

Forum: [Hack Forums](#)

Thread: [????MAFIA???? Cryptography Glossary | Full Information On Cryptography](#)

Black Mamba™ - April 16, 2011, 12:24 am

This topic is intended to gather frequently used terms in this section of the forum and define them informally taking into account the context in which they occur.

That is, it is not a dictionary definition or of an entire Wikipedia article, this is a brief definition by adding interesting facts relating them to the subforum.

Bring this terms with or without corresponding definition, they we will be putting in this post and creating a glossary.

The terms can be composed of several words and definitions were modified to create a more or less uniform (extension, registration of the language used ...).

We hope to do together a compilation of terms that is useful and above all fun to read.
Thank you for your participation.

-AKA: Also Known As "=" Also known as. "

- Brute Force: Method to crack the key is to sequentially test keys until you find the right one, is usually slow, resource consuming and often infeasible.

- Encrypt: To apply a mathematical algorithm that aims to theoretically impossible to read a message.

- Charset: Set of characters that can get to write to a key (eg, lowercase, uppercase, spaces, numbers, special characters, the whole spectrum ASCII).

- Ciphertext: Message after being encrypted.

- Cracking: In cryptography, a ciphertext crack, means finding your own plaintext without the decryption key. If one speaks of a Hash, involves finding an input value of the Hash function that results in the hash that is trying to crack.

- Cryptography: The science that studies the different ways to hide information or make it unreadable to anyone who should not read it.

- Symmetric cryptography: a cryptographic method which uses the same key to encrypt and decrypt messages.

- As-symmetric cryptography or Public Key Cryptography is a method in which a key used to encrypt (known as public key) and one to decrypt (known as private key).

- Decoding: Apply a mathematical algorithm that aims to make legible return an encrypted message.

- Steganography: is the discipline in which they study and apply techniques that allow the hiding of messages or objects, within others, called carriers, so you do not notice their existence.

- Hash: well-defined mathematical function having as input any size and type of data and output as a string value of defined size. In order to be considered a hash algorithm must meet the following requirements:

- Low computational cost: It should be easily calculable.
- Deterministic: For the same input value, there must be a single output value.
- Uniform: The output values must be distributed evenly.
- No reverse: It should not be possible to reverse the hash algorithm.

- Infeasible: syntax used to describe events that are theoretically possible, but the amount of time or resources to achieve those facts, so that it exceeds them extremely impractical.

- Plaintext: Message before being encrypted.

- Rainbow table: They are lookup tables that allow a memory-space sharing in the cracking of Hash's. That is, pre-calculated hashes and placed on a table, these tables, usually large, compared with the hash you're trying to crack.

Credits: MAFIA ([PM](#) me if you need any kind of assistance.)

Please Don't Leech It.

Thanks & Vouches Is Always Appreciated.

Always - April 16, 2011, 12:25 am

Nice glossary, it will help members new to encryption.

Black Mamba™ - April 16, 2011, 12:27 am

Thank you for reading this stuff.