Bài tập 6

Bài 1: Lập bảng mô tả 6 hệ thống chứng thực số (3 ở nước ngoài và 3 ở Việt Nam): Đặc điểm, dịch vụ đi kèm, giá cả, quy mô...

	Đặc điểm	Dịch vụ	Giá cả	Quy mô
BkavCA	Là dịch vụ chứng thực chữ ký số công cộng do Công ty Cổ phần BKAV quản lý, được Bộ Thông tin và Truyền thông cấp phép. Đảm bảo xác thực danh tính cao, với các loại chứng thư như SSL (mã hóa 256-bit), CodeSigning, và Client. Tuân thủ RFC 3647, Thông tư 31/2020/TT-BTTTT, và các quy định khác. Sử dụng HSM đạt chuẩn FIPS 140-2 cấp 3 cho lưu trữ khóa bí mật, với khóa RSA 1024/2048 bits.	Cung cấp phát hành, quản lý, gia hạn, và thu hồi chứng thư số. Hỗ trợ kiểm tra trạng thái chứng thư qua CRL và OCSP, hoạt động 24/7. Không cung cấp dịch vụ đóng dấu thời gian hiện tại. Dữ liệu thuê bao được lưu trữ ít nhất 5 năm sau khi chứng thư hết hạn, truy cập tại https://directory.bkavca.vn	Giá tùy thuộc vào thời hạn 1 đến 3 năm dao động từ 1.150.000VNĐ đến 1.826.00 VNĐ	Hoạt động dưới RootCA của Cổng Dịch vụ Công Quốc gia, phục vụ cá nhân và tổ chức. Có trung tâm dữ liệu tại IDC Hòa Lạc (Km 29, ĐCT08, Thạch Hoà, Thạch Thất, Hà Nội) và VNPT IT (136 Nguyễn Phong Sắc, Cầu Giấy, Hà Nội), với khả năng khôi phục trong 24 giờ sau thảm họa, đồng bộ dữ liệu hàng ngày.
FPT-CA	Thuộc Hệ thống Thông tin FPT (FPT IS), được Bộ Thông tin và Truyền thông cấp phép. Là một phần của hệ sinh thái công nghệ	Cung cấp phát hành, quản lý, gia hạn chứng thư số, hỗ trợ giao dịch như kê khai thuế, hải quan, hóa đơn điện tử. Có dịch vụ ký số từ xa không cần USB Token/SIM, đảm bảo an toàn và không giới hạn giao dịch. Hỗ trợ 24/7, với	Giá cho đăng ký mới dao động từ 1.350.000 VNĐ đến 1.850.000 VNĐ	Phủ sóng toàn quốc, phục vụ cá nhân và doanh nghiệp, với hạ tầng bảo mật đa tầng (4 cấp: nhân viên an

	FPT, tập trung vào chứng thực chữ ký số cho giao dịch điện tử. Tuân thủ các tiêu chuẩn quốc tế và quy định Việt Nam, sử dụng HSM đạt chuẩn FIPS 140-2 cấp 2 trở lên.	khôi phục thảm họa trong 72 giờ.		ninh, thẻ truy cập, sinh trắc học, mô hình M/N cho hoạt động CA). Đội ngũ nhân viên được đào tạo chuyên sâu, kiểm tra lý lịch mỗi 5 năm.
Viettel-CA	Do Tập đoàn Công nghiệp - Viễn thông Quân đội (Viettel) cung cấp, được cấp phép ngày 05/10/2020 bởi Bộ Thông tin và Truyền thông. Đạt tiêu chuẩn bảo mật quốc tế, phát triển bởi đội ngũ kỹ sư CNTT hàng đầu, với hệ thống bảo mật đa lớp.	Hỗ trợ các giao dịch điện tử như kê khai thuế, hải quan, bảo hiểm xã hội, hóa đơn điện tử, ngân hàng số. Cung cấp chứng thư số trên USB Token, hỗ trợ 24/7 miễn phí qua hotline 18008000 Nhánh 1. Có hướng dẫn chi tiết như thay đổi thông tin, gia hạn chủ động trên Token Manager Viettel	Viettel-CA có nhiều gói cước khác nhau cho chữ ký số doanh nghiệp, cá nhân, di động và máy chủ, với thời hạn từ 1 đến 3 năm. Giá cho đăng ký mới chữ ký số doanh nghiệp dao động từ 1.390.000 VNĐ đến 1.890.000 VNĐ. Giá cho gia hạn dao động từ 950.000 VNĐ đến 1.790.000 VNĐ. Các gói này thường bao gồm VAT và USB token	Phủ sóng toàn quốc với mạng lưới 63 chi nhánh, là nhà cung cấp hàng đầu với thị phần lớn, phục vụ hàng triệu khách hàng nhờ mạng lưới viễn thông Viettel.
DigiCert	Là cơ quan chứng thực hàng đầu, chuyên về	Cung cấp SSL/TLS, ký mã, ký tài liệu, và quản lý vòng đời chứng thư qua nền tảng DigiCert ONE.	igiCert cung cấp các gói dịch vụ TLS/SSL khác	Phục vụ toàn cầu, là nhà cung cấp chính

	PKI, IoT, DNS, và bảo mật phần mềm. Cung cấp chứng thư với các mức xác thực khác nhau (DV, OV, EV), tuân thủ các tiêu chuẩn quốc tế như RFC 3647. Được tin dùng bởi phần lớn Global 2000, với công nghệ hiện đại như HSM đạt chuẩn FIPS 140-2.	Hỗ trợ tự động hóa, phát hiện, và quản lý chứng thư, với khả năng tích hợp IoT và DNS	nhau dựa trên mức độ xác thực (OV, EV) và loại chứng thư (Single Domain, Wildcard, Multi-Domain). Giá khởi điểm cho chứng thư OV Single Domain là 26 USD/tháng và cho chứng thư EV Single Domain là 39 USD/tháng. Các gói Secure Site và Secure Site Pro có giá cao hơn và đi kèm với nhiều tính năng bổ sung	cho các doanh nghiệp lớn, với hạ tầng bảo mật toàn diện và khả năng xử lý hàng triệu chứng thư.
GlobalSign	Thành lập từ năm 1996, là một trong 4 CA lớn nhất thế giới (theo Netcraft, 2015), cung cấp chứng thư SSL/TLS, ký mã, và xác thực danh tính. Đạt tiêu chuẩn bảo mật quốc tế, hỗ trợ HSM trên đám mây như Azure Key-Vault, AWS CloudHSM.	Cung cấp chứng thư DV, OV, EV, ký mã (EV và OV), ký tài liệu, và dịch vụ PKI quản lý. Hỗ trợ tự động hóa quản lý chứng thư, với CPS	Giá chứng chỉ số GlobalSign thay đổi tùy theo loại chứng chỉ, với SSL xác thực tên miền (DV) bắt đầu từ 249 đô la một năm, SSL xác thực tổ chức (OV) từ 349 đô la và SSL xác thực mở rộng (EV) từ 599 đô la, với các tùy chọn ký tự đại	Hoạt động toàn cầu, phục vụ nhiều quốc gia, với đội ngũ đa dạng và công nghệ tiên tiến, là đối tác chiến lược của nhiều doanh nghiệp lớn.

			diện làm tăng thêm chi phí.	
Sectigo	Trước đây là Comodo CA, là CA thương mại lớn nhất, phát hành hơn 100 triệu chứng thư trên 150 quốc gia. Cung cấp chứng thư SSL/TLS với mã hóa RSA, DSA, ECC, tuân thủ các tiêu chuẩn quốc tế.	Cung cấp SSL/TLS, ký mã, ký email (S/MIME), và nền tảng quản lý chứng thư (Certificate Manager)	Chứng chỉ SSL ectigo có giá khởi điểm khoảng 67 đô la một năm cho chứng chỉ Xác thực tên miền (DV) và có thể tăng lên tùy theo cấp độ xác thực, số lượng tên miền và gói đăng ký đã chọn.	Phục vụ toàn cầu, với hạ tầng mạnh mẽ, hỗ trợ hàng trăm nghìn khách hàng, bao gồm các thương hiệu lớn.

Bài 2: Phân tích sự khác nhau giữa kết nối Client-to-site và Site-to-site trong giao thức IPSec.

	Client-to-site	Site-to-site
Mục đích sử dụng	Được thiết kế để kết nối một thiết bị cá nhân (ví dụ: máy tính xách tay, điện thoại) từ xa vào mạng nội bộ của tổ chức, thường phục vụ cho nhân viên làm việc từ xa.	Kết nối hai hoặc nhiều mạng riêng biệt (ví dụ: trụ sở chính và chi nhánh) thành một mạng ảo thống nhất, cho phép trao đổi dữ liệu liên mạng tự động.
Đối tượng tham gia	Một thiết bị cá nhân (client) kết nối đến cổng VPN (gateway) của mạng đích.	Hai cổng VPN (gateway) tại các mạng khác nhau thiết lập kết nối trực tiếp với nhau.
Cấu hình và triển khai	Yêu cầu cài đặt phần mềm VPN client trên thiết bị người dùng. Người dùng khởi tạo kết nối thủ công hoặc tự động khi cần truy cập.	Triển khai trên thiết bị mạng (router, firewall) tại mỗi site. Kết nối thường luôn duy trì (always-on) và tự động mã hóa lưu lượng giữa các site.
Xác thực:	Sử dụng xác thực người dùng (username/password, certificate, OTP) kết hợp xác thực thiết bị.	Xác thực dựa trên thiết bị mạng, thường dùng pre-shared key (PSK) hoặc

		chứng chỉ số (digital certificate).
Định tuyến lưu lượng	Chỉ mã hóa lưu lượng từ thiết bị client đến mạng đích; các kết nối khác (ví dụ: truy cập web thông thường) không đi qua VPN.	Mã hóa toàn bộ lưu lượng giữa các mạng được kết nối, không phụ thuộc vào thiết bị cụ thể.
Tính mở rộng	Phù hợp với quy mô nhỏ, tập trung quản lý người dùng từ xa.	Phù hợp với quy mô lớn, kết nối nhiều site với lưu lượng ổn định.
Chế độ IPSec	Thường dùng chế độ Tunnel để đóng gói toàn bộ gói tin, nhưng có thể kết hợp với giao thức khác (như IKEv2) để linh hoạt hơn.	Hầu hết sử dụng chế độ Tunnel để bảo vệ toàn bộ IP header và payload.
Bảo mật	Rủi ro cao hơn do thiết bị client có thể không đảm bảo an toàn (ví dụ: malware). Thường áp dụng thêm kiểm tra thiết bị (NAC).	An toàn hơn do kết nối giữa các gateway đã được kiểm soát chặt chẽ, nhưng đòi hỏi cấu hình tường lửa phức tạp.
Ví dụ ứng dụng	Nhân viên truy cập vào file server công ty từ nhà.	Chi nhánh tại Hà Nội và TP.HCM chia sẻ dữ liệu qua VPN như trong cùng một mạng LAN.

Bài 3: Mô tả quá trình thiết lập kết nối SSL.
SSL/TLS là giao thức bảo mật tại tầng vận chuyển, được sử dụng để thiết lập kênh truyền thông an toàn giữa client và server. Quá trình này gồm các bước sau:

1. ClientHello
- Client gửi thông điệp ClientHello đến server, bao gồm:
  - Phiên bản SSL/TLS hỗ trợ (ví dụ: TLS 1.2, TLS 1.3).
  - Danh sách cipher suites (bộ giải thuật mã hóa, ví dụ: AES-256, SHA-256, RSA).
  - Một số ngẫu nhiên (Client Random) dùng để tạo khóa phiên.

2. ServerHello
- Server phản hồi bằng thông điệp ServerHello, chứa:
  - Phiên bản SSL/TLS được chọn.

    - Cipher suite đã thống nhất từ danh sách client cung cấp.
    - Số ngẫu nhiên (Server Random) để tạo khóa phiên.

3. Xác thực server (Server Certificate)
- Server gửi chứng chỉ số (digital certificate) cho client để xác thực danh tính.
- Chứng chỉ chứa khóa công khai của server và được ký bởi CA (Certificate Authority) đáng tin cậy.
- Client kiểm tra chứng chỉ:
    - Xác minh chữ ký CA.
    - Kiểm tra thời hạn và tên miền (domain) của chứng chỉ.

4. Trao đổi khóa (ServerKeyExchange)
- Server gửi thông tin khóa công khai (nếu sử dụng giao thức trao đổi khóa như Diffie-Hellman).
- Trong trường hợp dùng RSA, client sẽ tự sinh khóa phiên (pre-master secret) và mã hóa bằng khóa công khai của server.

5. ClientKeyExchange
- Client gửi pre-master secret đã mã hóa (bằng khóa công khai của server) đến server.

- Cả client và server dùng Client Random, Server Random, và pre-master secret để tính toán master secret → tạo khóa phiên (session key) dùng mã hóa dữ liệu.

6. Xác thực client (tuỳ chọn)
- Nếu server yêu cầu, client gửi chứng chỉ số của mình để xác thực.

7. ChangeCipherSpec
- Client và server gửi thông điệp ChangeCipherSpec để thông báo:
- Từ thời điểm này, mọi dữ liệu sẽ được mã hóa bằng khóa phiên đã thống nhất.

8. Finished
- Client và server gửi thông điệp Finished đã mã hóa để xác nhận quá trình bắt tay hoàn tất.
- Thông điệp này chứa hash của toàn bộ quá trình bắt tay, đảm bảo tính toàn vẹn và chống giả mạo.

9. Truyền dữ liệu an toàn
- Sau khi kết nối được thiết lập, client và server trao đổi dữ liệu qua kênh mã hóa bằng khóa phiên.
- Các thuật toán mã hóa phổ biến: AES (256-bit), SHA-256 (hàm băm), RSA (trao đổi khóa).