CIS 3362 10/24/25

Public Key Cryptography

Everything before this required 2 people to meet in a secure location to exchange a private key.

Is it possible for 2 people (Alice, Bob) to communicate on an insecure line so everyone can see what they're saying to each other, but at the end of the conversation they've exchanged a secret key that no one else can decipher?

Whitfield Diffie - gave talks about the possibility of a public key exchange protocol.

Martin Hellman - was interested in what Diffie had to say + decided he wanted to work with him on it.

1972-3-4?

took about a year!

Diffie-Hellman Key Exchange

Security is based on the difficulty of the Discrete Log Problem.

Public keys

p = large prime

g = generator

Alice

Alice pick secret value a, $1 < a < p-1$

Alice computes $B^a \bmod p$

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

$\equiv g^{ab} \bmod p$

Alice sends $A = g^a \bmod p$ →

← Bob sends $B = g^b \bmod p$

Observer sees g^a, g^b, but doesn't see a or b.

Bob

Bob picks secret value b, $1 < b < p-1$

Bob computes $A^b \bmod p$

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

$\equiv g^{ab} \bmod p$

Shared key

$(g^a)(g^b) = g^{a+b}$ not helpful

$(g^a)^{g^b} = g^{ag^b} \equiv$ not helpful