Analysis on HTML Encrypter

Ridhi Shah[*1], Rohan Bist[*2], Snehal Shinde[*3], Mrs. Archana Salaskar[#4]
[*] Student, Dept. of Computer Technology
[#]Lecturer,Dept. of Computer Technology
Shah & Anchor Kutchhi Polytechnic
Mumbai, India
shah.ridhi99@gmail.com[1], *rohanbist59@gmail.com*[2],
snehal199488@gmail.com[3], *archanasalaskar@gmail.com*[4]

Abstract:-In today's developing corporate world major role has played by business through internet and through social networking. People develop HTML websites for their business so that they can publish their content all over the world. By viewing the source code of that particular website or html file there are high risks of copying of codes of HTML. Preventive measures can be taken such as "Hiding" or "Encrypting" the HTML source code to overcome that problems so that one can read the code but cannot understand it & resources such as web content, images / files is easily hided by encrypting so one cannot make copy of it. This Html Encrypter does the same job. If someone goes for view source code of the website then he would be able to see the code but in encrypted format.

Keywords:-*Encryption, HTML, AES, DES, Data Security.*

*****

1. INTRODUCTION

As the world is moving toward the new era of online things where almost everything is done using website from reading of books by children to shopping by adults is interconnected with the Website, the very vital right of website privacy is being compromised. The business Website, Bank Website and many more Web pages that are the fundamental things of people in day to day life are been stolen and the integrity and confidentiality of the pages is lost. It is very important that the code of the website is kept secure and should not be known to anyone outside the intended ones. Encryption is well known and widely used technique that manipulates information (code) in order to encrypt or hide their existence. This technique have many applications in computer science and other related fields: they are used to protect military messages, personal files, credit card information, corporate data, Emails, etc. [12]

Encrypting the source code of the webpage would protect the code from losing its integrity and also allows the owner of the site to be safe and protective about their website.Hiding HTML source code from rippers, email extractors and content filters can be done using encrypting the source code.

Encryption is the process of encoding or hiding data or information in a way that only legitimate and authorized people can access or read it. Interception itselfis not prevented by encryption but it does deny the data to the interceptor. In encryption the data (source code) is encrypted using an encryption algorithm, generating the text that is in encrypted format and only read if decrypted.

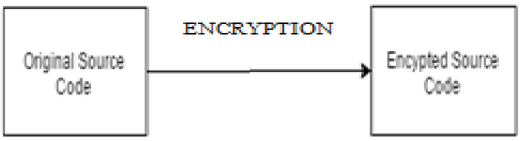

Figure 1. Flow of Encryption

Html encryption will hide the source code from many programs used by spammers, thieves and censors. If the code is protected, mass downloader's and site rippers will not be able to follow the links within the site and will not be able to download it. There are many dishonest webmasters and other people that download the entire sites of their successful competitors, and thenhave their site up and running in less than a day without any effort by just changing some images and texts. Encrypt code and secure all the other files. The images can also be protected on the site. Where the most common form of theft on the web page is commonly the Image theft. A lot of people look for this after having their website pirated or stolen. It's cruel that in a few minutes someone can steal hours of your work, but hiding your source code can help in many of that ways. After the source is encrypted using HTML Encrypter it can be hosted on sever using protocols but in encrypted format only so that when people view the source code the code may be visible but in encrypted form which may be readable but cannot be understandable.

2. BACKGROUND

In this proposed system a Website that is designed or developed fully with its source code is to be uploaded on the server then the HTML Encrypter is to be used to encrypt the source code which takes the input as original source code and generates the output as encrypted code.The Website source code should be html that is that the website should only be developed in html language. The system would be developed using Java language. The original source code could be encrypted in any one of the algorithm from AES and Blowfish. Both the algorithm does the same job of encryption but in different way. Many other algorithms can be used in this Encrypter to encrypt the source code such as, Blowfish, TEA, Rabbit, Escape, DES, Triple DES,etc. [7] The user has the ability to then upload that encrypted file on the server using FTP protocol or CSS and the encrypted source code is links, and graphics. In addition to encrypting the source code and making it impossible for people to read, Encrypt HTML.

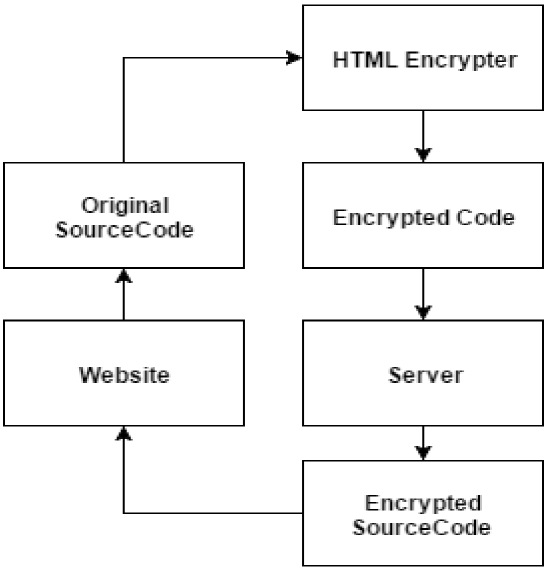

Figure 2. Flow of System

2.1 Encryption

HTML Encrypter allows you to encrypt HTML pages with strong encryption algorithms and protect them from email extractors and content filters. The basic HTML encryption worked quite well, and the code was adequately protected. Encrypted pages will have the same look as the original ones and can be viewed in all modern web browsers.The encryption algorithms used AES and Blowfish are all the new encryption algorithms where AES is Advanced Encryption algorithm is not yet been cracked by anyone and is considered to be the best till now and the Blowfish is the latest algorithm which is also considered to be the best. In the Encryption module the reason for using two algorithms is Blowfish is new so no risk can be taken if anyone can crack it but the AES is the one which is not been cracked yet and also is at its best.

3. LITERATURE SURVEY

3.1 Encrypt HTML Pro

Encrypt HTML Pro is an application to encrypt and protect your HTML pages in just a few clicks. It can prevent others from viewing and reusing your Web page source code, including HTML source code, JavaScript, VBScript, text,

3.1.1 Advantages

- The interface for this program is extremely easy to use, plenty of options, and is very quick.
- Encrypt HTML Pro also allows you publish your pages protected on removable media like CD, DVD, USB.

3.1.2 Disadvantages

- This software allegedly allows you to encrypt only parts of a page but this function does not work
- It is a an Expensive Software

3.2 HTML Guardian

HTML Guardian will encrypt your HTML, JavaScript, VBscript and ASP code and make impossible stealing and reusing it. It will protect your links from stealing and leeching, your images, applets, etc. Many additional protection options are available - you can disable right click, page printing, text selection or copying and offline usage of encrypted files. You can also add password protection and referrer check to them.

3.2.1 Advantages

- **Protection of Internet code:** The basic HTML encryption worked quite well, and the code was adequately protected.
- **Protection of files:** HTML Guardian can also protect other file types. For instance, you can choose to disable the right-click feature so that others can't right-click on your images to Save As.

3.2.2 Disadvantages

- **Outdated interface:** HTML Guardian looks out of date in the Windows 8.1 environment and is therefore harder to navigate for someone who is used to more modern navigation structures.
- **Complicated features:** The more advanced features are hard to access and complicated to use.
- Complicated for beginners.

3.3 HTML Encryption(Online)

Hide HTML source code from email extractors and content filters. HTML encryption will hide your source code from many programs used by thieves, spammers and censors. If your code is protected, site rippers and mass downloader’s will not be able to follow the links within your site and will not be able to download it.

There are many dishonest webmasters that download the entire sites of their successful competitors, just change some images and texts and have "their" site up and running in less than a day without any effort. Encrypt links and secure all other files. Encrypt JavaScript and VBscript source. Encrypt ASP code. Full website encryption with just a few clicks. Protect images on your site. Image theft is maybe the most common form of theft on the web.

3.3.1 Advantages

- Online website no need to install any software
- Free to use
- Encrypts any websites

3.3.2 Disadvantages

- Can't download the Encrypted file.
- NO decryption option.

4. COMPARISON

There are many Encryption algorithms which are developed and are used for information security. They are categorized into mainly two types depending upon the type of security keys. The two categories are symmetric and asymmetric encryptions. In symmetric or private encryption only one key is used to encrypt or decrypt the data. Strength of the symmetric encryption depends upon the size of the key. For the same algorithm, encryption using the longer key is tough to break than one using smaller key. In a symmetric or publicencryption two keys are used, one is used to encrypt and other is used to decrypt the data [6]. Brief definitions of the most common encryption techniques are given as follows:
AES is a block cipher .It has variable key length of 128, 192, or 256 bits; default 256. It encrypts data blocks of 128 bits in 10, 12 and 14 round depending on the key size. AES encryption is fast and flexible; it can be implemented on various platforms especially in small devices. Also, AES has been carefully tested for many security applications [8], [9].

DES: (Data Encryption Standard), was, recommended by NIST (National Institute of Standards and Technology) and was the first encryption standard. DES is (64 bits key size with 64 bits block size). Since that time, many attacks and methods recorded the weaknesses of DES, which made it an insecure block cipher [9], [10].

3DES is an enhancement of DES; it is 64 bit block size with 192 bits key size. In this standard the encryption method is similar to the one in the original DES but applied 3 times to increase the encryption level and the average safe time. It is aknown fact that 3DES is slower than other block cipher methods [9].

Blowfish is block cipher 64-bit block that can be used as a replacement for the DES algorithm. It takes a variable length key, ranging from 32 bits to 448 bits; default 128 bits. Blowfish is unpatented, license-free, and is available free for all users. Blowfish has variants of 14 rounds or less. Blowfish is successor to Twofish [1]. This paper is organized as follows: Related work has been presented in section 2, performance analysis of different encryption algorithm in section 3, study of Blowfish algorithm in section 4, Study of proposed algorithm to modify Blowfish using 4-states 5 and finally section 6 describes Conclusions and future scope.

Table 1: Comparison of DES, 3DES, AES and Blowfish algorithm [11]

Algorithm	Key Size	Block Size	Rounds	Cracked?
DES	56 bits	64 bits	16	Yes
TripleDES	112 bits or 168 bits	64 bits	48	No
AES (Rijndael)	128 bits, bits, 256 bits	128 Bits	10, 12 or 14	No
Blowfish	32-448 bit in steps of 8 bits. 128 bits default	64 bits	16	No

5. IMPLEMENTATION DETAILS

5.1 System Architecture

In this system when we need to give original source code od the website to the Encrypter system, that we need to provide security by the Encryption. During Encryption, the source code could either be encrypted using AES or Blowfish algorithm as per selected by the user, which will be generating the encrypted code. Further this encrypted code will be provided to upload or host it on server. As a result, the encrypted source code would be uploaded on server of the website.

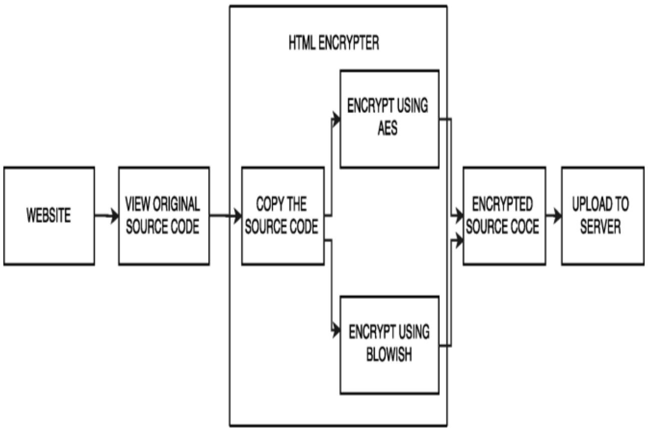

Figure 3. System Architecture

5.2 No. Of Models with explanantion

There are four modules in our project which are as follows:

5.2.1 WebDesign Module

This module is for creating a Website which will be general purpose Website. The website is to be created in clear and contextual language of HTML written and scripted along with additional plug ins and PHP and Java script support. The WebDesign module forms the basis of our project as that enables us to create our website which shall be put under the encryption process. The WebDesign module features simple, comprehensive and responsive website in HTML that can be access from any web browser. The WebDesign module is also responsible for the creation and the main design of the website that will allow the user to navigate through and better understand the project. WebDesign module makes use of simple and clean code to avoid confusion and improve implementation efficiency

5.2.2 Encryption with AES module

This module does the encryption of a HTML code. In this module the algorithm used for encrypting the source code is AES (Advanced Encryption System). AES encryption The AES algorithm operates on a 128-bit block of data and executed Nr - 1 loop times. The key length is 128, 192 or 256 bits in length respectively. The first and last rounds differ from other rounds in that there is an additional AddRoundKey transformation at the beginning of the first round and no MixCoulmns transformation is performed in the last round. In this paper, we use the key length of 128 bits (AES-128) as a model for general explanation. An outline of AES encryption[6].

5.2.3 Encryption with Blowfish module

This module does the encryption of a HTML code.In this module the algorithm used for encrypting the source code is Blowfish Algorithm. Blowfish is a symmetric encryption algorithm, meaning that it uses the same secret key toboth Encrypt and decrypt messages. Blowfish is also a block cipher [5], meaning that it dividesa message up into fixed length blocks during encryption and decryption. The block length for Blowfish is 64 bits; messages that aren't a multiple of eight bytes in size must be padded.

5.2.4 Uploading to Server module

This module does the work of uploading the Encrypted HTML source code on the server via FTP (File Transfer Protocol).And if the person views the source code of that website then they cant see the HTML code but the Encrypted code which would be readable but not understandable.

First the website will be created with the HTML language, and when whole of the website making is done the source code is viewed this would be the original source code viewed .That original code will be copied in the text box and encrypt the code.

During Encryption phase, the original source code will be supplied to the Encryption module for the process of Encryption. In the Encryption process the user will be getting two options to choose the Algorithm by which the encryption would be processed. After the Encryption process, the Encrypted code will be uploaded on the server through FTP protocol[2]. As a result, the Encrypted source code will be uploaded on the server.

5.3 Algorithm

5.3.1 Algorithm for basic system

Step 1: Right click on website
Step 2: Chose view page source from the drop down menu.
Step 3: Select the original source code.
Step 4: Copy the source code.
Step 5: Past the source code in the HTML Encrypter text box.
Step 6: Chose the algorithm with, which you want to encrypt the code.
Step 7: Click on encrypt button.
Step 8: Give the output as encrypted code.
Step 9: Upload the encrypted file on the server.
Step 10: Stop

5.3.2 Algorithm for AES Encryption

Step 1: SubBytes Transformation:

The SubBytes transformation is a non-linear byte substitution, operating on each of the state bytes independently. The SubBytes transformation is done using a once-precalculated substitution table called S-box. That S-box table contains 256 numbers (from 0 to 255) and their corresponding resulting values. This approach has the significant advantage of performing the S-box computation in a single clock cycle, thus reducing the latency and avoids complexity of hardware implementation.

Step 2: ShiftRows Transformation:

In ShiftRows transformation, the rows of the state are cyclically left shifted over different offsets. Row 0 is not shifted; row 1 is shifted one byte to the left; row 2 is shifted two bytes to the left and row 3 is shifted three bytes to the left.

Step3: MixColumns Transformation:

In MixColumns transformation, the columns of the state are considered as polynomials over GF (28) and multiplied by modulo x4 + 1 with a fixed polynomial c(x), given by: c(x)={03}x3 + {01}x2 + {01}x + {02}.

Step 4: AddRoundKey Transformation:

In the AddRoundKey transformation, a Round Key is added to the State - resulted from the operation of the MixColumns transformation - by a simple bitwise XOR operation. The RoundKey of each round is derived from the main key using the KeyExpansion algorithm. The encryption/ decryption algorithm needs eleven 128-bit RoundKey, which are denoted RoundKey[0] RoundKey[2].

5.3.3 Algorithm for Blowfish Encryption

Step 1: Key Expansion

The first step in the algorithm is to break the original key into a set of subkeys. Specifically, a key of no more than 448 bits is separated into 4168 bytes. There is a P-array and four 32-bit S-boxes. The P-array contains 18 32-bit subkeys, while each S-box contains 256 entries.The following steps are used to calculate the subkeys:

1. Initialize the P-array and S-boxes
2. XOR P-array with the key bits. For example, P1 XOR (first 32 bits of key), P2 XOR (second 32 bits of key), ...
3. Use the above method to encrypt the all-zero string
4. This new output is now P1 and P2
5. Encrypt the new P1 and P2 with the modified subkeys
6. This new output is now P3 and P4
7. Repeat 521 times in order to calculate new subkeys for the P-array and the four S-boxes

Step 2: encryption using blowfish algorithm

```
1. Begin
2. x/2=xL&xR
3. xL=xL XOR Pi ; xR=F(xL) XOR xR
4. swap xL and xR
5. IF i<16 go to step 3
6. ELSE swap xL and xR
7. xR=xR XOR P17 ; xL=xL XOR P18
8. Recombine xL and xR
9. End
```

The Function F explained

```
1. Begin
2. xL/(4) = a,b,c,d ; where a,b,c,d are 8-bit quarters
3. F(xL)=((S1,a+S2, b mod 232) XOR S3,c)+S4,d mod 232
4. End [1].
```

6. OBSERVATIONS

The purpose implementation of HTML Encrypter will provide a robust and high level of security for the website source code using the encryption algorithms. Analysis and survey done for our project which is presented here shows that HTML Encrypter will establish a highly impenetrable layer of security which will provide security and privacy for the foreseeable future of the website to be the original one. This provides a strong security for the website without any changes in the website design which remain according to code written for each part of the website. And provide the one of the best way suitable for the integrity and the originality on the website and the option for further implementation of new ideas related to web designing.

7. REFERENCES

[1] Bruce Schneier, “Applied Cryptography”, John Wiley & Sons, Inc. 1996

[2] Jawahar Thakur, Nagesh Kumar,“DES,AES andBlowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis,“ in International Journal of Emerging Technology and Advanced Engineering (ISSN 2250-2459, Volume 1, Issue 2, December 2011), pp.6-12

[3] http://cryptolearning.blogspot.in/2013/01/explanation-of-blowfish-encryption.html

[4] .https://en.wikipedia.org/wiki

[5] Orhun Kara and Cevat Manap (March 2007). "A New Class of Weak Keys for Blowfish" (PDF). FSE 2007

[6] Hoang Trang and Nguyen Van Loi HoChiMinh City, VietNam- “An efficient FPGA implementation of the Advanced Encryption Standard algorithm”(IEEE.2012).

[7] http://sourceforge.net/projects/htmlencrypte

[8] Daemen, J., and Rijmen, V. "Rijndael: The Advanced Encryption Standard."Dr. Dobb's Journal, March 2001, PP. 137-139.

[9] W.Stallings, "Cryptography and Network Security 4th Ed," Prentice Hall, 2005, PP. 58-309.

[10] Coppersmith, D. "The Data Encryption Standard (DES) and Its Strength against Attacks."IBM Journal of Research and Development, May 1994, pp. 243 -250

[11] Nagesh Kumar, Jawahar Thakur, Arvind Kalia on “PERFORMANCE ANALYSIS OF SYMMETRIC KEY CRYPTOGRAPHY ALGORITHMS:DES , AES and BLOWFISH “ in AnInternational Journal of Engineering Sciences ISSN: 2229-6913 Issue Sept 2011, Vol. 4 ,pp.28-37

[12] ”Two new approaches for secured image steganography using cryptographic techniques & type conversions” by Sujay Narayana and Gaurav Prasad published at Signal and Image processing: an international journal(SIPIJ) Volume 1, No.2 December 2010.