A diagram of a mailing process

Description automatically generated with medium confidence

Phân tích quá trình thiết lập kết nối SSL:

* Trong mô hình giả định, ta có một Client (browser) cố gắng giao tiếp với Server.
* Đầu tiên, Client gửi lời chào đến Server.
* Thứ 2, Server tiếp nhận lời chào từ Client.
* Thứ 3, Server gửi chứng chỉ kèm khóa công khai của Server cho Client.
* Thứ 4, Server yêu cầu ngược lại chứng chỉ của Client.
* Thứ 5, Client gửi chứng chỉ của bản thân kèm public key của nó cho Server.
* Thứ 6, Client mã hóa Section key được tạo ra bởi Client bằng khóa công khai của Server và gửi tin nhắn muốn trao đổi khóa. Sau khi nhận tin thì Server dùng khóa bí mật của bản thân để giải mã và lấy được Section key chung của cả Client và Server.
* Thứ 7, Client gửi 1 tin nhắn chứng thực chứng chỉ của bản thân cho Server. Nhằm đảm bảo Section key được gửi từ phía Client chứ không phải bên nào khác, đồng thời đảm bảo tính toàn vẹn của thông điệp trao đổi khóa.
* Thứ 8 và thứ 9, cả 2 bên trao đổi xác nhận đã thiết lập kết nối với nhau và từ bây giờ khi trao đổi với nhau thì thông điệp sẽ được mã hóa bằng section key.