Web Page Encryption using PKCS

Myo Myint Aung
University of Computer Studies, Mandalay
theplutomma@gmail.com

ABSTRACT

A lot of system has been developed with security feature. This paper describes the cryptography techniques in Web Page. The browser will interpret by HTML commands and tags for display Web Page. In this paper, Web Page encryption system using is purposed.

The system provides for a client user to security and privacy in which to safety downloads and send to other user. Web page can take to secure and protect for the bug guys that are transform it into a bunch of number known as ciphertext in a particular cryptography and to disguise of their Web Page.

Web Page Encryption a batch process software to encrypt and protect HTML files, web pages, web site. This is a useful tool for web Developers, Author, Designer, Web site Programmer to guard and protect their new html techniques and resources or any part of the web pages, defend unauthorized web copy, protect unique and professional web site page style, html manner; Pass web content Filter.

In this paper, independent and support of Microsoft Internet Explorer and then the program source code of HTML structure encrypts using PKCS of NTRU Algorithm.

1. INTRODUCTION

During the past year, the increasing use of internet for commercial transactions and the growing potential communication around the world created new demands for security of exchanging private information over a non-secure channel. A network like the Internet is not a secure channel unless we use a cryptosystem.

Web Page Security depends on details of standards, that are likely to change and implement of user choices Encrypts Saving in a computer with Web Browser. The system is to reversing the transformation. By using the system, to disguise our data so that eavesdropper gain no information and allows us to create an unforgivable message and detect if it has been modified in transit.

Developers, Author, Designer, Web site Programmer to guard and protect their Web site, new html techniques or resources or any part of the web pages, defend unauthorized web copy, prevent unwanted files(pictures, movies, texts, images, links, etc.) download from web , protect unique and professional web site page style, html manner; pass File content Filter or Fire Wall to bring huge number visitors.

2. RELATED WORK

Some people are believe that keeping a cryptography system as secret as possible will enhance its Security of their Web Page.

Web Page Encryption based on [1] showed the key aspects of Basic NTRU Algorithm and some enhancement for speed optimization Implementation & Analysis. The project implemented the NTRU Algorithm including some enhancement suggested by NTRU Cryptosystem. The test showed that the most time consuming part of NTRU algorithm is polynomial multiplication. The parameters we used are obtained by trial and denial method. The analysis of the effects of different parameters on the accuracy and efficiency of NTRU algorithm will be a good subject for a future study.

"NTRU [2]: A Ring Base Public Key Cryptosystem", in Algorithmic Number theory Third international Symposium (ANTS3) in convenient to make a judgment unless analyzing the security aspects of this theory. MSDN Library

[4] is concepts of paper generated to useable for internet user.

3. PKCS

Public Key Cryptography Standard is more appropriate than symmetric key cryptosystems for security purposes. Public key methods are very powerful and give us much more flexibility. However this flexibility comes at a computational cost. The amount of computation needed in public key systems is several orders of magnitude more than the amount of computation needed in symmetric key systems such as DES. For this reason, public key cryptography is used in applications where only small amount of data must be processed. There has been significant effort for the creation of computationally inexpensive public key cryptosystems [1].

3.1 Public-Key Encryption

Public-key encryption uses a private key that must be kept secret from unauthorized users and a public key that can be made public to anyone. The public key and the private key are mathematically linked; data that is encrypted with the public key can be decrypted only with the private key, and data that is signed with the private key can be verified only with the public key. The public key can be made available to anyone; it is used for encrypting data to be sent to the keeper of the private key. Public-key cryptographic algorithms are also known as asymmetric algorithms because one key is required to encrypt data, and another key is required to decrypt data. Both keys should be unique for each communication session. However, although this requirement is true for symmetric algorithms, in practice, asymmetric keys are generally long-lived [3].

3.2 NTRU

NTRU is a relatively new, ring based cryptosystem that is claimed to be more efficient than the conventional public key algorithms such as RSA. The NTRU algorithm uses a mixing system based on polynomial algebra and reduction modulo two numbers p and q. Its validity depends on elementary probability theory. The reason of the security of NTRU is difficulty of finding extremely short vectors for most lattices.
Encryption and decryption processes are extremely fast and key creation is fast and easy. The time complexity of encryption and decryption is $O(N^2)$, where N is the length of the message block. This complexity is much better than that of RSA, which requires $O(N^3)$ operations [5].

3.3 NTRU Algorithm

The NTRU algorithm is officially described in [1]. It depends on 3 integer parameters (N,p,q), where N is a prime integer, p and q are relatively prime integers and q is larger than p.

NTRU uses polynomial addition and multiplication in the ring $R = Z[x] / (x^N – 1)$. Any polynomial f in R is written as a vector

$$f = \sum_{i=0}^{N-1} F_i x^i = [F_0, F_1, \dots , F_{N-1}]$$

The addition used by NTRU is regular polynomial or vector addition. However the multiplication is not regular polynomial multiplication. It is given as a cyclic convolution product and denoted as $\otimes$.

$$F \otimes G = H \quad \text{with}$$

$$H_k = \sum_{i=0}^{k} F_i G_{k-i} + \sum_{i=k+1}^{N-1} F_i G_{N+k-i}$$

NTRU uses 4 sets L_f, L_g, L_r, L_m of polynomials of degree N-1 with integer coefficients. All these sets contain small polynomials. “Small” polynomial is a polynomial with coefficients close to zero [6].

3.4 Key Creation

To create public and private keys, 2 small polynomials f and g are randomly chosen from the sets L_f and L_g respectively. The polynomial f must have inverses modulo p and modulo q, denoted as F_p and F_q.

$$F_p \otimes f \equiv 1 \pmod p \quad \text{and} \quad F_q \otimes f \equiv 1 \pmod q$$

Then the polynomials f and F_p are the private keys. And the polynomial h, given by

$h \equiv p \otimes F_q \otimes g \pmod q$ is the public key.

3.5 Encryption

The message m must be a polynomial from the set L_m . To encrypt m, a random polynomial r is chosen from the set L_r . Then the encrypted message e is the polynomial computed by

$$e \equiv r \otimes h + m \pmod q$$

where h is the public key.

3.6 Decryption

To decrypt e, the polynomial a is computed first

$$a \equiv f \otimes e \pmod q$$

The coefficients of a must be chosen from the interval [-q/2, q/2]. Then the original message can be computed by

$$m \equiv F_p \otimes a \pmod q)$$

Table 1 . Different implementations of NTRU

Parameters	Moderate Security	High Security	Highest Security
N	107	167	503
Q	64	128	256
P	3	3	3
L_f	L(15,14)	L(61,60)	L(216, 215)
L_g	L(12,12)	L(20,20)	L(72,72)
L_r	L(5,5)	L(18,18)	L(55,55)

4. CRYPTOGRAPHY FOR WEB

Cryptography helps protect data from being viewed, provides ways to detect whether data has been modified, and helps provide a secure means of communication over otherwise nonsecure channels. For example, data can be encrypted by using a cryptographic algorithm, transmitted in an encrypted state, and later decrypted by the intended party. If a third party intercepts the encrypted data, it will be difficult to decipher.

This overview provides a synopsis of the encryption methods and practices supported by the .NET Framework, including the ClickOnce manifests, Suite B, and Cryptography Next Generation (CNG) support provided by the .NET Framework version 3.5 [4].

4.1. Encryption And Decryption Data

To encrypt and decrypt data, that must use a key with an encryption algorithm that performs a transformation on the data. The .NET Framework provides several classes that enable to perform cryptographic transformations on data using several standard algorithms. This section describes how to create and manage keys and how to encrypt and decrypt data using public-key and secret-key algorithms.

The System.Security.Cryptography namespace contains classes that allow to perform both symmetric and asymmetric cryptography, create hashes, and provide random number generation. Successful cryptography is the result of combining these tasks. This section describes the key cryptographic tasks that can perform to create a cryptographic scheme [2].

4.2 Creating Rights -Managed HTML Files

This topic describes how to create a rights-managed HTML file. A rights-managed HTML file is a compound file that contains MIME Encapsulation of Aggregate HTML Documents (MHTML) content that has been encrypted with Microsoft Windows Rights Management (RM) technology and optionally compressed. Access to the unencrypted content is managed by the Rights Management Add-on for Internet Explorer or other client software, so that only the intended recipient can view, print, or otherwise interact with the MHTML content in its original format [4].

To create a rights-managed HTML file from MHTML content, complete the following steps.

- Compress the MHTML Content
- Encrypt the MHTML Content
- Store the Encrypted Content
- Write the Data Spaces Storage
- Compress the Resulting Compound File

4.2.1 Compress the MHTML Content

Compressing the MHTML content is an optional step that can reduce the overall size of the resulting rights-managed HTML file. If content is compressed, compression should be done prior to encryption. After encryption, the data cannot be compressed as efficiently as it can before compressing the content, add a storage under transforminfo and an entry in the data space map stream that refers to the new storage.

Note Content compressed with this compression transform must use a compression level of 9, and a window size of 32768 bytes.

Then, compress the content. The rights-managed HTML format supports the compression method used in zlib. The zlib public library is available.

For compressed streams in the rights-managed HTML format, the uncompressed content is divided into segments of 4096 bytes. Each block of the compressed stream contains the following:

Table 2 . Description of Type and Name

Type	**Name**	**Description**
ULONG	marker	Must be 0x0FA0.
ULONG	OriginalSize	Size of the uncompressed data. Usually 4096. The last block may be less.
ULONG	CompressedSize	The size of the compressed data.
BYTE[]	CompressedData	The compressed data segment.

4.2.2 Encrypt the MHTML Content

Encrypt the MHTML content, or the compressed MHTML content, using the RM client software development kit (SDK). In addition to the encrypted content itself, maintain references to the signed issuance license and the content owner's end-user license. Both of these are used when creating the data spaces storage.

4.2.3 Store the Encrypted Content

Place the encrypted MHTML content in a **stream** in the root **storage** of the compound file. This stream must be named `\0x09DRMViewerContent`.

Note Rights-managed HTML that references external script or behaviors is not supported.

4.2.4 Write the Data Spaces Storage

Write the data spaces storage as described in Data Spaces Structure for Rights-Managed Content.

The signed issuance license must be stored in the primary stream for the encryption transform definition.

Optionally, one or more end-user licenses can be placed in streams in the encryption transform definition storage. Typically, the end-user license for the content owner is stored here.

The data space map stream must include an entry that maps a data space to the `\0x09DRMViewerContent` stream.

4.2.5 Compress the Resulting Compound File

The final step is to compress the resulting compound file with the compression method used in zlib (library available **http://www.gzip.org**).

This is an optional step that can help reduce the overhead associated with storing data in a compound file. Even if compress the MHTML content before Encryption, can still recognize a reduced file size by compressing the compound file.

Note Content compressed with this compression transform must use a compression level of 9, and a window size of 32768 bytes.

The uncompressed compound file is divided into segments of 4096 bytes. Each block of the compressed stream contains the following:

4.3 EncryptedData Object

The **EncryptedData** object provides properties and methods to encrypt and decrypt data using a *session key* derived from a ecret.**Note** CAPICOM does not support the PKCS #7 EncryptedData content type but uses a nonstandard ASN structure for **EncryptedData**. Therefore, only CAPICOM can decrypt a CAPICOM **EncryptedData** object.

Table 3 . The EncryptedData object defines the following methods.

Method	Description
Decrypt	Decrypts encrypted content using the secret.
Encrypt	Encrypts the content using the current secret and encryption algorithm.
SetSecret	Sets the secret from which the encryption/decryption session key is derived.

Properties

The **EncryptedData** object has the following properties.

Algorithm

Data type: **Algorithm**
Access type: Read-only
Algorithm used for encryption/decryption.

Content

Data type: **String**
Access type: Read/write
The content to be encrypted or decrypted. Setting this property must be done before the **Encrypt** method is called.

When the value of this property is reset, directly or indirectly, the whole *state* of the object is reset, and any encrypted content in the object is lost.

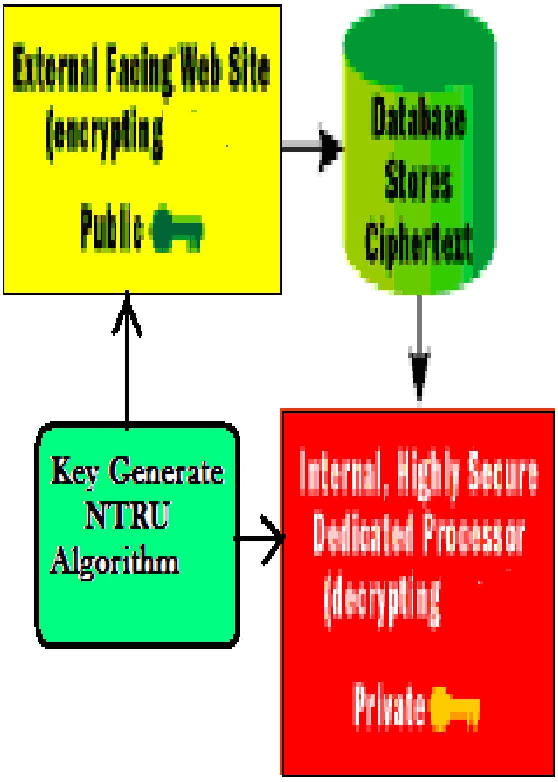

Figure 1. Encryption Method of NTRU

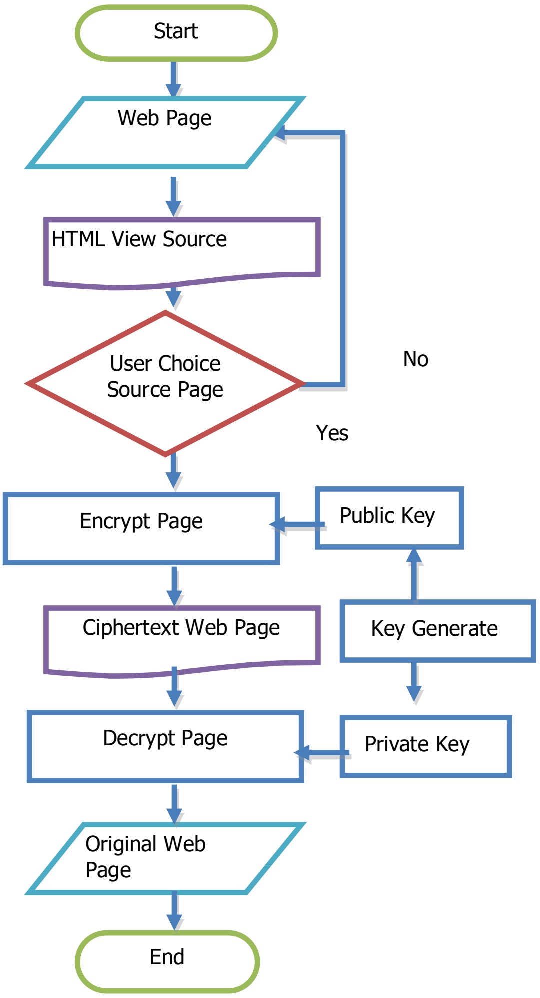

Figure 2 . System Design of Encryption

5. System Evaluation

The NTRU Algorithm are determines the status of a security patch by evaluating the presence of specific registry keys, file versions, and file checksums that are associated with a specific update. By default, NTRU receives the patch detection information from the Mssecure.html file. In some cases, to detect a patch browser can only search for specific registry keys.

Advantages of Web Page Encryption is protect the bag guys and secure for every Web Page, to disguise of data that eavesdroppers gain no information and allows us to create an unforgivable message and detect if it has been modified in transit.

Developers, Author, Designer, Web site Programmer to guard and protect their Web site, new html techniques or resources or any part of the web pages, defend unauthorized web copy, prevent unwanted files(pictures, movies, texts, images, links, etc.) download from web , protect unique and professional web site page style, html manner; pass File content Filter or Fire Wall to bring huge number visitors.

In this paper that describes to transfer cache and can take to secure with the Web Page Encryption System. In network security PKCS are suitable for user safely download and send to other client or server.

Both the whole connection of web browser and element of detailed structure can be Encrypt must we tried to next generation.

6. CONCLUSION

This system can be Encrypted one page in browser of active server page. If can be Encrypt of link list or other communication are not Encrypt. In this system that describes to transfer cache and can take to secure with the Web Page Encryption System. In network security PKCS are suitable for user safely download and send to other client or server.

REFERENCES

[1] Dr. Cetin Kaya Koc
Basic NTRU Algorithm and some enhancements for speed optimization Implementation & Analysis "Project ECE 575" Winter 2003

[2] J,Hoffstein, J.Pipper, and J,H.Silverman,
"NTRU: A Ring Base Public Key Crypto
System", in Algorithmic Number theory
: Third International Symposium (ANTS3).

[3] Wei Ren, NRTU Cryptography Public Key Cryptosystem , Department of Electrical and Computer Engineering University of Nevada, Las Vegas

[4] MSDN Library