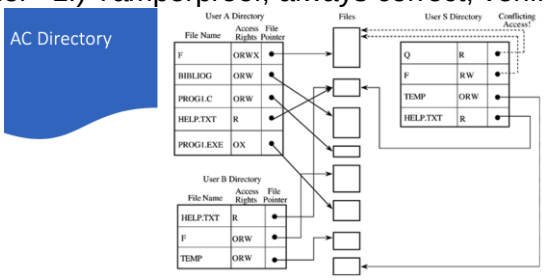
Security Mindset
CIANA
Confidentiality
Integrity
Availability
Non-repudiation
Authentication
- What you are, know, have

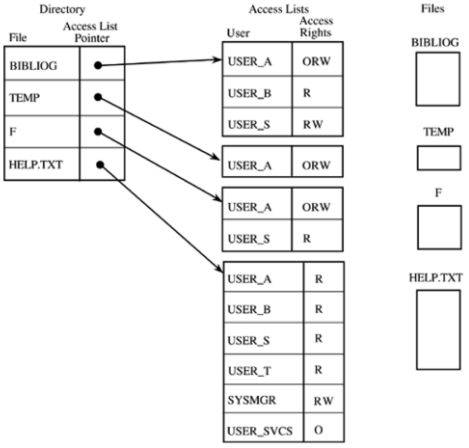
Asymmetric Advantage
The attacker only needs to exploit one weakness

Security in Depth
Layers, two factor authentication is SiD if on two different devices. Ex: Biometrics, email verification, encrypt then Mac.

Threat Modeling
•Assets: What are we trying to protect? How valuable are those assets?
•Adversaries: Who might try to attack, and why?
•Vulnerabilities: How might the system be weak?
•Threats: What actions might an adversary take to exploit vulnerabilities?
•Risk: How important are assets? How likely is exploit?
•Possible Defenses

Access Controls
Reference Model - 1.) Tamperproof, always correct, verifies every access attempt
AC Directory -
AC Matrix
AC List





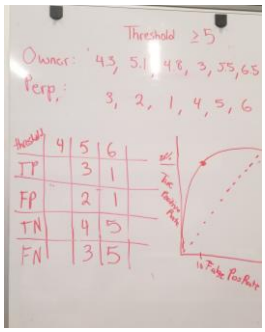
Authentication Mechanisms
Types of Password Attacks
- Brute Force
- Dictionary
- Phishing
- Rainbow Table
- Credential Stuffing
- Password Spraying

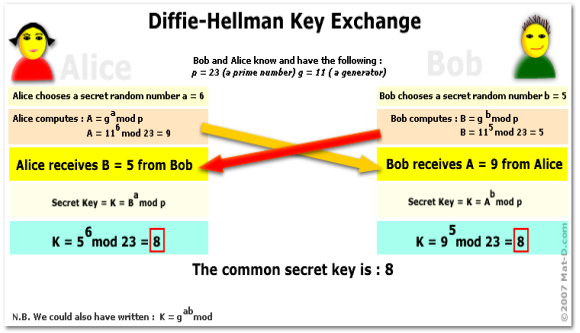
Entropy Formula
Summation of log(base2)(1/p)

Cryptography

MAC (Message Authentication Code)
HMAC (Hash Message Authentication)

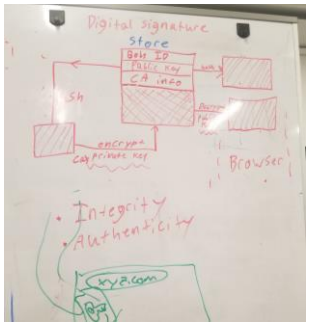
Sensitivity: TP/# of positives
Specificity: TN/# of negatives
Accuracy: TP + TN / P + N

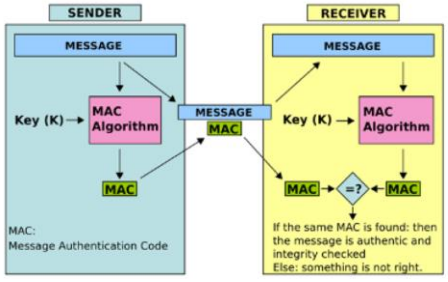


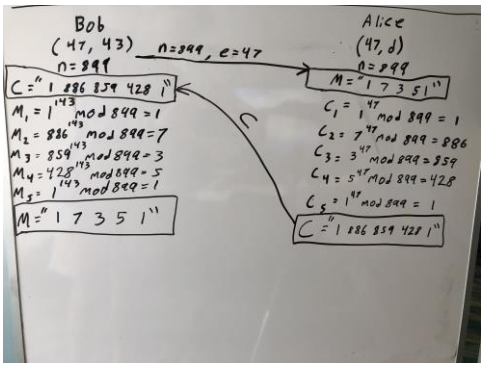


Kerckhov's Principle
- The secrecy of the private key is all that matters. Contrary to the security by obscurity principal.

size(message space) == size(key space) == size(cipher space) ➔ PERFECT SECRECY







Three Ways