Encryption

Monoalphabetic ciphers
Symmetric Encryption
- Caesar cipher (the key is how many letters to rotate it)
- Need secure algorithm, they can’t decipher ciphertext or key even if they have some examples of ciphertext along with decrypted version
- Keys need to be distributed in secure manner

Cryptanalysis
- They know something (either plaintext, or algorithm to deduce the key)
- Brute force
  - Try every possible combination to guess the key.

Stream Ciphers

Hash functions:
- MD5
- SHA1sum
- For message authentication. Encryption protects against passive attacks. Hash is used for active attacks (falsification of data and transactions). (Still falls under data integrity)

PKI

Proposed in 1976 (Diffie-Hellman)
- Two separate keys
- 6 ingredients to PKI
  - Plaintext
  - Encryption Algorithm
  - Public and private key
  - Each user generates a pair, public key is publicly available

PKI More

- Encrypt message using persons public key, only corresponding private key can decrypt
- Private keys are never distributed
- Can ensure a person is who they say they are
- When sending messages, we can ensure confidentiality
- When receiving messages, we can ensure authentication and/or data integrity
  - Ciphertext
  - Decryption algorithm

PKI More

- Look at /etc/moduli
- Diffie-Hellman key exchange process
  - Enables 2 users to securely reach agreement about shared secret that can be used as a secret key
for symmetric encryption of messages

- Asymmetric encryption algorithms
  - RSA = block cipher
  - currently uses 1024 bit key

Digital Signatures

- Bob creates message, generates hash value for the message, and encrypts hash code with private key, creating a digital signature
- Alice receives messages plus signature
  - Recalculates hash value for message
  - Decrypts signature using Bob's public key
  - Compares calculated hash value to decrypted hash value
- The message is safe from alteration, but not from observation

Certificates

- Downside: Some user could send their public key, purporting to be Bob.
- Solution is public key certificate
  - Consists of public key, userid, plus signed by trusted 3rd party (ie verisign)