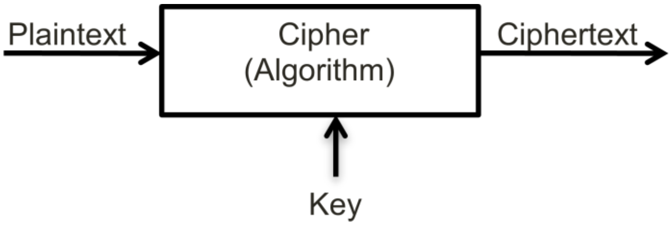
Biometric Key Terms

- **Authentication** – The process of claiming to be someone and then proving it by presenting a credential.

- **Credentials** – Something that identifies who you are. Real world examples would include Passports and Drivers licenses. A password would be an example of a digital credential.

- **Encryption** is the process of transforming information (referred to as plaintext) using an algorithm (called a cipher) to make it unreadable to anyone except those possessing special knowledge. The special knowledge is called the key.



- **Symmetric Encryption** – uses the same key to both encrypt and decrypt the message. The key must be kept a secret between the two parties or else the encryption protection is broken.

- **Asymmetric Encryption** - uses two keys. If one key encrypts the message it can only be decrypted by the other key.

- **PKI (Public key Infrastructure) -** An Asymmetric encryption system where you receive a public and private key, issued by a Certificate Authority (e.g. VeriSign). You publish your public key which people can use to encrypt messages they send you that only you can open … with your private key.

- **GINA** – Graphical Identification and Authentication DLL *(Dynamic Link Library – think of it like a sub-routine)*. When you write a windows logon application that is different then the conventional windows "Welcome Screen" you use this GINA DLL and you application is referred to as a "GINA logon".

- **HASH - cryptographic hash function** is a deterministic procedure that takes an arbitrary block of data and returns a fixed-size bit string, the **hash value**, such that an accidental or intentional change to the data will almost certainly change the hash value. Currently used hash algorithm is SHA-1 although SHA-3 is coming.

  Hash functions are used as part of the process of digitally signing things

- **One time Password (OTP).** A password that is only good one time so you don't care if someone intercepts it.

  OTP's are typically generated with a cryptographic hash algorithm using at least one piece of secret information that both the user and the server that the user is authenticating to share.

  OTP's can be time driven (e.g. RSA) or event driven

- **Seed** - symmetric encryption key, a shared secret between a hardware authenticator and an authentication server. The hardware authenticator, sometimes called a token, and the server work together in a time synchronous, or time dependent mode to provide a one-time password that the token holder enters at login.

- **Single Sign On (SSO)** – A middleware software program that enables a user to log in once and gain access to the resources of multiple software systems without being prompted to log in again.
- **Active Directory** (**AD**) is a technology created by Microsoft that provides a variety of network services. Active Directory allows administrators to assign policies, deploy software, and apply critical updates to an organization. Active Directory stores information and settings in a central database. Active Directory networks can vary from a small installation with a few hundred objects, to a large installation with millions of objects.
- **Compliance Standards –** Allows you to show the standards logo.

  USB – verifies that the product Plug N Play and meet all of the ISB specification.

  FCC – Verifies that you meet part 15 emission standards of the FCC.

  CE – Verifies that you meet the Europe compliance standards.
- **FIPS** – Federal Information Processing Standards – A group of numbered standards that define various aspects and requirements for information processing. FIPS standards are controlled and issued by NIST (National Institute of Science & Technology).
- **FIPS-140 –** The FIPS standard that governs cryptographic processing.
- **Cryptography** – The science of encrypting and decrypting information. Encrypting information makes it unreadable unless you have the key to decrypt it.
- **Common Criteria -** An international standard (ISO/IEC 15408) for computer security certification. With time Common Criteria will probably replace FIPS 140 as the main standard for Computer Security products.
- **Trusted Device / Trusted Peripheral** – A device (could be a PC peripheral) which the organization trusts has not been tampered with and that the data that comes from this device is “true & trustworthy”.
- **Firmware -** Fixed programs that are stored in a medium that cannot be changed or at least cannot be changed without special techniques that are not available to users.
- **Provisioning** – Setting up a computer or a device so that it complies with all of the organizations requirements. In the ideal situation, provisioning can be done over the network.