Cryptography

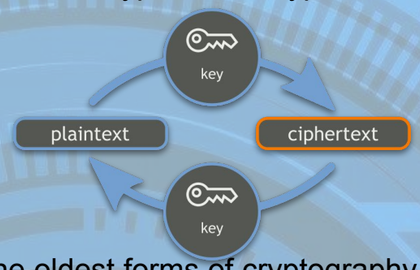
Early History

One of the first recorded uses of cryptography was the use of the Caesar Cipher, a method of substitution cipher that replaced each letter with one further down in the alphabet. The Vignere Cipher, another substitution,Cipher replaced letters based off of a keyword and grid.

Cryptographic methods greatly increased in complexity by using mechanical machines such as the enigma machine. these machines and the bombe, which was made to break its code, are thought of to be the advent of Computers by many, but these machines still followed the same principle, changing the letter every time, but increasing the possibilities that the letter could be changed to.

Secret key

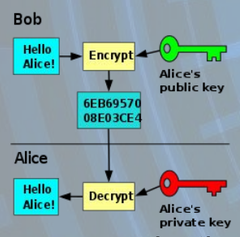
Uses stream and block ciphers, such as RC4 and AES algorithms to encrypt data. Two parties share a secret key and use it to encrypt and decrypt a message.



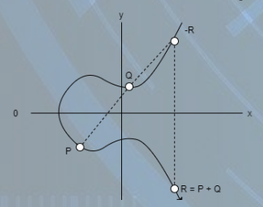
It is one of the oldest forms of cryptography and still sees use today in securing voice communications because of how quick it is to decrypt.

Public Key

Public key uses a key pair one public and one private to encrypt data.
The public key is shared and used to encrypt messages while the private key is kept private and used to decrypt these messages. The two keys are mathematically linked so only one key can decrypt the other.



It is used in securing communications, identity checking and key protection.
It uses algorithms like RSA EIGamal and Elliptic Curve to encrypt message.



Hash Functions

A hash function is a function that can be used to map data of any size onto a number of fixed size.The values returned by a hash function are called hash values, hash codes, digests, or hashes. The values are used to index a fixed-size table called a hash table.

A hash function takes an input as a key. The output is a hash code used to index a hash table holding the data to them.They have three requirements:

To be fast.
To have an avalanche effect.
And be able to avoid collisions.

Quantum Computing

Computers are constantly getting faster. This means we need to make the parts smaller (atom size). When you go this small, electrons behave differently. Quantum computers use Qbits which can be set to 0, 1 or both. this allows for much faster computing.

A Quantum Computer will be much better at dealing with large amounts of data. Checking every combination of data become way faster with Quantum Computers. They only need the square root of the time a normal computer would need. People will need to start working on new ways of staying safe.

Interesting Findings

XOR gates are used in many encryption methods.

The use of curves in the creation of key pairs

Hash functions are less secure then you would think and they are only used for file transfer.

Crypto cracking

While the purpose of a cryptographic algorithm is to provide full security, many algorithms can be attacked and deciphered.

With cryptanalysis, attackers might work out a mathematical way of breaking an encryption. Popular types of attacks include known plaintext, chosen ciphertext or a blinding attack.

VPN and Blockchain

Cryptography has many practical uses. It lies at the core of Virtual Private Networks that allows for safe and private network browsing.

The blockchain technology, is based around hash functions and one of its implementations is in cryptocurrencies like Bitcoin.

Graphics: Bitcoin image by Sinisa Maric, background by Pete Linforth, enigma picture by Fill from pixabay.com, secret and public key diagrams from wikimedia.org, padlocks from openclipart-vectors.com.