CS 428 - Applied Cryptography
Module 4 Homework
Cameron Stark

1.) What is a determing factor, if a scheme is secure?
If every adversary succeeds in breaking the scheme with only neglible and highly improbable chance.

2.) What is the AES?
Standardized definition of encryption done by NIST in 2000, defining that the block length should be 128 bits and key length of either 128, 192 or 256 bits.

3.) What does it mean if a scheme is malleable?
Means that the it is possible to modify the cipher text and thereby cause a predictable change to the plain text.