

Forum:[Hack Forums](#)

Thread: [\[TUT\]Web cryptography part 1\[TUT\]](#)

theAbsolute - October 26, 2012, 12:17 pm

Web Cryptography

In this tutorial I will try to introduce you to web cryptography, that's why it's in php section. Also in later tutorials I will use php to handle data crypting.

p.s. English grammar correction would be of use, so if anybody is interested to correct my mistakes, that would be great.

Term and use

Term cryptography is originated from the Greek word "kriptos" which means "hidden" and the verb "grapho" which means "write".

It goals presents transformation of data into unrecognizable form, with the possibility of returning to the initial state

using various mathematical operations.

Little bit of history

If you are lazy, you can skip this part, but it's good to know this, why not.

Cryptography is not young like it could seems at first. People used to use the safe ways of sending information.

First crypted data is found in Egypt than we find similar technique in Bible known as Atbash.

Julie Cesar also had crypted language, and so many other examples which leads us to modern time, and using crypted messages during wars, WW2 for example.

Now we got to 20th century and computer age. First crypting system is developed by IBM in seventies. It was really gold in that time.

Like you can imagine, than people started making algorithms and developing this system more and more. Their system was called Lucifer and method DES (Data Encryption Standard).

In 1984. USENET group made rot13 system. Main goal of this system was to hide content from child abuse.

1990. leads us in Switzerland and new system called IDEA (International Data Encryption Algorithm), which had intention to change DES.

1991. is important because of first PGP (Pretty Good Privacy) scripts which had goal to crypt important data and email messages.

They used RSA algorithm which is most commercial nowadays.

Crypting depends of computer speed, so it's developing as fast as computer standards.

Opposite of crypting, we have decrypting technologies, most known as brute forcing.

Techniques

In this part of tutorial we will see how some techniques work as well.

Tips:

- You need to have control of your crypting data, and be informed if you face unauthorized crypting

of your own data.

- Crypted data security. When you crypted your data, you need to be sure just authorized pesons can view that data.

- Inability to avoid unauthorized access of encrypted data.

At the present time, this is a very important condition that a cryptographic method must meet.

One reason is the large number of financial transactions that are conducted through the Internet.

Symmetric crypting methods

This method use same key for crypting and decrypting data. It's lighter method if you like, so because it's not really secure, it's used only for personal purposes.

Sequential encryption system

Sequential data encryption methods are based on the use of mathematical and logical operations XOR (exclusive OR), and fall under the so-called. symmetric encryption methods.

Block encryption

Block encryption as a subset of symmetric encryption methods is an algorithm where the data is sent in groups of two or more elements (blocks of data).

The best known representatives of this type of data encryption algorithms are Lucifer, DES, IDEA, Blowfish, Twofish, and others.

Asymmetric encryption methods

Unlike Symmetric encryption method, which uses the same key to encrypt and decrypt data, for asymmetric encryption methods used techniques of private and public keys.

Hash encryption methods

This is the one you faced if you ever worked with passwords I think.

Hash algorithms, provide verification of identity decrypted data and original data. The most famous Hash algorithms are SHA-1, MD5, RIPEMD-160, and others.

Digital Signatures

Digital signatures allow the authenticity of the received material, as well as guaranteeing the identity of the sender.

A digital signature, in many countries, has validity in court. Any serious email program, and word processor has the option of signing personal digital signature.

I will continue writing in this field, so you can expect more practice work in next parts of tutorials.

Dogs Toy - October 26, 2012, 5:22 pm

Interesting read, although most seems like common sense

alphabot - October 26, 2012, 5:40 pm

Would you say mcrypt() is secure with the cipher rijndael-256?

razem - October 28, 2012, 1:05 pm

This was pretty interesting. Thanks, OP.

