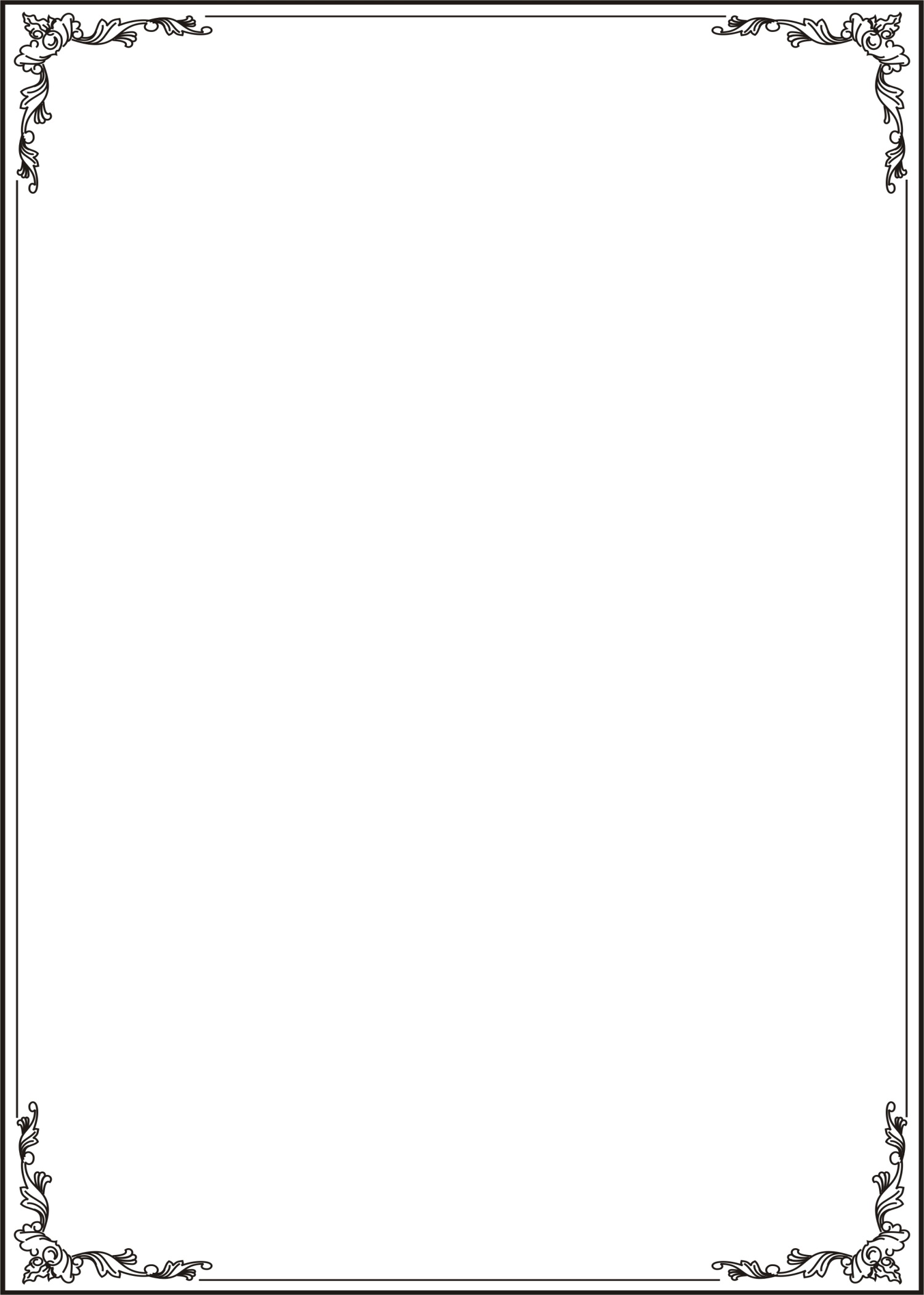
ĐỀ CƯƠNG NGHIÊN CỨU KHOA HỌC

*ĐỀ TÀI:* **Mã Hóa Dữ Liêu**

**NGƯỜI HƯỚNG DẪN KHOA HỌC:**

**NHÓM SINH VIÊN THỰC HIỆN:**

**Trương Thị Thùy Dung MSSV: K35.103.008**

**Phạm Thị Bích Ngọc MSSV: K35.103.043**

**Hồ Chí Minh, tháng 11, năm 2012**

MỤC LỤC

[1. Giới thiệu tổng quan 3](#_Toc341360329)

[2. Mục tiêu thực hiện đề tài 3](#_Toc341360330)

[3. Nội dung thực hiện đề tài 4](#_Toc341360331)

[4. Tóm tắt nội dung khóa luận 5](#_Toc341360332)

[5. Kết quả dự kiến của khoá luận 6](#_Toc341360333)

[6. Kế hoạch thực hiện 6](#_Toc341360334)

[7. Tài liệu tham khảo 7](#_Toc341360335)

# khung doiGiới thiệu tổng quan

Xã hội ngày một phát triển , nhu cầu con người ngày càng tăng cao cùng với đó sự phát triển không ngừng của mạng intenet. Internet đã đóng gơp rất lớn vào sự phát triển của nhân loại nhưng nó cũng có nhiều bất cập vẫn chưa được giải quyết triệt để như là “BẢO MẬT THÔNG TIN”.

Về cơ bản, ta có thể coi internet như là một môi trường trung gian để trao đổi THÔNG TIN, mọi hoạt động trên internet đều HẦU NHƯ CHỈ xoay quanh việc tiếp nhận, trao đổi và truyền nhận THÔNG TIN. Qua đó ta có thể thấy được thông tin quan trọng như thế nào.

Để giải quyết vấn để này phương pháp “Mã Hóa” ra đời và đóng góp rất lớn vào sự thành công của của xã hội internet.

Nhưng trong đó vẫn còn nhiều điểm yếu trong ngành “Mã Hóa” chưa được giải quyết ,, vì vậy việc nghiên cứu về các thuật toàn “Mã Hóa” cần được phát triển.

# Mục đích thực hiện đề tài

* Mục tiêu cụ thể
  + Hiểu Cách hoạt động của các phương pháp “Mã Hóa” hiện đại đang được sử dụng phổ biến
  + Trình bày điểm mạnh, điểm yếu của các phương pháp “Mã Hóa”.
  + Một số phương pháp tối ưu việc bảo mật dữ liệu
  + Thực hành Mã Hóa với một ứng dụng của bản thân , giao tiếp mã hóa với Database

# Nội dung thực hiện đề tài

## Phân loại các phương pháp mã hóa

* Mã hóa cổ điển
* Mã hóa một chiều
* Mã hóa đối xứng
* Mã hóa bất đối xứng

## Căn bản về mật mã học

* + Cryptographic Services (Dịch vụ mật mã)
  + - Integrity and Authenticity (Tính xác thực và Toàn vẹn)
  + Confidentiality (Mã hóa)
  + Public Key Cryptography (Mật mã khóa công khai)
  + Phân tích mật mã

## Những thuật toàn phổ biến

***- 1 .Cryptographic Hashes***

**- 2 .*Integrity with MD5 and SHA-1***

*2.1.MD5*

2.2.SHA

**- 3 . Authenticity HMAC**

***- 4. Key Management***

# Tóm tắt nội dung

# Kế hoạch thực hiện

**Xác nhận của người hướng dẫn Nhóm Sinh viên thực hiện**

(Ký và ghi rõ họ tên) (Ký và ghi rõ họ tên)