CS 428 - Applied Cryptography

Module 5 Homework

Cameron Stark

1.) What are the three aspects of MAC and explain?

*Gen: Generates the key*

*Mac: Encrypts the message*

*Vrfy: Sends a request to access, which receives either 0 or 1 for accepted or rejected*

2.) What are the drawbacks of a fixed length MAC?

* *Message must be of fixed length*
* *Messages must also be short, 128 bit block size*

3.) What are some examples of a hash function in practice?

*MD5, SHA-1, SHA-2 and SHA-3*