

Cryptography can
decipher what the
other enciphers.



**ASSIGN
BUSTER**

Cryptography is way you can keep information secure. A person who does not know the method used to change the information to keep it secure cannot copy the method used or reverse the change. The basic components of cryptographic systems are used to encipher (scramble) information so that it is difficult to determine the meaning without the appropriate key or key(s) to decipher (unscramble) the information. The components include cryptographic algorithms (mathematical functions) for enciphering or deciphering information and keys. Symmetric and asymmetric are two examples of cryptographic systems.

Symmetric systems use the same key to encipher and decipher. Asymmetric systems generate and use different keys to encipher and decipher a secure key pair. With this key pair, consisting of a public key and a private key, only one key can decipher what the other enciphers. Merely knowing one key does not make it very likely that someone will be able to figure out the other key.

Asymmetric key pairs are used in creating digital signatures and transporting symmetric keys. In the past, most encryption systems only used symmetric cryptography. The problem with symmetric cryptography though, is the difficulty encountered in distributing keys to certain people.

Since symmetric cryptography uses the same key for enciphering and deciphering, a person has to use creative and difficult means to prevent someone from intercepting the key. If a third party were to intercept the key, they could use it to decipher anything it was used to encipher. A solution to this problem is public key cryptography which uses asymmetric

cryptography to transport symmetric keys. In such a system, a recipient's public key is used to encipher a symmetric key. Once enciphered, the symmetric key can only be easily deciphered using the corresponding private key. Keys can be of varying length, typically from 128-bits to over 2000-bits.

Obviously, the larger the key, the more secure the information you're encrypting. Category: Technology