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 ceasar cipher and how does it work?

-A cipher that shifts text characters a certain amount of letters forward or backwards 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 the receiver's private key can decrypt the message sent using the public key.

Which key is distributed freely?

-One’s public key.

Why is a digital signature used for?

-The digital signature is used to authenticate the message and it is is appended to a message using the message itself and the sender’s private key.

Why do you think encryption is necessary?

-I believe that as our world becomes more and more online based then encryption will become more and more important. For example, when it was only word documents and pictures encryption was only necessary to maintain privacy however nowadays the public has banking details and other private information online and this data must be protected for both safety and privacy.

Do you think software companies should create backdoors for encryption to allow law enforcement to gain access to data for criminal investigations?

-I believe that companies should always have access to a key that is able to decrypt it’s information and if a law authority requires access then, and only then, can the get a warrant for the key. That being said the key should not be public in any sense unless the company desires so.