CIS 3362 10/28/24

1) Grade Calculation – Will post how to calc our grade by tommorow.

2) Homework 6 will be made up soon -look for it! (might have prize!)

3) Public Key Cryptography

Privek Key / Symmetric 2 people must ~~to~~ meet in a secure location and exchange a shared secret key.

Is it possible for 2 people to have a conversation with others listening, but at the end of it, exchange some secret info that the others can't ~~decod~~ deduce or figure out?

Goal #1: Exchange a secret key (bitstring)
Public Key Exchange

Goal #2: Straight up exchange messages of our choosing.
Pbublic Key Cryptography

Both Solved in the 1970s. → 1976 Key → 1977 Crypto

- Publicly known / ~~post~~ published solution
- Secret Solution (person didn't get credit for a long time) → 1972/3 (both) Clifford Cocks (Whitfield Martin)

Today's Lec: Diffie-Hellman Key Exchange

Look at Discrete Log Problem

$c = b^e \bmod p$ } easy calc forward

but given c, e and p hard to solve out b.

Public Components

p = large prime (many digits)

g = generator of prime

Private Keys

a = Alice's secret key

b = Bob's secret key

$1 < a, b < p-1$

Alice

$c_1 = g^a \bmod p$

sends to Bob →

receives c_2

← sends to Alice

$K = c_2^a \bmod p$

↳ shared key

$c_2^a = (g^b)^a \bmod p$

$= g^{ab} \bmod p$

Bob

receives c_1

$c_2 = g^b \bmod p$

$K = c_1^b \bmod p$

↳ shared key

$c_1^b = (g^a)^b \bmod p$

$= g^{ab} \bmod p$

PUBLIC

c_1

c_2

p

g

As a bystander you know:

p - prime

g - gen

$g^a = c_1$

$g^b = c_2$

$c_1 \times c_2 = g^{a+b}$ X

$c_1^{c_2} = \left(g^a\right)^{g^b} = g^{a^{g^b}}$ X

→ knowledge of c_1, g and p doesn't compromise knowledge of a (Discrete Log Problem)