ENCRYPTION

By: Peyton Cotten
Chip Sheppard
Amber Gavin
Trinity Modisette
Dezmond Cordova
Tristan Hancock

What is Encryption and how does it work?

Encryption is the process of changing original text and mixing it into an unreadable format. Unencrypted data is known as plaintext while encrypted data is called ciphertext. Only authorized parties are able to decipher a ciphertext back to plaintext and access the information.

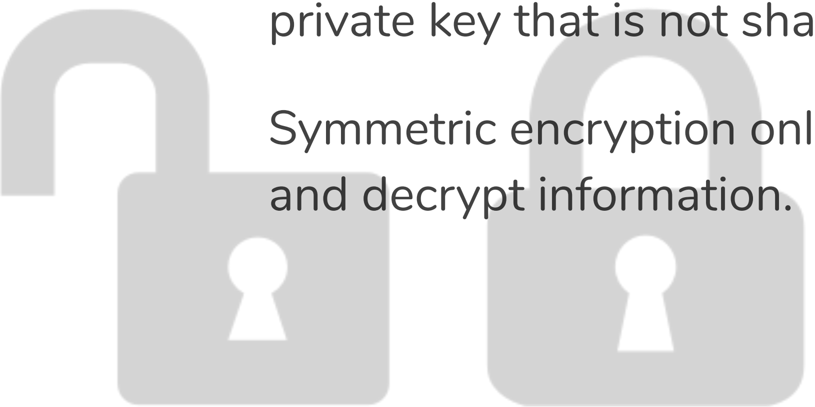
Encryption is a great way to achieve data security. In order for anyone to decipher the code they would need to have access to a key or a password.

Symmetric and Asymmetric Encryption

Encryption is created with algorithms and the key is supposed to be unique.

Asymmetric encryption is used with two keys for encryption and decryption. A public key is shared with users while a private key that is not shared with users.

Symmetric encryption only uses one password to encrypt and decrypt information.



History of Encryption

- Encryption has been utilized all through history… dating times back to the B.C Era. Encryption comes from the Greek word “Kryptos” which means hidden.
- It’s not only utilized with words but also with pictures, dating back to B.C 19th century Egyptian scribes writing hieroglyphs.
- Around 500-600 BC the Hebrew would use a method called Atbash. EX: “a” is z, “b” is y….. Etc this is probably one of the simpler substitution cipher.
- During World War II, the US Navy penetrated through the Japanese cryptography system, JN-25… with this piece of intel aided the U.S the win at the Battle of Midway.

Main Types of Encryption

There are quite a few types of encryption, such as

File Folder or container, and they are easy to manage and use. The drawback being they are also easy to access as an unintended user.

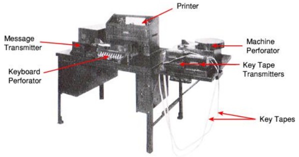
Full disk ~ The term full disk encryption (FDE) or whole disk encryption is used to signify that everything on a disk is encrypted. With FDE, data is encrypted automatically when it's stored on the hard disk and decrypted when it is read from the disk. Drawback is a system failure can mean all data is corrupted.

USB~ USB encryption is similar to folder encryption in that all files on the USB are encrypted. All files dropped into the container are encrypted, file dragged out of the container or unencrypted. Drawbacks include losing the USB drive and all its contents.

Encryption Usage

Encryption today is what allows our society to exist online without exposing all of us to danger. Nearly every company that exists online uses some form of encryption to secure their data. Authentication and digital signatures are used to transmit messages without the fear of interception, while time stamping is used to ensure a document's authenticity and reliability (you can see this in documents from google drive). Banks use these encryptions to transfer your money from place to place without it being compromised mid-transaction. Various programs also exist to alter ciphers to provide an even more secure flow of data. Anonymous remailers can send messages while keeping the identity of the on sending it a complete mystery. Disk encryption is used to completely lock down a disk hard drive, so even direct access is difficult to obtain without knowing the cipher.

Encryption Devices
Military applications



- TSEC/KY-99A is an Advanced Narrowband Digital Voice Terminal (ANDVT), developed in 1994 by the US National Security Agency (NSA). It was used for many years by the US Department of Defence (DoD) for secure voice and data communication over narrow band radio channels.
- A key transfer device is an electronic device that is used (most commonly by the military) for the distribution of cryptographic variables, such as crypto keys and frequency hopping tables. Key fillers often use a standard data protocol, such as DS-102 or DS-101 — both developed by the US National Security Agency, NSA — but devices with proprietary protocols are used as well.
- Telekrypton was an electromechanical one-time tape cipher machine, built around 1933 in the United States by the Western Union Telegraph Company. Built in small quantities it was based on the so-called Vernam Cipher, invented in 1918 by Gilbert Sandford Vernam (1890-1960) and described in US Patent 1310719 [2]. It is further described in an AIEE journal in February 1926 [3].

Future of Encryption

- Homomorphic encryption
- Hardware-based whole disk encryption
- Moving target defense
- Wearable two-factor authentication
- A resurgence of physical-based security
- Quantum cryptography
- Smart contracts for encrypted payments
- Honey encryption
- IoT product security
- Voice biometrics and facial recognition
- Blockchain
- Tokenization

References

https://us.norton.com/internetsecurity-privacy-what-is-encryption.html

https://computer.howstuffworks.com/encryption.htm

https://www.laits.utexas.edu/~anorman/BUS.FOR/course.mat/SSim/life.html

https://kb.wisc.edu/security/page.php?id=17489

https://www.cryptomuseum.com/crypto/usa/index.htm

https://thenextweb.com/contributors/2018/04/27/12-big-encryption-trends-will-keep-data-secure/

http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.741.6752&rep=rep1&type=pdf