# Diffie-Hellman Key Exchange

a method of exchanging cryptographic keys over a public channel
one of the first practically implemented secure methods to exchange keys
in this protocol, two parties mutually establish a shared secret key without having any prior shared secret

the protocol

Alice and Bob mutually agree on $p$ and α (alpha)

$p$ is a large prime number

α is a primitive root modulo $p$ (more details below)

Alice choses a secret integer, $a$, then sends Bob $A_{pub}=\alpha^{a}(mod\, p)$

Bob choses a secret integer, $b$, then sends Alice $B_{pub}=\alpha^{b}(mod\, p)$

Alice computes $S=B_{pub}{}^{a}(mod\, p)$

Bob computes $S=A_{pub}{}^{b}(mod\, p)$

subsequently, they both share the same common key that they can use for symmetric cryptography

an example

public parameters $(p,\alpha)=(5,3)$

Alice chooses $a=10$ ; Alice sends Bob $A_{pub}=3^{10}(mod\,5)=4$

Bob chooses $b=7$ ; Bob sends Alice $B_{pub}=3^{7}(mod\,5)=2$

Alice computes $S=2^{10}(mod\,5)=4$

Bob computes $S=4^{7}(mod\,5)=4$

at both ends, $S=4$

given $p$, how would you find a primitive root modulo $p$?

in the above example, $p=5$ ; so:

| potential α | $\alpha^{1}(mod\,5)$ | $\alpha^{2}(mod\,5)$ | $\alpha^{3}(mod\,5)$ | $\alpha^{4}(mod\,5)$ |
|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 1 |
| 2 | 2 | 4 | 3 | 1 |
| 3 | 3 | 4 | 2 | 1 |
| 4 | 4 | 1 | 4 | 1 |

here, 2 and 3 are the candidate primitive root modulo 5

because the values on each of their columns are unique

we can randomly choose any of these two numbers as our α

a prime number $p$ will have at least two primitive root modulo values in the range 2 to $p-1$

validity of Diffie-Hellman

i.e., S must be equal on both sides (Alice and Bob)

$$S=A_{pub}{}^{b}(mod\, p)=(\alpha^{a})^{b}(mod\, p)=\alpha^{ab}(mod\, p)=\alpha^{ba}(mod\, p)=(\alpha^{b})^{a}(mod\, p)=B_{pub}{}^{a}(mod\, p)=S$$

note: $p$ is a large prime number in practice

but α does not have to be large

usually, α is a small integer

the discrete log problem

- given all the publicly known values: $p, \alpha, A_{pub}, B_{pub}$
- it is (almost) impossible to determine the values of *a* and *b*, and the private keys of Alice and Bob
- why?
  - it's a discrete log problem
  - generally, $\log_b a = x \equiv b^x = a$
    - given *a* and *b*, find *x* (pretty easy – with a calculator)
    - e.g., $a=19683, b=3:\ x=\frac{\log(19683)}{\log(3)}=9$
  - a discrete log reduces the scope of *x* to groups like prime numbers, for example
  - it's similar to the above, except $(mod\ p)$
  - generally, $\alpha^x (mod\ p) \equiv y$
    - e.g., $3^x (mod\ 17) \equiv y$
    - when raising 3 to values of *x* from 2 to $p-1$, every result is equally likely
      - e.g., $3^{13} (mod\ 17) \equiv 12$
    - given *p*, *y*, and $\alpha$, find *x*
      - e.g., $3^x (mod\ 17) \equiv 12$
      - trial and error is really the only way to solve this
  - discrete logs can be very hard to solve
    - if *p* is a large prime number, then efficiently finding *y* is intractable