# Chương 1:

1. Kiến trúc máy tính
2. Stack
   1. Chức năng:
      1. Chứa các biến cục bộ
      2. Lưu địa chỉ trả về khi gọi hàm
      3. Truyền tham số khi gọi hàm
      4. Lưu giữ con trỏ “this” trong lập trình hướng đối tượng
   2. Thao tác trên ngăn xếp:
      1. Trong x86 mỗi phần tử stack là 4 byte
      2. Stack được quản lý qua ESP
      3. Hai thao tác cơ bản: PUSH và POP
      4. Cộng trừ 4 byte
3. Hàm và gọi hàm
4. Lỗ hổng phần mềm

BTVN: Chu trình phát triển phần mềm SDLC + Sec, viết 1 app C/C++ 🡪 IDA/Ollydbg 🡪 xem lại địa chỉ các biến, các hàm

## SDLC là gì ?

SDLC là viết tắt của Software Development Life Cycle hay còn gọi là Application Development life-cycle, là một quy trình có hệ thống để xây dựng phần mềm nhằm đảm bảo chất lượng và tính đúng đắn của phần mềm được xây dựng. Quy trình SDLC nhằm mục đích sản xuất phần mềm chất lượng cao đáp ứng mong đợi của khách hàng. Việc phát triển hệ thống phải được hoàn thành trong khung thời gian và chi phí đã xác định trước.

* Cung cấp cơ sở để lập kế hoạch, lập lịch trình và ước tính dự án
* Cung cấp khuôn khổ cho một tập hợp các hoạt động và sản phẩm tiêu chuẩn
* Là một cơ chế để theo dõi và kiểm soát dự án
* Tăng khả năng hiển thị của lập kế hoạch dự án cho tất cả các bên liên quan có liên quan của quá trình phát triển
* Tăng và nâng cao tốc độ phát triển
* Cải thiện quan hệ khách hàng
* Giúp giảm thiểu rủi ro dự án và chi phí kế hoạch quản lý dự án

## Các giai đoạn của SDLC ?

* Giai đoạn 1: Thu thập và phân tích yêu cầu
  + là giai đoạn đầu tiên trong quá trình SDLC. Nó được thực hiện bởi các thành viên trong nhóm cấp cao với đầu vào từ tất cả các bên liên quan và các chuyên gia lĩnh vực trong ngành. Lập kế hoạch cho các yêu cầu đảm bảo chất lượng và nhận biết các rủi ro liên quan cũng được thực hiện ở giai đoạn này.
  + cần các team lên yêu cầu chi tiết và chính xác. Điều này giúp các công ty chốt được timeline cần thiết để hoàn thành các công việc của hệ thống đó.
* Giai đoạn 2: Nghiên cứu khả thi
  + Quá trình này được thực hiện với sự trợ giúp của tài liệu 'Đặc điểm kỹ thuật yêu cầu phần mềm' còn được gọi là tài liệu 'SRS' (Software Requirement Specification). Nó bao gồm mọi thứ cần được thiết kế và phát triển trong vòng đời của dự án.
  + Chủ yếu có năm loại kiểm tra tính khả thi:
    - Về kinh tế: Có thể hoàn thành dự án trong phạm vi ngân sách hay không?
    - Pháp lý: Có thể xử lý dự án này theo luật không gian mạng và các khuôn khổ / quy định pháp lý khác không.
    - Tính khả thi của operation: Có thể tạo ra các hoạt động mà khách hàng mong đợi không?
    - Kỹ thuật: Cần kiểm tra xem hệ thống máy tính hiện tại có thể hỗ trợ phần mềm hay không
    - Lịch trình: Quyết định rằng dự án có thể được hoàn thành trong tiến độ đã cho hay không.
* Giai đoạn 3: Thiết kế
  + Trong giai đoạn thứ ba này, hệ thống và tài liệu thiết kế phần mềm được chuẩn bị theo tài liệu đặc tả yêu cầu, giúp xác định kiến ​​trúc hệ thống tổng thể. Giai đoạn thiết kế này đóng vai trò là đầu vào cho giai đoạn tiếp theo của mô hình.
  + Có hai loại tài liệu thiết kế được phát triển trong giai đoạn này:
    - Thiết kế cấp cao (High-Level Design - HLD)
      * Mô tả ngắn gọn và tên của từng mô-đun
      * Sơ lược về chức năng của mọi mô-đun
      * Mối quan hệ giao diện và sự phụ thuộc giữa các mô-đun
      * Các bảng cơ sở dữ liệu được xác định cùng với các yếu tố chính
      * Sơ đồ kiến trúc hoàn chỉnh cùng với chi tiết công nghệ
    - Thiết kế cấp thấp (Low-Level Design - LLD)
      * Logic chức năng của các mô-đun
      * Các bảng cơ sở dữ liệu, bao gồm loại và kích thước
      * Toàn bộ chi tiết của giao diện
      * Giải quyết tất cả các loại vấn đề phụ thuộc
      * Danh sách các thông báo lỗi
      * Hoàn thành đầu vào và đầu ra cho mọi mô-đun
* Giai đoạn 4: Mã hóa
  + Trong giai đoạn này, các nhà phát triển bắt đầu xây dựng toàn bộ hệ thống bằng cách viết mã sử dụng ngôn ngữ lập trình đã chọn. Trong giai đoạn mã hóa, các nhiệm vụ được chia thành các đơn vị hoặc mô-đun và được giao cho các nhà phát triển khác nhau. Đây là giai đoạn dài nhất của quy trình SDLC.
  + Trong giai đoạn này, Nhà phát triển cần tuân theo một số nguyên tắc mã hóa được xác định trước. Họ cũng cần sử dụng các công cụ lập trình như trình biên dịch, trình thông dịch, trình gỡ lỗi để tạo và triển khai mã.
* Giai đoạn 5: Thử nghiệm
  + Nhóm kiểm thử bắt đầu kiểm tra chức năng của toàn bộ hệ thống để xác minh rằng toàn bộ ứng dụng hoạt động theo yêu cầu của khách hàng.
  + Trong giai đoạn này, QA và nhóm kiểm tra có thể tìm thấy một số lỗi / khiếm khuyết và sẽ thông báo cho nhà phát triển. Nhóm phát triển sửa lỗi và gửi lại QA để kiểm tra lại. Quá trình này tiếp tục cho đến khi phần mềm không có lỗi, ổn định và hoạt động theo nhu cầu kinh doanh của hệ thống đó.
* Giai đoạn 6: Cài đặt / Triển khai
  + Dựa trên phản hồi do người quản lý dự án đưa ra, phần mềm cuối cùng được phát hành và kiểm tra các vấn đề triển khai nếu có.
* Giai đoạn 7: Bảo trì
  + 3 hoạt động sau sẽ diễn ra
    - Sửa lỗi - lỗi được báo cáo do một số tình huống chưa được kiểm tra
    - Nâng cấp - Nâng cấp ứng dụng lên các phiên bản mới hơn của Phần mềm
    - Cải tiến - Thêm một số tính năng mới vào phần mềm hiện có
  + Trọng tâm chính của giai đoạn SDLC này là đảm bảo rằng các nhu cầu đó tiếp tục được đáp ứng và hệ thống tiếp tục hoạt động theo thông số kỹ thuật được đề cập trong giai đoạn đầu tiên.