

# Information Assurance: Review Topics for Exam 2

## Test Issues

You can use a calculator, and you can bring a single sheet of notes. Make sure your calculator can calculate exponents (e.g.  $x^y$ ). It is closed book otherwise.

## Basic Cryptography

Reading: Chapter 9 CS

Concepts:

- Classical Cryptography
  - Two basic mechanisms: Substitution, Transposition
    - Product ciphers are a combination of the two
  - Early Crypto Systems
    - Caesar Ciphers
    - Rail Fence Cipher
    - Vigenere Cipher
    - One time pad
    - Enigma Rotor Machine
  - Methods of statistical analysis
    - Character frequencies compared to natural language
    - Index of Coincidence – measuring variation in characters in a text
- Symmetric Cryptography
  - Feistel Networks
    - Structured to use the same S-Boxes and P-Boxes for both encryption and decryption
  - DES is a Feistel Network
    - SBoxes are key to cipher strength
    - Avalanche effect
    - Attacks: brute force, differential crypto analysis
    - Block modes: ECB, CBC
  - AES
    - Faster and longer keys
    - Iterative but not a feistel network
    - Number of rounds vary on key length
  - Limitations of multiple encryptions
- Public Key Cryptography – Concept of having public and private keying information
  - Based on hard problems
  - Looked at two algorithms specifically
  - Diffie-Hellman – To generate unique shared keys
    - Relies on discrete logarithm problem
  - RSA – For more general encryption/decryption and signatures

- Relies on factoring large primes
- Cryptographic Checksums
  - Hash or message digest
    - Computationally infeasible to find two inputs that result in the same hash
  - Keyed cryptographic hashes, e.g. block ciphers in CBC or HMAC

## Key Management

Reading: Chapter 10 CS

Concepts:

- Interchange keys and Session keys
- Trusted Third Parties to enable session key agreement
  - Needham-Schroeder
  - Modifications to avoid replay attacks
  - Kerberos
- Key Generation
  - True Random and Pseudo-Random generation
    - Strong mixing function needed for Pseudo-random generation
- Public Key for session key exchange
  - Basic plus additions to avoid man-in-the-middle attacks
- X.509 Certificates
  - Certificate Authority and Certificate Chains
  - Certificate Revocation List
- PGP web of trust
  - Multiple signatures and levels of trust
- Digital signatures
  - Need to proof for a third party to verify
  - Trusted third party with symmetric keys
  - Public Keys
    - Attacks: Encrypt then sign and multiple signatures
- Key Escrow
  - Clipper chips
  - Yaksha

## Cipher Techniques

Reading: Chapter 11 CS

Concepts:

- Stream ciphers
  - Synchronous key streams
    - LFSR and NLFSR
    - Block ciphers in Output Feedback mode or Counter mode
  - Self-synchronous ciphers

- Autokey from plaintext or ciphertext
  - Block mode in cipher feedback mode
- Limitations of multiple encryptions for block ciphers
  - Meet in the middle attack
- Cryptography and the ISO network stack
  - PEM: Example Application level system
    - Practical issues for backwards compatibility
  - SSL: Example Transport level system
    - 4 way handshake to negotiate keys and algorithms
  - IPSec: Example Network level system
    - AH and ESP
      - Sliding window replay check
    - Tunnel and Transport mode

## Authentication

Reading: CS Chapter 12

Concepts:

- Authentication system formalisms
- Passwords
  - Dictionary attacks: Type 1 (offline) and type 2(online)
    - Anderson's formula
  - Picking good passwords
  - Salt
- Challenge-Response authentication
- Biometrics
- Multi-factor authentication

## Network Security Mechanisms

Readings: Intrusion Detection – Chapter 25 in CS. Network Security - Chapter 26 in CS

Concepts:

- Network security architecture
  - Security Domains and perimeter defense
  - Virtual Private Network
  - Intranet, DMZ, and Internet
- Firewalls
  - Packet filter versus proxy
  - Hybrid stateful packet filters
  - Ingress and egress filtering
  - Address translation
    - Address hiding or NAT
    - Static translation

- Denial of service examples
  - TCP Syn Attack
  - Smurf attack
- Intrusion detection
  - Agents, directors, and notifiers
  - Signature detection versus anomaly detection
  - Host based and network based IDS