**Question 1**

openssl enc -aes-128-cbc -d -in encrypted -out decrypted1 -iv 143124152 -K 00112233445566778899887766554

Welcome to CS 6324: Information Security

**Question 2**

openssl dgst -sha1 encrypted

SHA1(encrypted)= dab3eddc62bd38370293515b29bff769ec520d8a

openssl dgst -sha256 encrypted

SHA256(encrypted)= 0e276bd77b7e5462fe4598079777d08dc22b1cb87207d2dc94621742d447338b

SHA-1 is a cryptographic hash function used by NIST. SHA-1 creates a hash for the certificate or the file without revealing their content. Breaking the SHA-1 means createing a forged certificate so browsers will accept it. Malicious files can also be forged in place or normal files.

SHA-1 is also widely used in TLS certificate signature, GIT versioning system, document signature and backup system. SHA-1 certificates are considered insecure by 2017. SHA-0 has already been broken using computing power of a smartphone.

Shattered attack has been accomplished using GPU to compute SHA-1. Attacking using the CPU is easier to implement, but using the GPU is far more efficient. Using

The implication of a SHA-1 attack it reduced the attack time of brute force to a reasonable amount of time and financial cost.