CS363 Information Assurance and Security

-- Final Exam Study Guide

***(I reserve the right to interpret if a question is covered by this guide. Still, only about 90% of questions are covered by this guide****. )*

**Midterm-study guide**

**Malware**:

1. Can explain different types of malware.

* Can rephrase it.
* Can give application examples.

**Cryptography**:

1. Can explain terms used in cryptography
2. Understand symmetric encryption
   1. DES, 3DES, AES
   2. Why 3DES is adopted other than 2DES
   3. Block cipher modes (ECB, CBC, CTR): pros and cons
3. Understand asymmetric encryption
   1. Diffie-Hellman (key exchange), RSA (encryption and decryption)
   2. Man-in-the-middle attack of diffie-hellman & defense
   3. Attacks to RSA & defense

**Networking**:

1. Can explain network attacks: packet sniffing, session hijacking, DOS, DNS caching poison,
2. Can explain network defense: IPSEC, S-BGP, DNSSEC, firewall, traffic shaping, IDS/IPS