Math 4400
Week 6 - Tuesday
Shift ciphers and Diffie-Hellman.

A basic shift cipher.

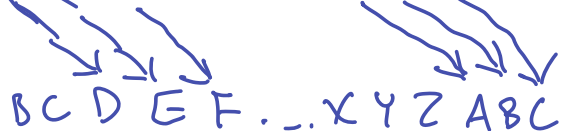
HELLO

↓

KHOOR

3-shift

A B C D E .... X Y Z



A B C D E F ... X Y Z A B C

To encode, shift each letter by 3.

To decode, shift each letter by −3.

Example: Decoding C H E U D
↓
Z E B R A.

Nothing special about 3 ⇝ can shift by any integer K (but only depends on K mod 26).

Problem - If I know you are using a shift cypher, and want to decode an intercepted message, I can just try all 26 shifts.

Better – change the shift often:

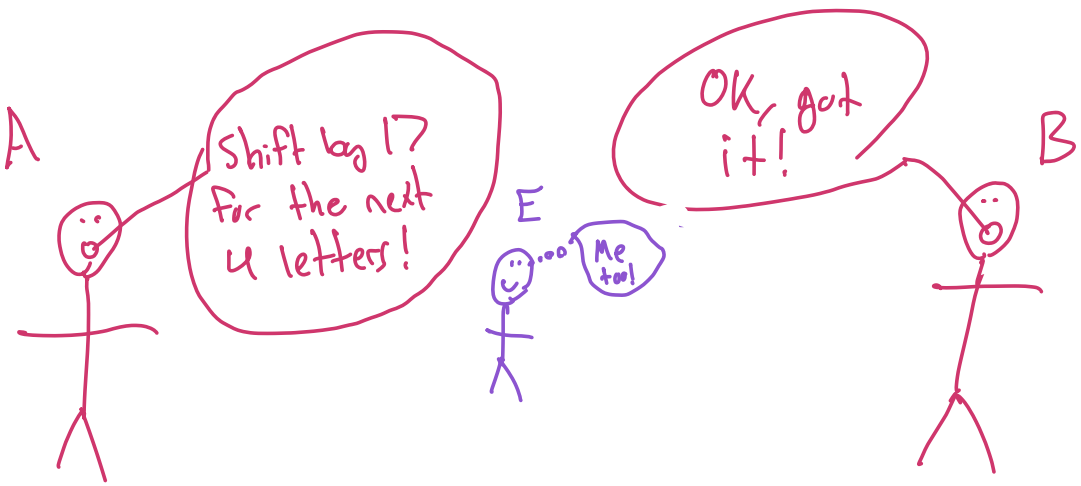
T E N M O N K E Y S Pick 3 different

shift by K₁ | shift by K₂ | shift by K₃

... 3 shifts k_1, k_2, k_3

Now 26^3 possible shifts!

But if Alice wants to communicate with Bob, how can they make sure they both know the right shifts without anyone else finding out?



The Diffie-Hellman key exchange
(A way to establish a shared secret using public communication channels).

Setup: Choose a prime p and a primitive root* $g \in \mathbb{F}_p^\times$. (public knowledge)

Example: $p = 29$. $a = 2$.

Goal: For Alice and Bob to get a shared secret ~ an element $Z \in \mathbb{F}_p^\times$ that only they know.

Step 1: Alice and Bob each pick a (private) numbers a and b

Example: $a = 10$ $\quad b = 18$

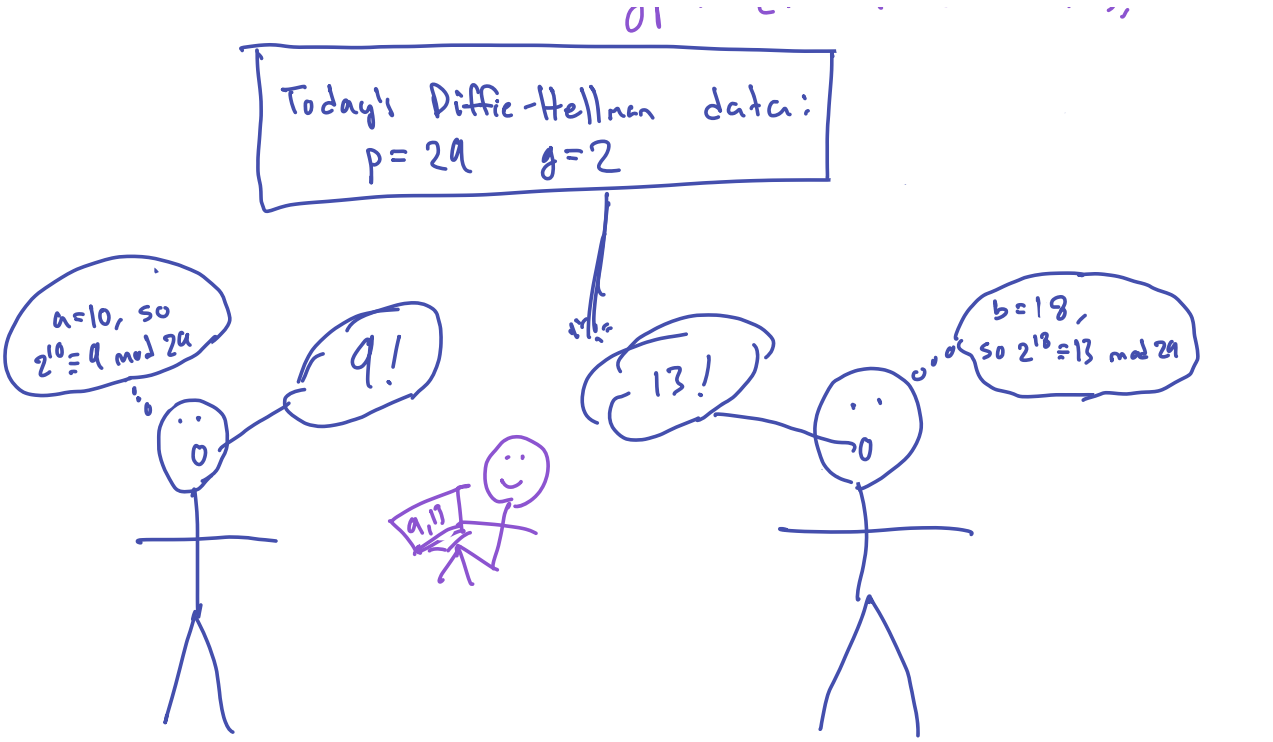
Step 2: Alice sends Bob $X = g^a \bmod p$
Bob sends Alice $Y = g^b \bmod p$

Example: $X = 9 \equiv 2^{10} \bmod 29$ $\quad Y = 13 \equiv 2^{18} \bmod 29$.

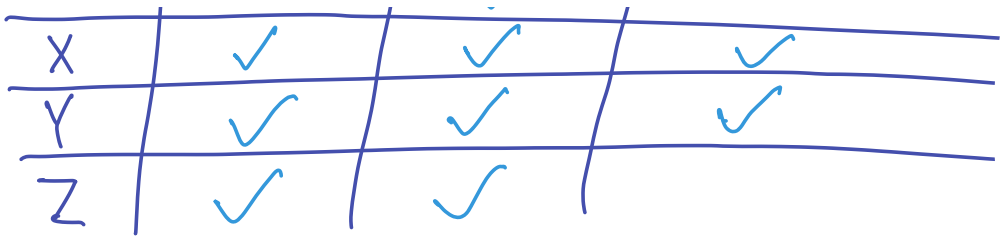
Step 3: Alice computes $Z = Y^a = (g^b)^a = g^{ba} \bmod p$.
$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad\; \| \; ba = ab$
Bob computes $Z = X^b = (g^a)^b = g^{ab} \bmod p$.

Example: $Z = 13^{10} \equiv 7 \bmod 29$ ← Alice's computation
$Z = 9^{18} \equiv 7 \bmod 29$ ← Bob's computation.

The shared secret is 7! They can safely use it for a shift cypher (for a little while)



	Alice	Bob	Eve
p, g	✓	✓	✓
a	✓		
b		✓	



To compute Z, Eve needs to know a or b.

$g^a = X$ $\quad\quad$ $g^b = Y$

$\Updownarrow$ $\quad\quad$ $\Updownarrow$

$a = \log_g X$ $\quad\quad$ $b = \log_g Y$

"Discrete logarithm" (log in a finite field).

Example: To compute $\log_2 9$ in $\mathbb{F}_{29}$, basically the only way is to just list out all powers of 2 until you find the right one.

In $\mathbb{F}_{29}$:

$2^0 = 1$ $\quad$ $2^1 = 2$ $\quad$ $2^2 = 4$ $\quad$ $2^3 = 8$ $\quad$ $2^4 = 16$

$2^5 = 3$ $\quad$ $2^6 = 6$ $\quad$ $2^7 = 12$ $\quad$ $2^8 = 24$ $\quad$ $2^9 = 19$

$\boxed{2^{10} = 9}$ $\quad$ $\log_2 9 = 10$ $\quad$ ⇐ I found Alice's secret.

So can get $Z = Y^a = 13^{10} = ?$

Not impossible, just hard if p is very large.

(In comparison, Alice and Bob only have to compute

2 powers each!)

*: If $\mathbb{K}$ is a finite field, $g \in \mathbb{K}^\times$ is a <u>primitive root</u> if

$$\mathbb{K}^\times = \{g^0, g^1, g^2, \dots\}$$

i.e. if every element of $\mathbb{K}^\times$ is a power of g.