**Encryption**

**Transforms plain text to ciphertext**

* Uses a type of cipher
* Most ciphers use a pseudo random key for encryption

Use to hide sensitive data so that only the intended recipient can view the message

**Common algorithms:**

* RSA
* AES
* 3DES

**Symmetric Encryption**

* Uses same crypto key for encryption and decryption

**Drawbacks:**

* Each partyu member will have the same key
* If one gets compromised, theyre all compromised
* Pseudo random key generators are used for the leyus and can sometimes lack randomness
  + Because of this, there have been past attacks on symmetric algorithms

**Two types of ciphers**

Stream ciphers

* Encrypts digits and letters, one at a time in a stream

Block ciphers

* Takes a set number of bits and encrypts them as a single entity
* If the plaintext does not fit the block cipher bit size, it will pad the data to make sure it fits

**Asymmetric Encryption**

* Public key cryptography
* Uses public and private keys to encrypt and decrypt, generated as a pair at once
  + this is opposite of symmetric encryption
* public keys are sent out to 3rd parties whereas private keys are stored locally

**Public Key**

* is public
* client will use this to encrypt messages for the private key owner
* no one but the holder of the private key can decrypt the message encrypted with the public key
* compromission of the public key is no where near as bad as a compromise of a symmetric key

**Private Key**

* is private
* used to decrypt messages from public key holder
* should not be shared with anyone

**Common Uses of Asymmetric Encryption**

* TLS
* RSA
* Diffie-Hellman

**RSA**

**Uses Asymmetric Encryption**

* Commonly used in hybrid encryption
  + Symmetric is used to transfer data but then RSA will be used to encrypt the symmetric encryption key
* Used for digital signatures
* Uses 2 very large prime numbers and performs the Factoring Problem

Drawbacks

* Very slow
* Wouldn’t want to use it on full connections or an entire file
* The resources required to do so are too much for most common systems

**AES**

Advanced Encryption Standard

* Symmetric cipher
* Utilizes a block cipher of different sizes
* Common block sizes
  + 128
  + 192
  + 256

The symmetric key length is important

The data encrypted with the **symmetric key will be encrypted over and over** depending on its size

* AES-128 – 10 times
* AES-192 – 12 times
* AES-256 – 14 times