RSA: factoring hard

next: DH/ElGamal: discrete logs hard

"$x = \log_3(4)$" EG $4 \equiv 3^x \pmod 7$ Find x.

Try $x = 2, 3, 4, \ldots$

$3^2 \equiv 2$, $3^3 \equiv 2 \cdot 3 \equiv -1$, $3^4 \equiv -1 \cdot 3 \equiv 4$

$\Rightarrow x = 4$

EG $3 \equiv 2^x \pmod{101} \Rightarrow x = 69$

Diffie-Hellman key exchange:

- A+B select large p, primitive root $g \pmod p$
- A selects random y, reveals $g^y \pmod p$
  B x $g^x \pmod p$

$\Rightarrow$ A+B now share secret: $g^{xy} \pmod p$

[A: knows y, $g^x \Rightarrow g^{xy} = (g^x)^y$]

EG A+B select $p = 53$, $g = 5$ for DH.

$A \xrightarrow{43} B$, $B \xrightarrow{20} A$ What is shared secret?

$43 = 5^y$ $20 = 5^x$

Compute $5^2, 5^3, \ldots \pmod{53}$:

$5^2 = 25$, $5^3 \equiv 19$, $5^4 \equiv 19 \cdot 5 \equiv -11$

$5^5 \equiv -11 \cdot 5 \equiv -2$, $5^6 \equiv -2 \cdot 5 \equiv -10 \equiv 43$

$\Rightarrow$ A's secret is $y = 6$

$\Rightarrow$ shared secret: $5^{xy} = (5^x)^y = 20^6 \pmod{53}$

$\equiv 9$

CDH computational Diffie-Hellman problem: given $g, g^x, g^y \pmod p$, find $g^{xy} \pmod p$