Diffie-Hellman
Key-Exchange Algorithm

• Alice and Bob agree on a large prime, $n$ and $g$, such that $g$ is primitive mod $n$.
• These two integers don’t have to be secret; Alice and Bob can agree to them over some insecure channel.
• They can even be common among a group of users.


• A primitive element in a group is an element whose powers exhaust the entire group.
• Thus 3 is primitive in the group of units mod 7 as
  - $1=3^6$, $2=3^2$, $3=3^1$, $4=3^4$, $5=3^5$, and $6=3^3$,
• but 2 is not primitive in this group as there is no exponent $e$ such that $3=2^e \pmod{7}$.
  More commonly we say that 3 is primitive mod 7 but 2 is not.

http://www.math.umbc.edu/~campbell/NumbThy/Class/Glossary.html
The protocol goes as follows:
1) Alice chooses a random large integer \( x \) and sends Bob \( X = g^x \ mod \ n \)
2) Bob chooses a random large integer \( y \) and sends Alice \( Y = g^y \ mod \ n \)
3) Alice computes \( k = Y^x \ mod \ n \)
4) Bob computes \( k' = X^y \ mod \ n \)

- Both \( k \) and \( k' \) are equal to \( g^{xy} \ mod \ n \).
- No one listening on the channel can compute that value; they only know \( n, g, X, \) and \( Y \).
- Unless they can compute the discrete logarithm and recover \( x \) or \( y \), they do not solve the problem.

- \( k \) is the secret key that both Alice and Bob computed independently.