**Đồ án lý thuyết cuối kỳ khóa 2013 (học kỳ 2/2015-2016)**

🞎 Bài tập cá nhân 🗹 Bài tập nhóm (nhóm tối đa 02 sinh viên)

🞎 Bài tập tự luyện tập 🗹 Bài tập cần nộp (Đồ án cuối kỳ)

**Quy định về đồ án lý thuyết:**

* **Yêu cầu:** mỗi nhóm sinh viên tự chọn 1 trong 2 chủ đề dưới đây để thực hiện

Các yêu cầu chức năng nêu trong phần mô tả của mỗi chủ đề ***chỉ là gợi ý***. Mỗi nhóm sinh viên có thể ***chủ động đề xuất***, thay đổi, điều chỉnh, bổ sung các yêu cầu, tính năng, ngữ cảnh.

1. Hãy xác định vấn đề về an toàn thông tin (security) có thể có trong hệ thống. Với mỗi vấn đề mà nhóm xác định được, hãy phát biểu chặt chẽ, rõ ràng, và giải thích rõ tình huống có thể xảy ra vấn đề này (nêu trình bày dạng mô hình hoặc ví dụ trực quan).
2. Trình bày giải pháp mà nhóm đề xuất để giải quyết các vấn đề mà nhóm đã xác định.

* **Thời hạn nộp bài**: theo thông báo của Giảng viên
* **Cách nộp**: nộp bài trên Website môn học vào mục **Đồ án lý thuyết cuối kỳ.**
* **Nội dung đồ án lý thuyết gồm:** 1 tập tin báo cáo về đề tài của nhóm. Trong file báo cáo cần ghi rõ thông tin của nhóm, bao gồm:
* Họ tên
* Mã số sinh viên
* Điện thoại
* Email liên hệ
* **Quy tắc đặt tên khi nộp bài:**
* Mỗi nhóm sinh viên có thể nộp tối đa **20 file**, mỗi file có **kích thước tối đa 12MB**. Nếu sinh viên chia file nén (ZIP/RAR) thành nhiều file nhỏ, cần kiểm tra kỹ nộp đầy đủ tất cả các file này.
* Tên file được đặt là MSSV1-MSSV2.\* nếu làm theo nhóm (với quy ước MSSV1 < MSSV2) hoặc MSSV.\* nếu làm cá nhân.
* **Lưu ý:**
* Sinh viên nên chủ động đề xuất các ý tưởng, giải pháp cho bài làm của nhóm mình.
* Những bài giống nhau hoặc giống bài làm của khóa trước, tùy theo mức độ vi phạm, sẽ bị 0 điểm hoặc bị trừ điểm.

# Chủ đề 01: Hệ thống quản lý tàu điện ngầm

*(chủ đề này được sử dụng từ đề thi môn Phân tích thiết kế phần mềm)*

Tàu điện ngầm (metro) là phương tiện giao thông công cộng phổ biến ở nhiều quốc gia trên thế giới. Tại nhiều thành phố, hệ thống các tuyến tàu điện ngầm được xây dựng thành mạng lưới trải rộng, cho phép người dân đi lại dễ dàng, tiện lợi và an toàn.

Công ty của bạn vừa nhận được dự án xây dựng hệ thống phần mềm e-Metro quản lý việc sử dụng hệ thống tàu điện ngầm của thành phố. Hệ thống có các chức năng sau:

* Quản lý các công ty tàu điện ngầm:
  + Thành phố có nhiều công ty tàu điện ngầm (company). Mỗi công ty có tên, địa chỉ website, địa chỉ trụ sở chính, số điện thoại liên lạc.
  + Phần mềm cho phép nhân viên của Sở giao thông thành phố quản lý thông tin của các công ty tàu điện ngầm (gồm thêm mới, tra cứu và cập nhật thông tin).
  + Khi cập nhật, nhân viên có thể sử dụng chức năng tra cứu công ty.
  + Không được phép xóa thông tin của bất kỳ công ty nào.
* Quản lý các ga:
  + Mỗi ga có một mã số (duy nhất), tên ga (thường là tên địa điểm của ga), mô tả vị trí, tình trạng hoạt động của ga (bình thường, đang sửa chữa, hay đã ngừng hoạt động).
  + Ngoài ra, mỗi ga còn có 1 bản đồ (dạng ảnh) chi tiết đường đi trong ga và các cổng ra vào ga (mỗi ga có thể có nhiều cổng ra vào ở nhiều hướng khác nhau).
  + Phần mềm cho phép nhân viên của Sở giao thông thành phố thêm mới, tra cứu, cập nhật thông tin của các ga.
  + Khi cập nhật, nhân viên luôn sử dụng chức năng tra cứu ga.
  + Không được phép xóa thông tin của bất kỳ ga nào.
* Quản lý các tuyến tàu điện ngầm:
  + Mỗi tuyến tàu chỉ duy nhất một công ty khai thác.
  + Mỗi tuyến có mã số (duy nhất), tên tuyến, xuất phát từ một ga, đi qua một số ga trung gian (kèm theo thời gian dừng tại mỗi ga – nếu có) và dừng tại một ga cuối.
  + Có 2 loại tuyến:
    - Tuyến tốc hành: trong lộ trình, tàu sẽ không dừng lại tại một số ga trung gian. Vì vậy, cần phải ghi nhận trong thông tin tàu có dừng lại hay không tại mỗi ga trung gian!
    - Tuyến thường: tàu dừng lại tại tất cả ga trung gian để khách rời tàu và đón thêm khách lên tàu.
  + Giá vé của mỗi tuyến tàu do công ty quy định (có thể thay đổi theo thời gian). Hành khách đi trọn tuyến hay chỉ đi 1 phần của tuyến đều mua vé với giá vé này.
  + Mỗi tuyến tàu có giờ bắt đầu hoạt động (vd: 5 giờ sáng), giờ chấm dứt hoạt động (vd: 12giờ đêm), khoảng thời gian chờ trung bình giữa 2 chuyến tàu liên tiếp của tuyến (vd: mỗi 10 phút sẽ có 1 chuyến tàu).
  + Ngoài ra còn có thông tin về tình trạng tuyến tàu (còn hoạt động hay không).
  + Việc quản lý thông tin của các tuyến tàu được nhân viên của mỗi công ty thực hiện (không phải nhân viên của Sở giao thông thành phố). Hệ thống phần mềm cho phép thêm mới, tra cứu, cập nhật thông tin của các tuyến tàu của công ty mình.
  + Khi cập nhật, nhân viên luôn sử dụng chức năng tra cứu tuyến tàu.
  + Không được phép xóa thông tin tuyến tàu.
* Bán vé:
  + Tại quầy vé ở mỗi ga, khách có thể mua vé theo một trong hai cách:
    - Mua vé tại quầy vé: Nhân viên bán vé sẽ bán vé cho khách. Khi đó, hệ thống e-Metro sẽ ghi nhận việc bán vé và in vé.
    - Khách tự mua vé tại các máy bán vé tự động: Việc xử lý tại mỗi máy bán vé do phần mềm chuyên dụng được cài đặt sẵn trong máy bán vé thực hiện. Khi bán vé thành công, máy bán vé sẽ tự in và xuất vé cho khách, sau đó sẽ kết nối vào hệ thống e-Metro để yêu cầu ghi nhận việc bán vé (hệ thống e-Metro không cần in vé).
    - Cần lưu ý là việc xây dựng và phát triển hệ thống máy bán vé tự động (bao gồm cả phần cứng và phần mềm) không thuộc phạm vi hệ thống e-Metro.
  + Có 2 loại vé:
    - Vé thông thường:
      * Mỗi vé có mã số vé (phân biệt), mã số tuyến, giá vé (tại thời điểm mua).
      * Hành khách sẽ mua 01 vé cho mỗi lần đi mỗi chuyến tàu (vé dùng 1 lần). Giá vé tùy thuộc tuyến tàu mà hành khách chọn (dù hành khách chỉ đi 1 phần của tuyến nhưng vẫn mua vé trọn tuyến).
      * Vé hợp lệ là vé chưa sử dụng lần nào.
    - Vé tháng:
      * Mỗi công ty phát hành vé tháng cho mỗi tuyến mà khách cần đi. Mỗi vé tháng có hiệu lực 30 ngày (từ khi mua), chỉ sử dụng được trên 1 tuyến cố định của công ty.
      * Mỗi vé tháng có mã số vé (phân biệt), mã số tuyến, giá vé (tại thời điểm mua), ngày mua.
      * Vé hợp lệ là vé còn hạn sử dụng.
* Kiếm soát vé:
  + Tại mỗi lối vào của mỗi ga có đặt sẵn các cổng soát vé tự động, khách sẽ sử dụng vé đã mua để vào cổng. Cổng soát vé xác định mã số vé và kết nối vào hệ thống e-Metro để kiểm tra tính hợp lệ của vé. Hệ thống e-Metro sẽ kiểm tra tính hợp lệ của vé. Nếu vé hợp lệ, hệ thống sẽ cập nhật thông tin của vé:
    - với vé thông thường, e-Metro sẽ ghi nhận tình trạng vé là đã sử dụng (không dùng lại được nữa) và thời điểm sử dụng vé
    - với vé tháng, e-Metro sẽ ghi nhận thêm 1 lần sử dụng vé (ghi nhận thời điểm sử dụng)

Nếu kết quả kiểm tra của hệ thống e-Metro xác nhận vé là hợp lệ, cổng soát vé tự động sẽ mở để hành khách vào ga. Cần lưu ý là việc xây dựng và phát triển hệ thống cổng soát vé tự động không thuộc phạm vi hệ thống e-Metro.

# Chủ đề 02: Hệ thống bán hàng trực tuyến

*(chủ đề này được sử dụng từ đề thi môn Phân tích thiết kế phần mềm)*

Giáng Sinh và năm mới là dịp mọi người mua sắm nhiều quà tặng cho gia đình, người thân, bạn bè. Để chuẩn bị cho mùa mua sắm năm nay, cửa hàng ABC quyết định mở thêm hệ thống dịch vụ bán hàng online. Hệ thống website bán hàng online e-Shopping gồm các chức năng chính sau đây:

* Chọn và đặt mua hàng:
  + Toàn bộ thông tin về sản phẩm được quản lý bằng Hệ thống quản lý sản phẩm đã được xây dựng sẵn và đang được sử dụng trong cửa hàng. Hệ thống e-Shopping sẽ kết nối vào hệ thống này để lấy thông tin về các sản phẩm khi cần thiết.
  + Mỗi sản phẩm có tên, mã số sản phẩm (phân biệt), tên nhà sản xuất, các hình ảnh minh họa, thông tin mô tả về sản phẩm, các thông số kỹ thuật, giá bán hiện hành (giá bán của sản phẩm có thể thay đổi) và tình trạng sản phẩm (còn hay hết hàng). Mỗi sản phẩm thuộc về một nhóm sản phẩm (ví dụ: máy chụp hình kỹ thuật số, đồ chơi, thiết bị điện gia dụng, thiết bị máy tính…).
  + Khách hàng có thể xem danh sách các sản phẩm trong mỗi nhóm sản phẩm. Với mỗi sản phẩm trong danh sách, khách có thể đưa sản phẩm được chọn vào giỏ hàng hiện tại, hoặc có thể xem chi tiết thông tin về sản phẩm này. Khi đang xem thông tin chi tiết về sản phẩm, khách hàng cũng có thể đưa sản phẩm được chọn vào giỏ hàng hiện tại.
  + Trong quá trình chọn và mua hàng, khách có thể xem danh sách các sản phẩm đã được chọn vào giỏ hàng, cập nhật giỏ hàng (loại bỏ sản phẩm ra khỏi giỏ hàng, cập nhật số lượng mỗi sản phẩm cần mua…).
  + Khách hàng chọn chức năng tính tiền sau khi đã chọn xong các sản phẩm cần mua để chính thức đặt mua hàng.
  + Quy trình đặt mua hàng và tính tiền bao gồm:
    - Hệ thống sẽ yêu cầu khách hàng đăng nhập hệ thống nếu khách hàng chưa đăng nhập, hoặc đăng ký khách hàng mới nếu khách chưa có tài khoản trong hệ thống (xem thêm chi tiết về cách đăng ký khách hàng mới).
    - Khách hàng chọn loại phiếu đặt hàng: có 3 loại phiếu đặt hàng (phiếu đặt hàng thường, phiếu đặt hàng chuyển phát nhanh, phiếu đặt hàng chuyển phát nhanh trong ngày) tương ứng với đơn giá khác nhau và thời gian xử lý đơn đặt hàng khác nhau.
      * Nếu tổng trị giá đơn đặt hàng từ 1 000 000đ trở lên, cửa hàng phục vụ chuyển phát nhanh miễn phí cho khách hàng. Nếu tổng trị giá từ 5 000 000đ trở lên, cửa hàng phục vụ chuyển phát nhanh trong ngày miễn phí cho khách.
      * Hệ thống sẽ tính chi phí giao hàng tùy thuộc vào khu vực giao hàng (theo địa chỉ người nhận) và loại hình giao hàng được khách chọn. Chi phí giao hàng (nếu có) sẽ được tính vào tổng trị giá hóa đơn.
    - Khách hàng nhập thông tin về người nhận hàng (gồm họ tên, địa chỉ, điện thoại). Lưu ý là người nhận hàng có thể khác với người mua (ví dụ như khi khách mua quà tặng cho người thân, bạn bè).
    - Khách hàng nhập thông tin thanh toán giao dịch bằng thẻ tín dụng. Thông tin của thẻ tín dụng gồm: loại thẻ (VISA, Master, Discover, American Express), số hiệu thẻ (Thẻ Visa/Master/Discover: 16 chữ số. Thẻ American Express: 15 chữ số), ngày hết hạn sử dụng, họ tên người chủ thẻ và mã số an ninh của thẻ (CSV – Card Security Value). Đối với Visa, Mastercard hay Discover, CSV gồm 3 chữ số; đối với American Express, CSV gồm 4 chữ số.. Mỗi loại thẻ có thể có mức lệ phí khác nhau cho mỗi lần sử dụng thanh toán giao dịch.
    - Hệ thống tự động kết nối với Hệ thống dịch vụ thanh toán trực tuyến (đây là hệ thống mà công ty đăng ký sử dụng) để kiểm tra tính hợp lệ của thông tin thẻ tín dụng và đảm bảo khả năng thanh toán của thẻ.
    - Nếu quá trình kiểm tra thành công, hệ thống sẽ ghi nhận đơn đặt hàng của khách, gồm các thông tin về các sản phẩm cần mua với số lượng và đơn giá tương ứng, thông tin người mua và người nhận hàng, thẻ tín dụng dùng để thanh toán, hình thức giao hàng, tổng trị giá đơn đặt hàng, thời điểm đặt hàng.
    - Nếu khách hàng có cung cấp địa chỉ email, hệ thống sẽ gửi email xác nhận việc đặt hàng thành công với đầy đủ thông tin của đơn đặt hàng (ngoại trừ thông tin về thẻ tín dụng được dùng để thanh toán – vì lý do an ninh cho khách hàng)
* Đăng ký tài khoản khách hàng:
  + Khách hàng có thể đăng ký tài khoản trong hệ thống.
  + Thông tin khách hàng gồm: họ tên, ngày sinh, số CMND/Passport, địa chỉ, điện thoại, tên đăng nhập, mật khẩu, địa chỉ email (để cửa hàng gửi email xác nhận mỗi khi mua hàng).

# Tham khảo (đề bài khóa 2012, học kỳ 1 năm học 2014-2015)

### Hệ thống website Hội nghị khoa học

Để chuẩn bị cho việc tổ chức hội nghị khoa học ABC, ban tổ chức chuẩn bị xây dựng hệ thống website của hội nghị.

Hệ thống website cho phép các tác giả có thể ***đăng ký tài khoản***, ***nộp/cập nhật/xóa*** các bài báo của nhóm mình lên hệ thống (trong thời gian quy định). Mỗi bài báo thuộc về 1 số chủ đề nhất định của hội nghị (do chính tác giả chọn khi nộp/cập nhật bài). Sau khi có kết quả phản biện, tác giả có thể ***xem chi tiết*** các nhận xét của những người phản biện (*nhưng không được phép biết thông tin cá nhân về người phản biện*).

Sau khi hết thời hạn nộp bài báo, ban tổ chức sẽ dựa theo chủ đề của từng bài báo (do chính tác giả đề nghị) để phân chia các bài báo cho các Giáo sư phản biện (mỗi bài báo sẽ do 3 Giáo sư phản biện). Mỗi người phản biện có ***tài khoản riêng*** trên hệ thống, sau khi ***đăng nhập*** thành công, có thể ***download*** các bài báo mà mình cần phản biện, đồng thời có thể ***viết/cập nhật*** nhận xét của mình cho từng bài báo mà mình phản biện…

**🖎Yêu cầu**:

* Hãy xác định vấn đề về an toàn thông tin (security) có thể có trong hệ thống trên. Với mỗi vấn đề mà bạn xác định được, hãy phát biểu chặt chẽ, rõ ràng, và giải thích rõ tình huống có thể xảy ra vấn đề này (nêu trình bày dạng mô hình hoặc ví dụ trực quan).

***Ví dụ***:

* Làm thế nào Ban tổ chức có thể chứng minh với các tác giả là bài báo mà Ban tổ chức đã chuyển giao cho người phản biện là phiên bản mới nhất và chính xác của tác giả?
* Làm thế nào đảm bảo không có sự giả danh người phản biện để gửi kết quả nhận xét?
* Làm thế nào để đảm bảo nhận xét của người phản biện không bị sửa đổi trái phép?
* Làm sao chứng minh được bài báo của tác giả khi chuyển cho giáo sư phản biện không bị sửa dữ liệu?
* Nếu 1 tác giả nghi ngờ có người giả danh mình sửa/ xóa bài báo cáo của mình, có cơ chế nào để tác giả đó chứng minh nghi ngờ của mình với BTC không?
* Trong trường hợp, 1 người vừa là tác giả của bài báo này, vừa là giáo sư phản biện của bài báo khác thì họ có thể thay đổi nội dung báo cáo của mình sau khi hết hạn nộp bài không?
* Làm sao để xác thực ai chính là tác giả bài báo được gửi lên? Không có sự giả danh của tác giả?

### Hệ thống Video-on-Demand

Hệ thống Video-on-Demand cung cấp dịch vụ cho phép khách hàng (đã đăng ký) có thể truy cập, chọn và xem các chương trình mà mình yêu thích. Dữ liệu video+audio tương ứng theo yêu cầu của khách hàng sẽ được truyền (streaming) về phía khách hàng. Thiết bị giải mã được đặt ở phía khách hàng, ngoài nhiệm vụ giải mã tín hiệu (decode), còn giúp nhà cung cấp dịch vụ ***quản lý việc truy cập*** của khách hàng và ***bảo mật nội dung thông tin***…

**🖎Yêu cầu**:

* Hãy xác định vấn đề về an toàn thông tin (security) có thể có trong hệ thống trên. Với mỗi vấn đề mà bạn xác định được, hãy phát biểu chặt chẽ, rõ ràng, và giải thích rõ tình huống có thể xảy ra vấn đề này (nêu trình bày dạng mô hình hoặc ví dụ trực quan).

***Ví dụ***:

* Làm thế nào hệ thống xác định được khách hàng nào đang yêu cầu dịch vụ? Có giải pháp nào không cần dùng username/password không? Có thể sử dụng smartcard không?
* Làm thế nào để đảm bảo dữ liệu không bị đánh cắp trên đường truyền? Nếu mã hóa dữ liệu thì việc mã hóa, giải mã phải thực hiện ra sao tại server và client?
* Làm thế nào để khách hàng không lưu trữ offline dữ liệu video/audio và xem lại sau đó? Hoặc nếu cho phép khách hàng có thể xem offline thì có thể kiểm soát số lần xem hay không? Ngoài ra có thể đảm bảo khách hàng không phân phối lại nội dung (offline) multimedia này hay không?
* Làm sao hệ thống đảm bảo DL được truyền đầy đủ, có thể phục hồi khi tới người dùng?
* Làm thế nào để người dùng phát hiện ra dữ liệu chuyển tới tay mình là không chính xác, không đầy đủ, có thể đã bị thay đổi nhằm mục đích tấn công?
* Làm thế nào để hệ thống phát hiện vấn đề giả danh người dùng? VD: 1 user gửi yêu cầu, bị delay 1 khỏang thời gian đủ nhỏ để không bị phát hiện, sau đó tiếp tục gửi tới server và server gửi lại cho user theo đúng yêu cầu. User giả danh đã delay gói tin này và gửi đúng gói tin đó đến Server để được đáp ứng, hệ thống có kiểm tra được sự giả danh này hay không?

### Hệ thống dịch vụ lưu trữ trực tuyến (online storage)

Ngày nay, nhu cầu mang theo dữ liệu khi đi công tác, cũng như chia sẻ dữ liệu với nhau ngày càng trở nên cần thiết hơn. Bạn quyết định sẽ đầu tư xây dựng 1 hệ thống dịch vụ lưu trữ trực tuyến cho phép người ***đăng ký*** sử dụng dịch vụ có thể ***upload tài liệu*** lên server, ***download tài liệu*** khi cần thiết, ***chia sẻ tài liệu*** với người khác. Để bảo đảm bí mật, ***nội dung*** của tài liệu thường được ***mã hóa***.

Hệ thống bao gồm ***1 server trung tâm*** đảm nhận việc quản lý tài khoản và việc truy cập của khách hàng và **M *data server*** phục vụ việc upload/download tài liệu của khách hàng. Khi người dùng cần upload file, server trung tâm sẽ chọn 1 trong số M data server để lưu trữ dữ liệu của người dùng (người dùng sẽ upload trực tiếp lên data server này). Khi người dùng cần download file (mà mình đã upload, hay có link hợp lệ mà người quen cung cấp), server trung tâm sẽ tìm và xác định data server nào hiện đang chứa tài liệu này và yêu cầu data server gửi file cần thiết về cho người dùng…

**🖎Yêu cầu**:

* Hãy xác định vấn đề về an toàn thông tin (security) có thể có trong hệ thống trên. Với mỗi vấn đề mà bạn xác định được, hãy phát biểu chặt chẽ, rõ ràng, và giải thích rõ tình huống có thể xảy ra vấn đề này (nêu trình bày dạng mô hình hoặc ví dụ trực quan).

***Ví dụ***:

* Làm thế nào khách hàng chắc chắn được mình đang liên lạc với server trung tâm thật? Có khi nào khách hàng bị “lừa” và nhập thông tin đăng nhập vào 1 trang web giả không?
* Làm thế nào để đảm bảo file dữ liệu của người dùng không bị tiết lộ nội dung trong quá trình upload lên server/download từ server?
* Làm thế nào 1 data server kiểm tra được yêu cầu gửi dữ liệu mà mình lưu trữ cho khách hàng thật sự do server trung tâm yêu cầu? Có khi nào 1 máy tính khác giả dạng làm server trung tâm để yêu cầu data server gửi dữ liệu hay không?
* Làm thế nào đảm bảo tính toàn vẹn của dữ liệu khi người dùng upload/download tài liệu lên server?
* Có cách nào giúp người dùng phát hiện được tài khoản của mình đang bị người khác sử dụng hay không? Cảnh báo khi có những dấu hiệu tấn công vào tài khoản?