**Youngjun Kim**

**Block C**

**April 5, 2017**

**Lecture Cryptography**

**Questions**

**What is the process called that converts plaintext into ciphertext?**

Encryption

**What is a cipher?**

A cipher is 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.

**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?**

Private Keys

**Which key is distributed freely?**

Public Keys

**Why is a digital signature used for?**

It's used to ensure the authenticity of a message

**Why do you think encryption is necessary?**

It helps protect data that you don't want to spread or be known to anyone else.

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

I do not think companies should create backdoors for encryption. They might share unneccessary information with the government/police and it could harm them in a way.