Diffie-Hellman

Diffie-Hellman

- Invented by Williamson (GCHQ) and, independently, by D and H (Stanford)
- A "key exchange" algorithm
  - Used to establish a shared symmetric key
- ***Not*** for encrypting or signing
- Based on **discrete log** problem:
  - **Given:** g, p, and $g^k \bmod p$
  - **Find:** exponent k

Modular Arithmatic

- Given prime number *p*
- Multiplicative group of p: {1, 2, …, p-1}
- Primitive root mod p (generator of the group)
  - g^k generates all the group members
  - i.e., for any x in {1, 2, …, p-1}, there exists k s.t. $g^k \bmod p = x$
- EX
  - p=7, g=3, 5
  - p=5, g=2, 3

Diffie-Hellman

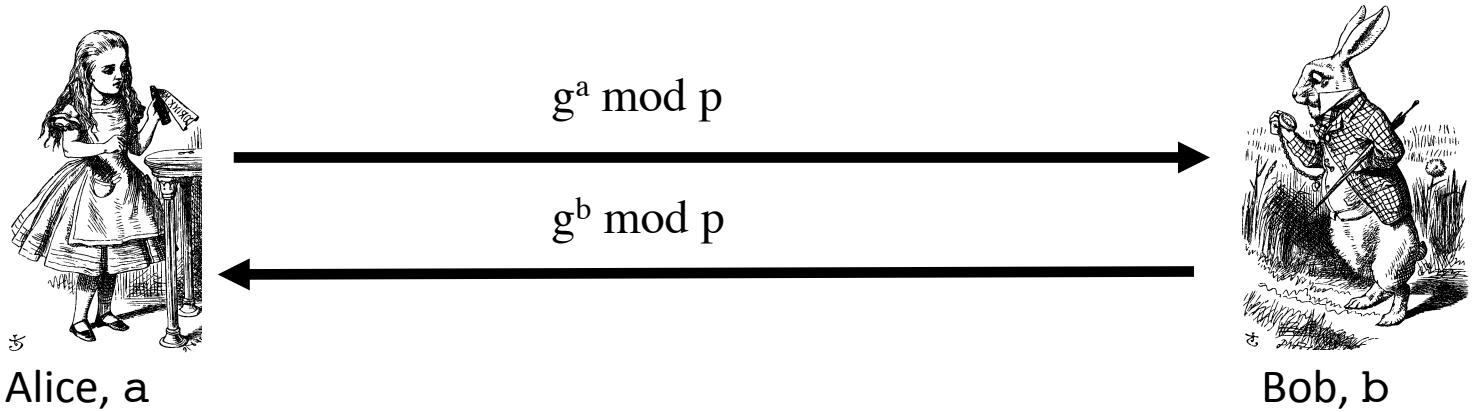
- Let p be prime, let g be a **generator**
  - For any $x \in \{1,2,\ldots,p\text{-}1\}$ there is n s.t. $x = g^n \bmod p$
- Alice selects her private value a
- Bob selects his private value b
- Alice sends $g^a \bmod p$ to Bob
- Bob sends $g^b \bmod p$ to Alice
- Both compute shared secret, $g^{ab} \bmod p$
- Shared secret can be used as symmetric key

Diffie-Hellman

- Suppose Bob and Alice use Diffie-Hellman to determine symmetric key $K = g^{ab} \bmod p$
- Trudy can see $g^a \bmod p$ and $g^b \bmod p$
  - But… $g^a g^b \bmod p = g^{a+b} \bmod p \neq g^{ab} \bmod p$
- If Trudy can find a or b, she gets key K
- If Trudy can solve **discrete log** problem, she can find a or b

Diffie-Hellman

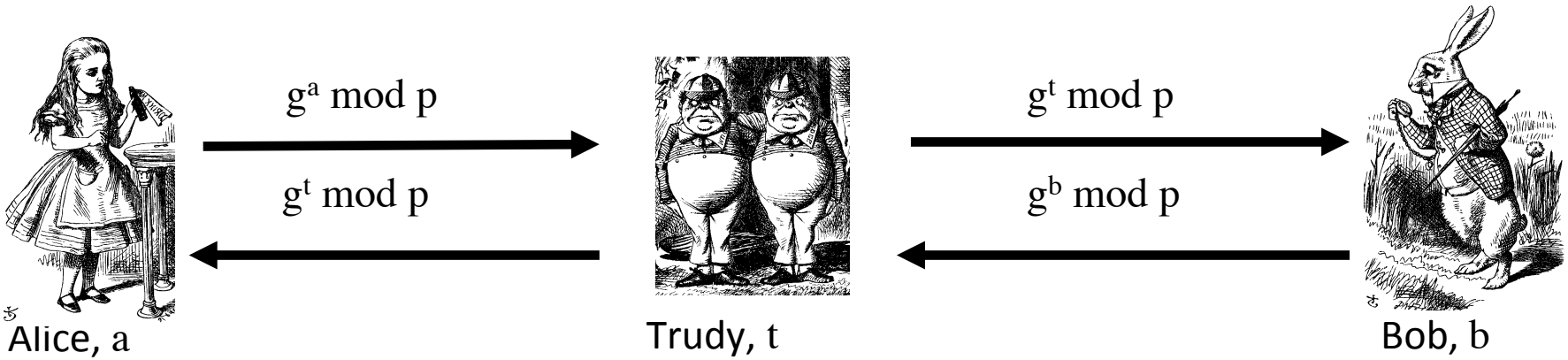
- **Public:** g and p
- **Private:** Alice's exponent a, Bob's exponent b



- Alice computes $(g^b)^a = g^{ba} = g^{ab} \bmod p$
- Bob computes $(g^a)^b = g^{ab} \bmod p$
- Use $K = g^{ab} \bmod p$ as symmetric key

Diffie-Hellman

- Subject to man-in-the-middle (MiM) attack



- Trudy shares secret $g^{at} \bmod p$ with Alice
- Trudy shares secret $g^{bt} \bmod p$ with Bob
- Alice and Bob don't know Trudy exists!

Diffie-Hellman

- How to prevent MiM attack?
  - Encrypt DH exchange with symmetric key
  - Encrypt DH exchange with public key
  - Sign DH values with private key
  - Other?
- At this point, DH may look pointless…
  - …but it's not (more on this later)
- In any case, you **MUST** be aware of MiM attack on Diffie-Hellman