

TRƯỜNG ĐẠI HỌC CÔNG NGHIỆP  
THÀNH PHỐ HỒ CHÍ MINH  
KHOA CÔNG NGHỆ THÔNG TIN

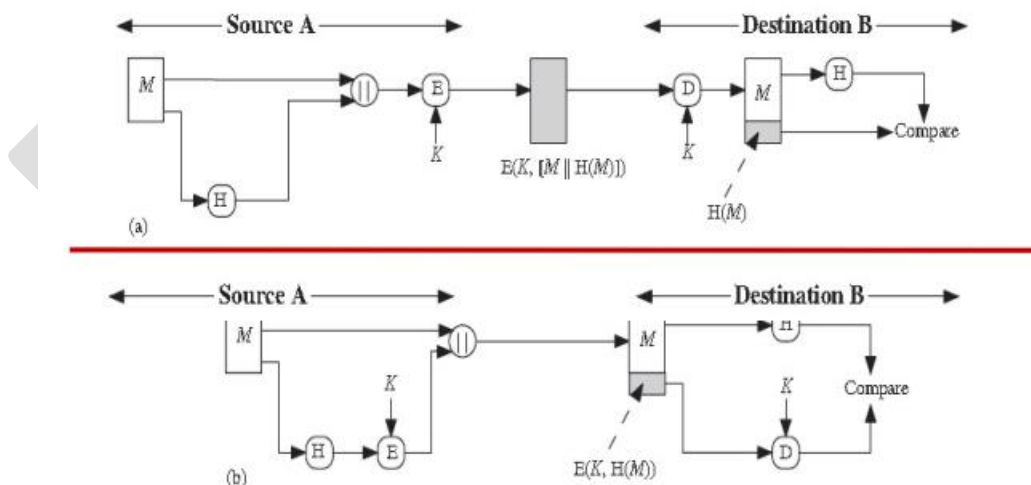
Kết thúc môn học: Nhập Môn ATTT  
Lớp học phần : DHKHM17B  
Ngày kiểm tra : 05/2024  
Thời gian làm bài : 60 phút  
(Không kể thời gian phát đề)

**Câu 1 (3đ):**

Cho  $p = 7$ ,  $q = 11$ ,  $e = 13$

- (1đ) hãy tạo và phát sinh khóa Công khai PU và khóa riêng PR bằng mã hóa bất đối xứng RSA
- (1đ) Hãy thực hiện mã hóa chứng thực với  $M_1 = 8$
- (1đ) Hãy thực hiện mã hóa bảo mật với  $M_2 = 9$

**Câu 2 (2đ):** Nêu khái niệm, đặc điểm hàm băm, và các ứng dụng của hàm băm. Giải thích được sơ đồ sau? So sánh 2 sơ đồ a và b



**Câu 3 (5đ):** Cửa hàng trực tuyến của công ty ABC có nhiệm vụ cung cấp các sản phẩm đa dạng cho khách hàng. Hiện nay, công ty có một website [www.trangthuongmaidientu.com/](http://www.trangthuongmaidientu.com/) để khách hàng xem, đặt hàng và thanh toán trực tuyến. Sau khi hoàn tất mua hàng, khách hàng cũng có thể theo dõi tình trạng đơn hàng và lịch sử mua sắm qua website này. Khi đặt hàng, khách hàng cần cung cấp đầy đủ thông tin cá nhân để cửa hàng lưu trữ và quản lý. Khi thanh toán trực tuyến, khách hàng phải cung cấp thông tin về thẻ ngân hàng hoặc phương thức thanh toán khác. Thông tin chi tiết về các sản phẩm cũng được cung cấp trên website để khách hàng tham khảo và lựa chọn. Nhân viên sau khi xử lý đơn hàng sẽ cập nhật trạng thái và thông tin giao hàng thông qua website.

Một trang web có đường link xem chi tiết sản phẩm như sau:  
[www.trangthuongmaidientu.com/sanpham.php?id\\_sanpham=2](http://www.trangthuongmaidientu.com/sanpham.php?id_sanpham=2)

Yêu cầu:

1. Hãy trình bày 2 loại thông tin / dữ liệu / chức năng nào cần nâng cao tính an toàn thông tin và nêu lý do tại sao?
2. Đưa ra giải pháp nào để cài đặt nâng cao tính an toàn cho từng loại thông tin/dữ liệu/chức năng ở trên và nêu lý do tại sao phương pháp pháp này là hữu hiệu. Trình bày giải pháp khắc phục cho loại tấn công hoặc lỗ hổng trên.

---

(Sinh viên được sử dụng tài liệu chép tay).

© 2024 – Hồ Phúc Lâm

Tài liệu tham khảo này được HPLamIT sưu tầm và chia sẻ với mục đích hỗ trợ học tập. Vui lòng không sử dụng tài liệu này cho các mục đích thương mại hoặc không chính đáng. Chúng tôi trân trọng sự tôn trọng và tuân thủ bản quyền của bạn.