

Forum:[Hack Forums](#)

Thread: [\[ILLUMINATI\] Understanding Cryptography \[TUTORIAL\]](#)

Cyber-Security - November 6, 2012, 1:08 pm

[img]http://gxf.net/images/2012/08/15/a1zIC.gif[/img]

Understanding Cryptography

What is Cryptography?

Cryptography is basically the practice of encoding and decoding messages. The whole point of cryptography is that you don't want your message seen by other eyes, so you encrypt it. Only the person with the decoding algorithm can bring the message back to its original form. A lot of people believe that cryptography is the art of "FUD Crypters" which is not true. This thread will be used to shine some light on what cryptography actually is and how you can get started with this interesting skill.

Cryptography in History

Believe it or not, good cryptography has been the turning point of wars. First, in the ancient times to the times of the colonization, cryptography was not as wide spread. The lords who demanded the use of cryptography in all their military based messages were the ones that usually won. Henry II of France used his own cipher, the french cipher. This cipher was made up of symbols around circles which ended creating a very complex and hard to break method. Here is the actual cipher machine:

As history progressed into the world wars, computers were already in their primitive stages. Since the messages were not physical but sent using electric signals, the snatching of data was a very real and very serious threat. During WWII, Great Britain built a computer called Colossus and it deciphered messages sent from the German's Lorenz SZ40/42 machine. Imagine knowing exactly what the enemy is thinking and about to do, that seriously can win wars.

[img]http://upload.wikimedia.org/wikipedia/commons/thumb/4/4b/Colossus.jpg/300px-Colossus.jpg[/img]

Now as cryptography was used more and more, numerous ciphers were built. In other words, more and more advanced ciphers were being created as the technology in the world grew. IBM was a forerunner in this practice, and eventually the US Data Encryption Standard was created. This encryption standard coupled with many more, are still used to this very day. Every password you have on sites, all the personal info you have entered on internet websites are most likely protected by different encryption methods, mainly to keep hackers out.

Types of Cryptography Symmetric Cryptography

Also known as Private Key Cryptography, this form of cryptography involves only one key. The sender encrypts the message and then the receiver uses the exact same copy of the key to decrypt it. The key has the ability to both encrypt and decrypt messages. This can cause security issues if someone else has a copy of the key.

Private Key Cryptography

This form of cryptography uses two different keys. One to encrypt the data and one to decrypt it. One of these keys are secret and one of them are public. This form of cryptography is used in your emails.

[img]http://upload.wikimedia.org/wikipedia/commons/thumb/1/1e/Public_key_signing.svg/250px-Public_key_signing.svg.png[/img]

Cryptologists

This is the point in which cryptography becomes a job, a very important one. A cryptologist's job is to convert, store, locate and retrieve documents, and data. Although you may think that this is a very useless job because you've never heard of it, you may be wrong. Take the next world war for example. WWI was the chemists war, it was fought using gas for the most part. WWII was the physicists war; the atomic bomb was what ended it all. WWII will be the mathematicians war; a war for information. This information will be protected by cryptologists, and whichever country has the best group of them will win.

Terminology

Note: This terminology is a direct excerpt from this trusted source:

<https://www.efa.org.au/Issues/Crypto/crypto5.html>

Asymmetric Algorithm

An algorithm in which the key used for encryption is different from that used for decryption. Also known as public key cryptography.

Block Cipher

An algorithm that encrypts data in blocks, commonly of 64 bits each.

CAST

A 64-bit block cipher, developed in Canada by Carlisle Adams and Stafford Tavares.

Cipher

A cryptographic algorithm, i.e. a mathematical function used for encryption and decryption.

Clipper

Originally the name for a tamper-resistant encryption chip designed by the U.S. National Security Agency for voice encryption. The chip has built-in key escrow features to facilitate wire-tapping. The term has subsequently been applied to further attempts by the US government to introduce key escrow provisions, the latest variation being the key recovery plan of October 1996, dubbed Clipper 4.

DES

Digital Encryption Standard. A symmetric block cipher using a 56-bit key which was originally developed by the US National Institute of Standards and Technology (NIST) in 1977 as a standard encryption algorithm. In 1999, the Electronic Frontier Foundation (USA) developed a machine to demonstrate that DES could be broken in a few hours with a brute-force attack. Encryption using single DES is generally no longer considered to be secure. (See Triple DES)

Diffie-Hellman

A public-key algorithm, invented in 1976.

DH/DSS

A type of key used in PGP since version 5.0. Contains a Diffie-Hellman key of between 1024 and 4096 bits for encryption and a 1024-bit DSS key for digital signatures.

DSS

Digital Signature Standard. A proposed standard for digital signatures using Digital Signature Algorithm.

Digital Signature

An encrypted message digest which is appended to a plaintext or encrypted message to verify the identity of the sender. The signature is encrypted with the user's private key and can only be decrypted with the corresponding public key. The same key pairs may be used for signature and encryption purposes but separate key pairs for each purpose are usually recommended.

IDEA

International Data Encryption Algorithm. It was introduced in 1992 as a potential alternative to DES and is regarded as very secure. It is a block cipher using a symmetric algorithm based on a 128 bit key. IDEA is the data encryption algorithm used in PGP.

Key

A value that is used to encrypt or decrypt a message.

Key Escrow

A concept that originated with the Clipper Chip program, by which a secret or private key is split and the two parts held by escrow agencies against the possibility that the key may be required for law enforcement surveillance or national security purposes.

Key Recovery

A key escrow system which relies on a trusted party to recover a user's confidential keys for use by law enforcement or national security agencies acting under "proper authority". The trusted recovery party might in some cases be internal to the user's organization, but in all cases notice to surveillance targets that their key information had been released would be prohibited. Key recovery is central to the US government's new encryption policy announced in October 1996.

PGP

A complete public-key cryptosystem for electronic messaging that has been released to the public domain. It was originally designed by Phil Zimmerman. It uses IDEA, CAST or Triple DES for actual data encryption and RSA (with up to 2048-bit key) or DH/DSS (with 1024-bit signature key and 4096-bit encryption key) for key management and digital signatures. The RSA or DH public key is used to encrypt the IDEA secret key as part of the message.

PKAF

Public Key Authentication Framework. A system for authenticating digital signatures based on a hierarchy of trusted signatures.

Private Key

The secret part of a private key/public key pair used in public key cryptography. The Private Key is normally known only to the key owner. Messages are encrypted using the Public Key and decrypted using the Private Key. For digital signatures, however, a document is signed with a Private Key and authenticated with the corresponding Public Key.

Public Key Cryptography

A concept first proposed by Diffie and Hellman in 1975 that has been largely responsible for

opening up the science of cryptography for commercial use. The encryption key is made public but only the person who holds the corresponding private key can decrypt the message.

RSA

The best known public key algorithm, named after its inventors: Rivest, Shamir and Adleman. RSA uses public and private keys that are functions of a pair of large prime numbers. The algorithm is best known for its application in PGP. It is patented in the USA only.

Steganography

A method of hiding a secret message in another message, e.g. within a graphic image.

Symmetric Algorithm

An encryption algorithm where the encryption key is the same as the decryption key, or where one key is easily calculated from the other. The sender and receiver have to agree on a key before they can communicate securely.

Triple DES

A method of vastly increasing the security of DES by encrypting 3 times with different keys.

scorpionwally8 - November 6, 2012, 2:00 pm

Very nice tut and easy to understand thank you

d4rkj4y - November 25, 2012, 2:18 pm

Thank you for this, it's a shame it gets lost in the midst of shitty skid spam in this section :(

Phaxol - November 25, 2012, 3:46 pm

Now THIS is the type of encryption I'm looking for, not those shitty crypters.

Clique - November 25, 2012, 4:15 pm

This is an amazing tutorial man.

Such a shame that this has gotten buried :/

TheDubWubCub - November 25, 2012, 4:54 pm

Good Tutorial! Wish to see more of this type of content rather than the crypter related ones. :P haha

Controllable. - November 25, 2012, 5:29 pm

A very nice tutorial to help someone understand cryptography clearly.

d4rkj4y - November 25, 2012, 6:25 pm

<https://hackforums.net/showthread.php?tid=2045696>

You guys should help get this section cleaned out by showing support on the suggestion thread, together I think we can pull something together.

?O?AL€™ - November 25, 2012, 6:29 pm

Thank you my friend. You helped me alot

TheDubWubCub - November 25, 2012, 7:06 pm

(Nov 25, 2012 07:25 PM)d4rkJ4y Wrote: [\[CITE\] https://hackforums.net/showthread.php?tid=2045696](https://hackforums.net/showthread.php?tid=2045696)

You guys should help get this section cleaned out by showing support on the suggestion thread, together I think we can pull something together.

Just posted on the thread! I hope that these sections actually get separated! It'd be nice to not get spammed with Crypter threads haha

J?mes - November 28, 2012, 4:24 pm

A decent informative thread that people should actually take a look at. These kind of threads are just getting spammed out of the section by the free crypters :(.

Thanks for the HQ thread.

PikaSmash - November 28, 2012, 7:05 pm

Thank you this was a decent start on what you need for a good basis

Deep Web - May 29, 2013, 6:28 am

ah thank you illuminati helped me a lot :)

Thangorn - May 29, 2013, 7:13 am

Beautifully laid out, really interesting read and a nice bit of accurate history! I really do love reading these over the usual people begging for free crypts.