greek word 'kryptos' (hidden) and 'graphein' (to write), is the art and science of making communication unintelligible to all except the intended recipients [1]. Security is omnipresent. With the advent of the Internet, the need of development of secured applications has been grown tremendously. Cryptography is the study of building cipher to ensure the confidentiality and integrity of information. This field of cryptography, known as cryptanalysis that ensures the ciphers are strong enough to defend against known form of attacks. Strong cryptographic algorithms are just one aspect, and in spite of their development, may not be useful for end-to-end security if not deployed properly. This paper shows the implementation of Caesar Cipher (Shift Cipher) combined Rail-fence encryption technique for transferring data over internet with ASP.NET and C# using.

Keywords:- Security, Encryption, Ciphers, Cryptography, State Management, QueryString from web-based threats, such as hackers, scams and malicious code.

I. INTRODUCTION

Digital world is spreading and changing at a tremendous speed. Internet allows us to transfer information from one place to another within a fraction of second. We should be aware that the technologies can leak or distort your message just as humans can. Internet data security is a major problem considering the pervasive impact of the Internet on nearly all the areas of computing industry. Systems used in home, education, business, government offices etc. are prone to the attack of being information stolen. There is a need to protect data from web-based threats, such as hackers, scams and malicious code.

This threat is depicted in the following Fig 1. [8].

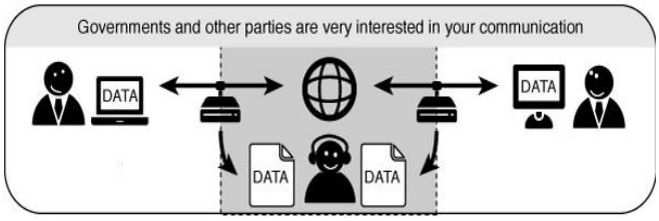

Fig. 1

This paper shows the building ASP.NET secured data transfer application using cryptography techniques.

II. LITERATURE SURVEY

Concepts related to the cryptography are introduced here in short:

a. Cryptography:

It is the art and science of protecting information from undesirable individuals i.e. intruders by converting it into a form non-recognizable by its attackers while stored and transmitted over the Internet [5]. In Cryptography, Caesar cipher is one of the most widely known encryption-decryption algorithm. Caesar cipher is a type of substitution cipher. In this kind of cipher each letter in the plaintext is replaced by a letter some fixed number of positions down the alphabet. The encryption is represented using modular arithmetic [6][3].

Encryption: It is a process by which we convert our data (plaintext) in no recognizable form (cypher-text).

Decryption: It is the process of converted encrypted text back into the original text.

Plain text: The original message to be encrypted.

Key: It is the object used to encrypt the plain text.

Cypher-text: The result of encryption on a plain text message. Cypher-text is not meaningful without having decrypted [4].

Cipher: The method of decryption and encryption is generally known as cipher.

b. Purposes of cryptography

Confidentiality: The principle of confidentiality specifies that only the sender and the intended recipient should be able to read (decode) the message.

Authentication: The authentication process verifies the origin or source of the message. It ensures that the origin of the message is correctly identified.

Integrity: Integrity allows the original contents to remain in the same state when it reaches to the intended recipient.

Non- repudiation: This method keeps proof of origin, receipt and contents. It does not allow the sender of a message to refute the claim of not sending the message.

Access Control: Access Control limits the entry to authorized users. It specifies and controls who can access what.[9]

C. Types of cryptographic algorithm

Secret Key Cryptography (SKC): It uses a single key which is known only to the parties that exchange the message. It is also called as symmetric encryption. Primarily used for privacy and confidentiality.

Public Key Cryptography (PKC): It uses two keys: a public key which is known to everyone and a private key which is known to the intended receiver only. It is also called as asymmetric encryption. Primarily used for authentication, non-repudiation, and key exchange.

Hash Functions: Uses a mathematical transformation (function) which takes an input and returns a hash values called as digital fingerprint or checksum or message digest or simply digest. Primarily used for message integrity. [10]

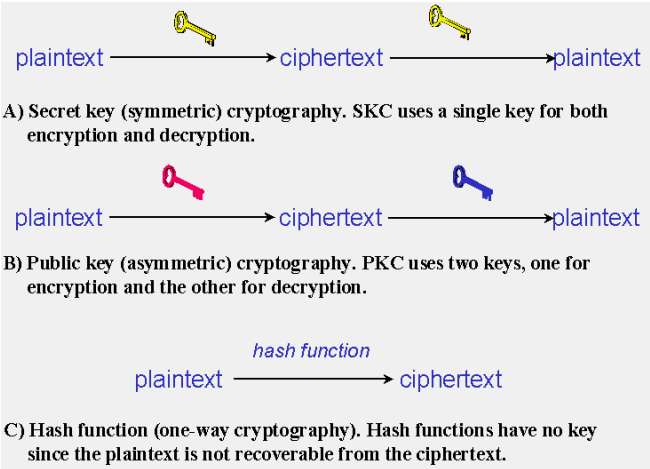

Fig. 2

Cryptography uses two techniques: Substitution technique and Transposition Technique

A. Substitution technique

Substitution cipher is a method of encoding by which units of plaintext are replaced with cipher-text, according to a fixed system; the "units" may be single letters (the most common), pairs of letters, triplets of letters, mixtures of the above, and so forth. Each letter retains its position but changes its identity. The receiver deciphers/decodes the text by performing the inverse substitution. [7]. Caesar Cipher is one of the substitution techniques.

Caesar Cipher:

A Cryptographic scheme proposed by Hulius Caesar is one special case of substitution cipher where each alphabet in the message is replaced by an alphabet, three places down the line, in the alphabetical order. Caesar cipher, also known as shift cipher, Caesar's cipher, Caesar's code or Caesar shift.

Thus "A" becomes "D" and "B" becomes "E"

Table 1 shows plain and cipher Text

Plain Text	A	B	C	D	E	F	G	H	I	J	K	L	M
Cipher Text	D	E	F	G	H	I	J	K	L	M	N	O	P

Plain Text	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Cipher Text	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Table.1

Caesar Cipher is very simple. But this simplicity comes with a cost. Obviously it is a very weak scheme.

Algorithm to break the Caesar Cipher:

1. Read each alphabet in the cipher text message, and search for it in the second row of the figure above.
2. When a math is found, replace that alphabet in the cipher text message with the corresponding alphabet in the same column but the first row of the table (eg. If the alphabet in cipher text is J, replace it with G).
3. Repeat the process for all alphabets in the cipher text message.

The process shown above will reveal the original plain text. Thus, given a cipher text message L ORYH BRX, it is easy to work backward and obtain the plain text I LOVE YOU as shown in table 2.

Plain Text	L	O	R	Y	H	B	R	X
Cipher Text	I	L	O	V	E	Y	O	U

Table 2

Caesar Cipher is good in theory, but not so good in practice.

B. Transposition technique:

Transposition technique differs from the substitution technique in the way that they do no simply replace one alphabet with another, but they also perform some permutation over a plain text. Each letter retains its identity but changes its position. Rail-fence is one of the Transposition techniques.

Rail-fence cipher:

Rail-fence technique involves writing plain text as a sequence of diagonal and then reading it row by row to produce cipher text.

Example: Original plain-text message: Do your homework

1. After we arrange the pain-text message as a sequence of diagonal, it wold look as follows(Write the first character on the first line i.e. D, then the second character on the second line i.e. o, then the third character on the third line i.e. y, then the forth character on the second line, i.e. and so on). This creates zigzag sequence as shown in Fig 3.

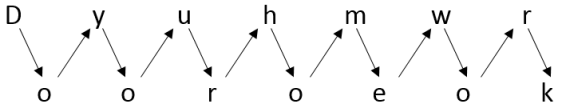

Fig. 3

2. Now read the text by row, and write it sequencially. Thus, we have dyuhmwrooroeok as the cipher-text.

What is state management in ASP.NET?

State management is the process by which you maintain state and page information over multiple requests for the same or different pages. [2]. HTTP is a stateless protocol. It does not retain the information during multiple requests for the pages in a website. Which means that the connection between client and server is lost once the transaction ends. State management enables maintain a state explicitly through coding. There are two types of state managements in ASP.NET as shown in Fig.3

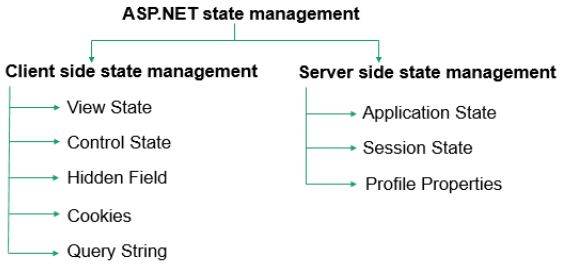

Fig. 3

Client – Side State Management

This stores information on the client's computer by embedding the information into a Web page, a uniform resource locator (url), or a cookie.

Query Strings

A query string is information that is appended to the end of a page URL. Querystring consists of the key and the value pairs. The key means the variable and the value means the data assigned to the key.

You can use a query string to submit data back to your page or to another page through the URL. Query strings provide a simple but limited way of maintaining some state information. For example, query strings are an easy way to pass information from one page to another, such as passing a product number to another page where it will be processed. [2]

Advantages of using query strings are:

- **No server resources are required**: The query string is contained in the HTTP request for a specific URLin the form of key and value pairs.
- **Widespread support:** Almost all browsers and client devices support using query strings to pass values.
- **Simple implementation:** ASP.NET provides full supports for transferring and extracting query string data.ASP.NET provides QueryString collection to extract the data that is sent from the user to the server.

Disadvantages of using query strings are:

Potential security risks: The information in the query string is directly visible to the user via the browser's user interface. A user can bookmark the URL or send the URL to other users, thereby passing the information in the query string along with it. Limited Data: Querystring can send limited data upto 255 characters.

Implementation with code:

Considering the potential risk passing the query string data, we have implemented combine encryption technique using Caesar Cipher and Rail-fence.

Proposed Technique with example:

Example: 1

A: Passing Encryption text

Step 1: Read the text to be sent on the internet

Example: **I will be sent on the Internet.**

Step 2: Apply Caesar Cipher Technique to get a first cipher-test.

Step 3: This first cipher-text will be treated as a plaintext to be given to the rail-fence algorithm. It will return resultant cipher-text as

Cipher text: **K"pvv0"ndgv"jpgvyngu"pgKtgk"q"p**

Therefore the resultant URL will look like:

http://localhost:4001/Implementation/ReadFromQueryString.aspx?Data=K%22pvv0%22ndgv%22jpgvyngu%22pgKtgk%22q%22p

fig.4 shows the screenshot with pain text which will be sent on the address of the browser as an encrypted string (cipher text)

Fig. 4

A: decryption of URL querystring

Step 1: Read the querystring from the URL
Example: K"pvv0"ndgv"jpgvyngu"pgKtgk"q"p
Step 2: Apply Caesar Cipher Technique to get a first decoded text.
Step 3: This first cipher-text will be treated as a plain-text to be given to the rail-fence decryption algorithm. It will return resultant plain text as
Plain text: I will be sent on the Internet.

Following fig.5 shows the screenshot with encrypted query string and corresponding decoded string:

Fig. 5

Example: 2
A: Passing Encryption text as shown in Fig. 6
Step 1: Read the text to be sent on the internet
Eample: **Khul-Jaa-Sim-Sim**

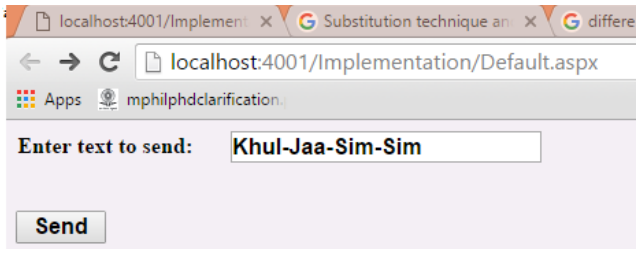

Fig. 6

Step 2: Apply Caesar Cipher Technique to get a first cipher-test.
Step 3: This first cipher-text will be treated as a plaintext to be given to the rail-fence algorithm. It will return resultant cipher-text as
Cipher text: **Mc/jLcoUw//kknUo**
Therefore the resultant URL will look as:
http://localhost:4001/Implementation/ReadFromQueryString.aspx?Data=Mc/jLcoUw//kknUo

B: decryption of URL querystring

Step 1: Read the querystring from the URL
Example: Data=Mc/jLcoUw//kknUo
Step 2: Apply Caesar Cipher Technique to get a first decoded text.
Step 3: This first cipher-text will be treated as a plain-text to be given to the rail-fence decryption algorithm. It will return resultant plain text as shown in Fig. 7
Plain text: **Khul-Jaa-Sim-Sim**

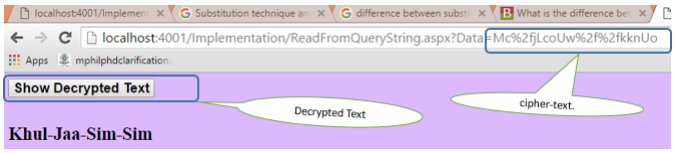

Fig. 7

III. CONCLUSIONS

In this paper, we have secured the state management technique using the combination Caesar Cipher encryption with Rail-fence encryption techniques. It shows that if we have a knowledge of cryptography in detail then we can develop secured ASP.Net application which passes data securely across the web pages over Internet.

The disadvantage of this method is that we can pass only limited characters that is the constraint imposed by web browsers. We can overcome this problem by compressing the text with the help of suitable compression algorithm.

REFERENCES

[1]. Luciano D. and Prichett G., "Cryptology: From Caeser Ciphers to Public-Key Cryptosystem", The College Mathematics Journal, vol 18, no 1, pp. 2 -17, 1987.
[2]. https://msdn.microsoft.com/en-us/library/z1hkazw7.aspx
[3]. Book-Cryptography and Network security, 3rd Edition, Fouroza, Mukhopadyaya-McGraw Hill Education.
[4]. AtulKahate, Cryptography and Network Security, 3rd Edition.
[5]. Hamdan.O.Alanazi, B.B.Zaidan and A.A.Zaidan, "New Comparative Study Between DES, 3DES and AES within Nine Factors", JOURNAL OF COMPUTING. Vol.2, Issue 3. Pp.152-157, MARCH, 2010.
[6]. S G Srikantaswamy, Dr. H D Phaneendra, "Improved Caesar Cipher with Random Number Generation Technique and Multistage Encryption", International Journal on Cryptography and Information Security (IJCIS). Vol. 2, No.4. pp. 39-49, December 2012.
[7]. https://en.wikipedia.org/wiki/Substitution_cipher

[8]. http://flossmanuals.net/basic-internet-security/

[9]. A Survey on Various Cryptography Techniques Mitali1 , Vijay Kumar2 and Arvind Sharma3, International Journal of Emerging Trends & Technology in Computer Science(IJETTCS) (Volume 3, Issue 4, July-August 2014, Page 307)

[10]. An Overview of Cryptography, Author-Gary C. Kessler (7 August 2016)