

What is the process called that converts plaintext into ciphertext?

Encryption

What is a cipher?

An algorithm used to encrypt and decrypt text.

What is a Caesar cipher and how does it work?

A Caesar Cipher is a substitution cipher that shifts characters a certain number of positions in the alphabet. It works by shifting characters a certain number of positions in the alphabet.

What is the process called that decrypts a message without knowing the cipher or the key used to encrypt it?

Cryptanalysis.

Which key is used to decrypt the message?

Only a Private key can decrypt messages.

Which key is distributed freely?

The public key is distributed freely.

Why is a digital signature used for?

Its used for ensuring the authenticity of the message.

Why do you think encryption is necessary?

Yes, if the message is important and can't fall into the wrong hands like Atomic weapons and formulas of dangerous drugs. Government plans, etc. It keeps important things from the prying eyes of dangerous people.

Do you think software companies should create backdoors for encryption to allow law enforcement to gain access to data for criminal investigations? Yes, even though everyone is right to privacy if that person is endangering lives then law enforcement can gain access to their plans and save lives. But, if its not dangerous and the law enforcement only wants to break our privacy then i don't think it is nessary. Only in certain situations would this be acceptable.