Midterm Review

- There will be T/F & M/C questions covering security basics, services & objectives
- Computational & unconditional security
- The EXOR and EXOR math
- Playfair matrix construction and usage
- Vigenere cipher
- DES main parameters and characteristics
- DES and its main vulnerabilities – the solutions to DES and any vulnerabilities to these solutions if they exist
- AES main parameters and characteristics
- RC4 stream cipher basics
- Stream vs. Block ciphers
- Modes of operation basic features