Nhập môn An Toàn thông tin

Nội dung ôn tập cuối kỳ

- Sinh viên được tham khảo tài liệu tự soạn chép tay không giới hạn (không được dùng tài liệu in, photo)
- Thời gian: 60 phút; Hình thức: Tự luận
- Các tình huống mang tính minh họa.

LO3 – Áp dụng được một số lý thuyết toán trong các hệ mật mã

- Thực hiện được việc mã hóa bằng các thuật toán như Caesar hoặc Playfair.
- Phát sinh một cặp khóa bằng mật mã bất đối xứng (RSA)
- Thực hiện mã hoá và giải mã (bảo mật)
- Thực hiện ký và thẩm tra chữ ký số (chứng thực)

LO4 - Giải thích được các khái niệm cơ bản về An toàn thông tin, hệ mã hóa

Giải thích các khái niệm như an toàn thông tin, tam giác CIA, mật mã học, mã hóa đối xứng và bất đối xứng, hàm băm, chữ ký số, chứng thực thực thể, chứng thực thông điệp, các loại khóa, quản lý khóa.

LO5 - Mô tả được tổng quan cơ chế / giao thức để thiết lập và nâng cao tính an toàn thông tin cho một tình huống cụ thể

Cho một tình huống có thể áp dụng các giải pháp an toàn thông tin. Sinh viên đưa ra và mô tả các cơ chế / phương thức có thể thiết lập và nâng cao an toàn thông tin phù hợp với tình huống đó. Các cơ chế / phương thức có thể gồm Mã hóa khóa bí mật, mã hóa khóa công khai, chữ ký số, khóa phiên, trao đổi khóa, chứng thực thực thể, chứng thực thông điệp.

Câu hỏi LO3 tham khảo:

1. Áp dụng mật mã Ceasar mã hóa bản rõ sau với khóa k = 4
   Actions speak louder than works
2. Áp dụng mật mã Playfair mã hóa bản rõ sau với khóa K = tinhoc
   Dai hoc cong nghiep
3. Cho p = 7, q = 11, e = 17. Hãy thực hiện phát sinh khóa công khai và khóa riêng theo cơ chế RSA.
   a. Mã hoá và giải mã bảo mật cho thông điệp M = 9 (mã hóa bảo mật)
      Mã hoá: $C = M^e \bmod n$
      Giải mã: $M = C^d \bmod n$
   b. Tạo và thẩm tra chữ ký RSA (mã hóa chứng thực) cho thông điệp M = 9
      Tạo chữ ký: $S = M^d \bmod n$
      Thẩm tra: $M = S^e \bmod n$

Câu hỏi LO4 tham khảo:

1. Khóa phiên (Session key) là gì? Khóa phiên có ưu điểm gì so với khóa bí mật chia sẻ (secret shared key)? Trình bày và giải thích một giao thức phát sinh khóa phiên mà bạn biết.
2. Chứng thực thực thể bằng sinh trắc học (biometrics) là gì? Trình bày các thành phần cơ bản cần có trong một hệ thống chứng thực sinh trắc học (ví dụ vân tay). Nêu ưu điểm và nhược

điểm của phương pháp này. Ở Việt Nam, phương pháp chứng thực sinh trắc học hiện nay được áp dụng ở những lĩnh vực nào?

3. Điều khiển truy cập là gì? Trình bày ít nhất 2 phương pháp mà bạn biết mà có thể cài đặt điều khiển truy cập một hệ thống thông tin.
4. Mật khẩu (password) là gì? Mật khẩu cố định (fixed password) và mật khẩu dùng một lần (one time password) khác nhau như thế nào? Trình bày điểm mạnh và điểm yếu của 2 loại mật khẩu.
5. Trình bày các loại mã OTP, nêu ưu điểm và nhược điểm của từng loại. Đưa ra một hệ thống mà bạn biết có sử dụng mật khẩu dùng một lần (one time password) và mô tả tình huống mà bạn có sử dụng mật khẩu để chứng thực người dùng/giao dịch. Nêu mục tiêu của việc chứng thực này.
6. Chữ ký số (digital signitures) là gì? Mục tiêu của chữ ký số? Trình bày hiện trạng áp dụng chữ ký số ở Việt Nam
7. Gợi ý: Khái niệm chữ ký số: ứng dụng của mã hóa khóa công khai, người dùng có (KUA, KRA); Tạo chữ ký: SAM = E(KRA, M) hoặc SAM=E(KRA, H(M)) – giải thích; Thẩm tra chữ ký D(KUA, SAM) → Yes/No – Giải thích; Mục tiêu của chữ ký số; Hiện trạng áp dụng chữ ký: 4 lĩnh vực đó là cơ quan Thuế, Bảo hiểm xã hội, Hải quan và Chứng khoán.
8. Mô tả chứng thư số là gì? Mục tiêu của chứng thư số? Nội dung có trong chứng thư số là gồm những nội dung gì?
9. Hệ thống quản lý an toàn thông tin (ISMS) là gì? Mục tiêu của hệ thống an toàn toàn thông tin?
10. Trình bày các đặc điểm của hàm băm? Trình bày giải pháp xử lý mật khẩu trước khi lưu vào cơ sở dữ liệu và giải thích vì sao?
11. SSL là gì? Tại sao cần cài SSL? Dấu hiệu nhận biết một website có cài SSL? Cách thức hoạt động của SSL?
12. Tường lửa là gì? Có mấy loại và nêu tác dụng của tuần loại?
13. Trình bày phương pháp phát hiện và ngăn chặn/tiêu diệt mã độc của phần mềm Antivirus? Qua đó giải thích vì sao phải thường xuyên cập nhật phần mềm Antivirus?
14. Ransomware là gì? Cách thức hoạt động và giải pháp bảo vệ dữ liệu trước Ransomware?

Câu hỏi LO5 tham khảo:

Tình huống 1:
Để phục vụ cho nhu cầu học tập và tra cứu của cán bộ, giảng viên và sinh viên của trường, nhà trường đã xây dựng một ***Hệ thống thư viện trực tuyến www.thuviendientu.iuh.edu.vn***, hệ thống giúp độc giả (cán bộ, giảng viên và sinh viên của trường) có thể tìm kiếm các loại sách, báo, tạp chí,… Đối với tài liệu điện tử thì độc giả có thể đọc trực tuyến hoặc tải về, đối với sách trong thư viện thì độc giả có thể đăng ký mượn. Độc giả cũng có thể yêu cầu mua các loại tài liệu điện tử và thanh toán phí mua trực tuyến. Hệ thống cũng giúp cho các thủ thư có thể quản lý thông tin mượn và trả sách của độc giả, hệ thống còn có tính năng thông báo nhắc nhở đến hạn trả sách bằng email, tạo báo cáo, thống kê.
Yêu cầu: Với tình huống đã cho, bạn hãy

1. Chỉ ra ít nhất 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.

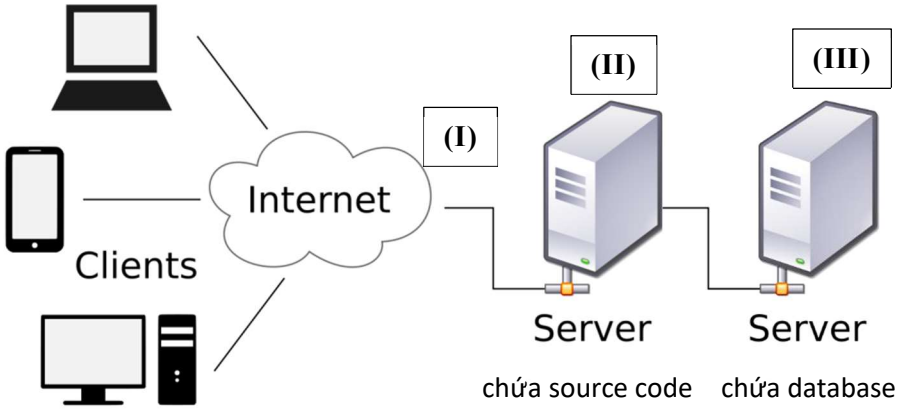
Tình huống 2:
Một trang web có đường link xem chi tiết sản phẩm như sau:

www.trangthuongmaidientu.com/sanpham.php?id_sanpham=2

Yêu cầu:

1. Theo bạn, cách truyền biến như trang web có đường link trên dễ bị loại tấn công hay lỗ hổng gì? Giải thích vì sao?
2. Trình bày giải pháp khắc phục cho loại tấn công hoặc lỗ hổng trên?

Tình huống 3:
Một hệ thống thông tin có hai máy chủ, một server dùng để chứa phần mềm (II), một server dùng để chứa cơ sở dữ liệu (III) và đường truyền (I) Internet để kết nối đến các máy khách (clients) như hình:



Yêu cầu:

1. Hãy nêu ra 2 rủi ro về an toàn thông tin có thể xảy ra trên đường truyền hoặc trên các máy chủ.
2. Trình bày các giải pháp giúp tăng cường an toàn cho hệ thống trong quá trình truyền tải ở (I), cho phần mềm ở (II) và dữ liệu lưu trữ ở (III)? Giải thích vì sao?