CprE 489
Lecture 29

Fall Semester 1997

Network Security

- Secrecy
  - Keeping information out of the wrong hands
- Authentication
  - Verifying who someone is
- Nonrepudiation
  - Verifying that a particular transaction actually happened
- Integrity
  - Verifying that the information received came from the person you think it did.

Cryptography and Attack

- Encryption - converting a plaintext into a cyphertext: C=E(P).
- Decryption - converting a cyphertext into a plaintext: P=D)E(P)).
- Standard Encryption - E and D are only known to the sender and receiver.
- Public Key Encryption - E is known publically and D only to the receiver.
- Note that P = E(D(P)) also, that is D and E are inverses of eachother.
- E and D depend on keys e and d: $E(P)=E_e(P)$ and $D(C) = D_d(C)$.
- The encryption and decryption methods are known.
- Cyphertext attack - Given several C's, discover D.
- Given plain text attack - Given P and E(P), for several P's discover D.
- Chosen plain text attack - Pick several P's and compute E(P) for each one, now discover D.
- Replay attack - Without breaking the cryptosystem, repeat a message.

Secret Key Encryption

- Both the encryption and decryption depend on the same key k.
- The key k is known only to sender and receiver.
- Example: One time pad.

  k = random bit string of length m, Assume P is m bits long.

  $E_k(P)$ = P exclusive or k

  $D_k(C)$ = C exclusive or k

  $D_k(E_k(P))$ = (P exclusive or k) exclusive or k = P

  Can be defeated by both given and chosen plain text attack.

DES

- DES = Data Encryption Standard
- Uses a 56 bit key which is breakable with enough computing power by brute force given meaningful encrypted messages.
- The plaintext is broken into 64 bit textblocks. Each block is encrypted separately, yielding 64 bit cypherblocks.
- Decryption with key k is identical to encryption with key k.
- There are extensions which apparently cannot be easily broken

Public Key Encryption

- Properties

  1. D cannot be easily deduced from E.
  2. E is secure from any plaintext attack.
- Can be used for digital signatures
- Best known method is RSA for Rivest, Shamir, and Adleman
- RSA can be broken if an efficient method for factoring integers could be found.

RSA

- Private key = (n,d) where n = p x q where p and q are large primes (100 digits or more) and d is an integer that is relatively prime to z = (p-1)x(q-1).
- Public key = (n,e) where n = p x q and e x d = 1 mod z.
- Encryption algorithm: Let P be a message such that $0 \leq P < n$ (P is interpreted as an integer).

  $E(P) = P^e \pmod n$
- Decryption algorithm:

  $D(C) = C^d \pmod n$
- By relatively elementary number theory it can be shown that

  $P = P^{ed} \pmod n$
- It is believed but not proven that given (n,e) and any kind of plaintext attack it requires expontential time to find d. If the factors of n can be found then e can be calculated easily.

Digital Signature using Public Key Encryption

- How to have A sign the message P for B.
- A sends $C = E^B(D^A([A,P]))$ to B
- To decrypt

  1. B decrypts C using its private key to get $D^A([A,P]) = D^B(E^B(D^A([A,P])))$
  2. B then encrypts $D^A([A,P])$ using A's public key to get $E^A(D^A([A,P])) = [A,P]$