**HỌC VIỆN KỸ THUẬT MẬT MÃ**

KHOA CÔNG NGHỆ THÔNG TIN



BÁO CÁO MẬT MÃ ỨNG DỤNG

TRONG AN TOÀN THÔNG TIN

ĐỀ TÀI:

**XÂY DỰNG ỨNG DỤNG SỬ DỤNG THƯ VIỆN OPENSSL**

***Cán bộ hướng dẫn: Ths Bùi Hữu Đông***

***Sinh viên thực hiện:***

* ***Trần Thị Ngọc***
* ***Phan Hoàng Trung***
* ***Lê Thanh Lâm***
* ***Võ Lê Huy***

***Lớp: ATUD***

**THÁNG 12, 2020**

**HỌC VIỆN KỸ THUẬT MẬT MÃ**

KHOA AN TOÀN THÔNG TIN

BÁO CÁO MẬT MÃ ỨNG DỤNG

TRONG AN TOÀN THÔNG TIN

ĐỀ TÀI:

**XÂY DỰNG ỨNG DỤNG SỬ DỤNG THƯ VIỆN OPENSSL**

Nhận xét của cán bộ hướng dẫn:......................................................................................

..........................................................................................................................................

..........................................................................................................................................

..........................................................................................................................................

..........................................................................................................................................

Điểm chuyên cần:.............................................................................................................

Điểm báo cáo:...................................................................................................................

**Xác nhận của cán bộ hướng dẫn**

Mục lục

**LỜI MỞ ĐẦU**

sCông nghệ thông tin trong giai đoạn hiện nay đang có những bước phát triển như vũ bão trên mọi lĩnh vực hoạt động ở khắp nơi trên toàn thế giới, điều xảy ra trong vài năm vừa qua ở Việt Nam là sự đầu tư ồ ạt vào công nghệ. Tin học đã và đnag là một trong những vấn đề không thể thiếu đối với bất kỳ một tổ chức, công ty thậm chí cá nhân nào. Đặc biệt tin học ngày càng có vai trò quan trọng trong quá trình quảng bá cũng như giới thiệu về công ty hoặc cá nhân, do đó việc phát triển một website để quảng bá công ty hay một website cá nhân không còn gì xa lạ.

OpenSSL là 1 thư viện phần mềm cho toàn bộ các ứng dụng bảo mật truyền thông qua mạng máy tính phòng chống nghe trộm hoặc cần phải xác định phe truyền thông ở phía đầu bên kia. Chúng được ứng dụng rộng rãi trong các máy chủ web Internet nhằm phục vụ đa số các website hiện nay.

Do đó nhóm em đã lựa chọn “Xây dựng ứng dụng sử dụng thư viện OpenSSL” là đề tài trong báo cáo của mình.

***Nhóm em xin chân thành cảm ơn!***

# GIỚI THIỆU THƯ VIỆN OPENSSL

## Nền tảng?

Để tận dụng tối đa bài viết này, bạn nên:

* Thành thạo lập trình C.
* Làm quen với giao tiếp Internet và viết các ứng dụng hỗ trợ Internet.

Không nhất thiết phải làm quen với SSL, vì phần giải thích ngắn gọn về SSL sẽ được đưa ra sau. Kiến thức về mật mã cũng là một lợi thế, nhưng không bắt buộc.

## SSL là gì?

SSL là từ viết tắt của Secure Sockets Layer. Nó là tiêu chuẩn đằng sau giao tiếp an toàn trên Internet, tích hợp mật mã dữ liệu vào giao thức. Dữ liệu được mã hóa trước khi nó rời khỏi máy tính của bạn và chỉ được giải mã khi nó đến đích dự kiến. Chứng chỉ và thuật toán mật mã đứng đằng sau cách tất cả hoạt động và với OpenSSL, bạn có cơ hội để chơi với cả hai.

Về lý thuyết, nếu dữ liệu mã hóa bị chặn hoặc bị nghe trộm trước khi đến đích thì không có hy vọng bẻ khóa dữ liệu đó. Nhưng khi các máy tính ngày càng nhanh hơn khi mỗi năm trôi qua và những tiến bộ mới trong phân tích mật mã được tạo ra, thì cơ hội bẻ khóa các giao thức mật mã được sử dụng trong SSL đang bắt đầu tăng lên.

SSL và các kết nối an toàn có thể được sử dụng cho bất kỳ loại giao thức nào trên Internet, cho dù đó là HTTP, POP3 hay FTP. SSL cũng có thể được sử dụng để bảo mật các phiên Telnet. Mặc dù mọi kết nối đều có thể được bảo mật bằng SSL, nhưng không nhất thiết phải sử dụng SSL trên mọi loại kết nối. Nó nên được sử dụng nếu kết nối sẽ mang thông tin nhạy cảm.

## OpenSSL là gì?

Từ trang Web OpenSSL:

* Dự án OpenSSL là một nỗ lực hợp tác để phát triển một công cụ mạnh mẽ, cấp thương mại, đầy đủ nổi bật và bộ công cụ Nguồn mở triển khai Lớp cổng bảo mật (SSL v2 / v3) và Các giao thức Bảo mật lớp truyền tải (TLS v1) cũng như một mật mã có mục đích chung toàn năng- thư viện raphy. Dự án được quản lý bởi một cộng đồng tình nguyện viên trên toàn thế giới sử dụng Internet để giao tiếp, lập kế hoạch và phát triển bộ công cụ OpenSSL và tài liệu liên quan của nó.
* OpenSSL dựa trên thư viện SSLeay tuyệt vời được phát triển bởi Eric A. Young và Tim J. Hudson. Bộ công cụ OpenSSL được cấp phép theo giấy phép kiểu Apache, về cơ bản có nghĩa là mà bạn có thể tự do lấy và sử dụng nó cho các mục đích thương mại và phi thương mại tùy thuộc vào một số điều kiện giấy phép đơn giản.

Nói tóm lại, OpenSSL là một thư viện phần mềm cung cấp một bộ công cụ mật mã đầy đủ tính năng như một triển khai của SSL. Phiên bản Unix, mà chúng tôi sẽ sử dụng, cung cấp hai thư viện, một cho SSL / TLS (ssl) và một cho bộ công cụ mật mã (tiền điện tử) cũng như công cụ dòng lệnh (OpenSSL).