CryptoParty Dictionary

Common terms used when discussing encryption and information security

Threat Model - A system for determining the level of security that something or someone would need given the assumed abilities of a theoretical attacker.

Plaintext - Content that has not been encrypted.

Ciphertext - Content that has been encrypted.

"Strong" Cryptography - Cryptography which uses algorithms that are advanced enough that encrypted content cannot be broken without a computer the size of a few galaxies.

Hash - A mathematical proof that verifies content has not been tampered with. Used like lid seal on a pickles jar.

Off The Record (OTR) - A set of rules for online chat programs to use in order to send and receive encrypted messages between each other. Commonly used to refer to specific chat programs that use OTR.

Fingerprint - A short, unique ID mathematically tied to a larger encryption key, usually a public key. Typically used to help verify you are using the correct public key for a person.

Pretty Good Privacy (PGP) - One of the first strong cryptography software suites made available to non-military in the 90s, now owned by Symantec.

OpenPGP - A set of rules for software to use when encrypting and delivering content between computers. Both PGP and GPG use these rules and can encrypt and decrypt under the same rules.

GNU Privacy Guard (GPG) - A software suite that implements OpenPGP's rules, usually used for encrypting email.

Public Key - A code used as an ID for you used when someone needs to secure content only you can see. It's like a lock which can be used to secure content only your private key can unlock.

Private Key - A secret code that can encrypt and decrypt content and must never be shared.

Secure Socket Layer (SSL) - A way to secure the connection between your computer and (typically) a website you are connecting to. It encrypts the connection to secure it, but the content can still be decrypted by the website.