CS 428 – Applied Cryptography

Module 3 Homework

Cameron Stark

1.) What does Perfect Secrecy mean?

Means that viewing the cipher text does not leak or reveal information about the message

2.) How does random number generation work?

Collect amounts of entropy data, and upon random value request, generates sequence of bit data

3.) What is drawback of One-Time Pad?

Any of the below answers

* Key length matches message length
* Keys can only be used to encrypt once
* Can be broken with a known-plaintext attack