CIS 3362 10/31/22

Story - Ch+6 Code Book

"Public Story"

Alice Eve (listening!) Bob

(1) Can Alice + Bob exchange a secret key w/o Eve figuring out what it is?

(2) Would it be possible for Alice + Bob to communicate period (regular cryptosystem) w/ Eve listening but only Alice + Bob understanding?

Whitfield Diffie, Martin Hellman - gave a talk - he listened — Worked together

Diffie-Hellman Key Exchange (1976)

On Wed, I'll tell you about Ron Rivest, Adi Shamir + Leonard Adelman. (RSA Encryption) (1977)

Actually discovered/invented 4 years earlier! British equivalent of NSA was working on public key cryptography.

Early 1970s hired a mathematician, Clifford Cocks.
Senior people describe both the key exchange + public key cryptosystem ideas at lunch w/ Clifford.
Within 3 weeks, Clifford formulated both
RSA encryption (he did this first)
Diffie-Hellman key exchange (he did this second)

1973!

Declassified in 1997

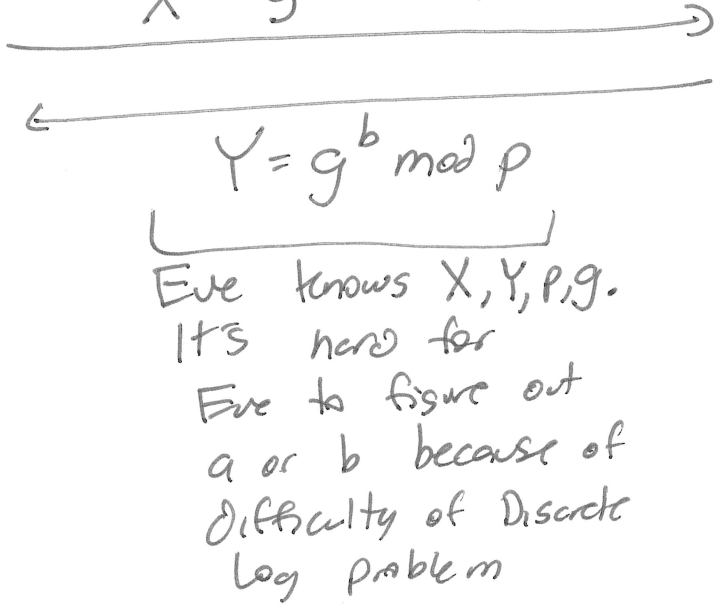
We want alice + bob to exchange a secret key. Eve hears all there communication.

* Neither Alice nor Bob pick their exchanged key.

Public Elements

p = prime (large)

g = generator/primitive root mod p



1. Pick random a, $1 < a < p-1$

2. Pick random b, $1 < b < p-1$

3. Calculate $Y^a \bmod p$

4. Calculate $X^b \bmod p$

Eve knows X, Y, P, g. It's hard for Eve to figure out a or b because of difficulty of Discrete log problem

$$Y^a \equiv (g^b)^a \bmod p \equiv g^{ab} \bmod p$$
$$X^b \equiv (g^a)^b \bmod p \equiv g^{ab} \bmod p$$
SAME

Eve knows X, Y, can she calculate the key?

$X \cdot Y = g^a \cdot g^b = g^{a+b}$ NO

$X^Y = g^{a \cdot g^b}$ pretty different!

Paper example

$p = 17 \quad g = 3$

Alice picks 5. Send $3^5 \bmod 17 = 5$.

Bob picks 6. Send $3^6 \bmod 17 = 15$

Alice computes $15^5 \equiv (-2)^5 \equiv -32 \equiv \boxed{2} \bmod 17$

Bob computes $5^6 \equiv (5^3)^2$
$\equiv (125)^2 \equiv 6^2 \equiv 36 \equiv \boxed{2} \bmod 17$

But mathematically, given 5 and 15, the numbers Eve sees, it's hard for her to calculate Alice + Bob's shared key.