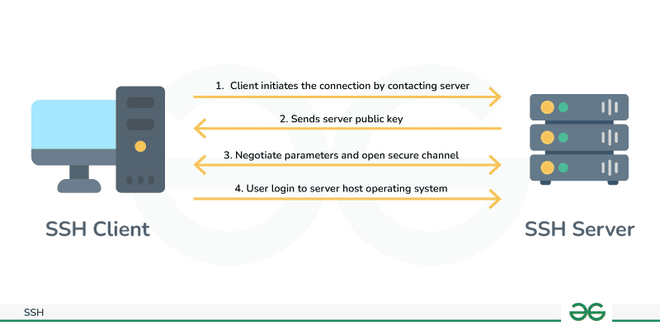
1. **Thuật toán Diffie-hellman trong thực tế.**

Thuật toán Diffie-hellman có rất nhiều ứng dụng quan trọng trong thực tế đặc biệt là sử dụng như một giao thực để trao đổi khóa. Một trong những ứng dụng tiêu biểu nhất của Diffie-hellman trong thực tế là Secure Shell.

* 1. **Secure Shell (SSH) là gì?**
* Secure Shell là một giao thức hỗ trợ các nhà quản trị mạng truy cập vào máy chủ từ xa thông qua mạng internet không bảo mật. Nói cách khác thì SSH là một giao thức mạng được sử dụng để truyền dữ liệu mã hóa qua mạng. SSH cho phép user kết nối với server mà không cần phải nhớ mật khẩu hay nhập mật khẩu cho từng hệ thống. Nó luôn đi kèm với hai khóa:
  + Public key: sử dụng cho mã hóa.
  + Private key: sử dụng cho giải mã.
  1. **Cơ chế của SSH.**



* Khởi tạo kết nối: Client kết nối đến server qua SSH, đầu tiên hai bên sẽ lựa chọn các thuật toán mã hóa, băm, và trao đổi khóa mà cả hai đều hỗ trợ.
* Xác thực server: Để đảm bảo rằng client đang kết nối với đúng server, server gửi public key của nó đến client. Client sẽ kiểm tra khóa này với danh sách các khóa mà nó đã lưu trước đó.
* Trao Đổi Khóa và Thiết Lập Kênh Mã Hóa: Để thiết lập kênh mã hóa bảo mật, SSH sử dụng thuật toán trao đổi khóa (thuật toán **Diffie-Hellman**)
* Xác Thực Người Dùng: Người dùng tiến hành gửi mật khẩu đã được mã khóa để server xác nhận.
  1. **Chức năng của SSH.**
* Cung cấp giao thức bảo mật cao cho các thông tin được trao đổi giữa client và server.
* Cung cấp giao thức bảo mật cho trao đổi file.
* Cho phép đăng nhập từ xa.
  1. **Ứng dụng của SSH.**
* Sử dụng trong datacenter: Giao thức SSH được sử dụng trong hầu hết datacenter.
* Ứng dụng cho hệ thống đăng nhập một lần: sử dụng trong hệ thống đăng nhập một lần SSO. Trong đó, người dùng có thể dễ dàng đăng nhập hoặc chuyển qua lại giữa các tài khoản một cách nhanh chóng.
* Mã hóa dữ liệu: SSH hỗ trợ mã hóa dữ liệu file, web, nhập lệnh …
* Xác thực thông tin: SSH có thể sử dụng để kết hợp với ID người dùng và mật khẩu khi xác thực thông tin.