CS 428 - Applied Cryptography

Module 10 HW

Cameron Stark

**Hash Functions - Marcell Gilliam**

1.) What are some implementations of Hash functions?

* Digital Signatures
* Public-key encryption
* Password protection
* Key agreement protocols

2.) What makes Hash functions secure?

The random and unpredictability of their output, creates a secure encryption model

3.) What are some types of Hash functions

* SHA-1
* SHA-2
* SHA-256

**Cryptolocker - Matthieu Privat**

1.) What is a Cryptolocker?

A piece of malware that is typically downloaded onto a machine from an email, or other form of file download, the malware encrypts a target file so that the host computer can not access the file.

2.) How does it work?

Searches the host computer for files to encrypt and then changes the file extension and encrypts the files using RSA 2048-bit key, and links to a web page that requests a ransom to unlock the files

3.) How to fix files under Cryptolocker?

If the ransom is paid the server looks for the key for the targeted machine and sends the key, with which the program does the work of decrypting.