**PHẦN 1: TỔNG QUAN**

Trong bối cảnh an ninh mạng ngày càng trở nên phức tạp, việc bảo mật thông tin đã trở thành yêu cầu sống còn đối với các cá nhân và tổ chức. Mật mã khóa đối xứng, một trong những phương pháp mã hóa lâu đời nhất, tiếp tục đóng vai trò quan trọng trong việc đảm bảo tính bí mật và toàn vẹn của dữ liệu. Bài báo cáo này tập trung phân tích nguyên lý hoạt động của mật mã khóa đối xứng thông qua nghiên cứu trường hợp điển hình về Tiêu chuẩn Mã hóa Dữ liệu (DES), đồng thời trình bày một ứng dụng thực tế sử dụng thư viện Python kết hợp giao diện đồ họa Tkinter. Các kết quả nghiên cứu chỉ ra rằng mặc dù DES đã được thay thế bởi các thuật toán hiện đại hơn như AES, việc hiểu rõ nguyên lý hoạt động của nó vẫn có giá trị học thuật quan trọng trong lĩnh vực an ninh thông tin.

1. **Khái Niệm Cơ Bản Về Bảo Mật Thông Tin** [1]

Bảo mật thông tin (Information Security) là tập hợp các biện pháp nhằm đảm bảo tính bảo mật, toàn vẹn, chính xác và sẵn sàng của thông tin trong quá trình lưu trữ và truyền tải. Bốn trụ cột chính của bảo mật thông tin bao gồm:

* Tính bảo mật (Confidentiality) - ngăn chặn truy cập trái phép;
* Tính toàn vẹn (Integrity) - đảm bảo thông tin không bị sửa đổi bất hợp pháp;
* Tính khả dụng (Availability) - duy trì khả năng truy cập thông tin khi cần thiết;
* Tính xác thực (Authenticity) - xác minh nguồn gốc thông tin1. Các nguyên tắc này tạo thành nền tảng cho mọi hệ thống an ninh mạng hiện đại, từ các giao dịch ngân hàng điện tử đến hệ thống quản lý dữ liệu của chính phủ.

1. **Thực Trạng An Ninh Mạng Hiện Nay** [1]

Theo báo cáo từ các chuyên gia bảo mật, năm 2025 chứng kiến sự gia tăng 35% các vụ tấn công mạng nhắm vào cơ sở hạ tầng quan trọng so với năm trước. Một nghiên cứu gần đây chỉ ra rằng 68% doanh nghiệp Việt Nam đã trải qua ít nhất một lần vi phạm dữ liệu trong năm qua, với thiệt hại trung bình ước tính 5.2 tỷ đồng mỗi sự cố. Các hình thức tấn công phổ biến bao gồm tấn công DDoS, mã độc tống tiền (Ransomware), và lừa đảo phishing. Trong bối cảnh đó, việc áp dụng các thuật toán mã hóa mạnh trở thành yêu cầu bắt buộc để bảo vệ dữ liệu nhạy cảm.

1. **Vai Trò Của Mật Mã Trong Bảo Mật Thông Tin** [1]

Mật mã học (Cryptography) là ngành khoa học nghiên cứu các phương pháp bảo vệ thông tin thông qua quá trình biến đổi thông tin thành dạng không thể đọc được bằng các thuật toán toán học phức tạp [2]. Hai phương pháp mã hóa chính bao gồm mật mã khóa đối xứng (Symmetric-key Cryptography) và mật mã khóa bất đối xứng (Asymmetric-key Cryptography)[3]. Trong khi mật mã khóa bất đối xứng sử dụng cặp khóa công khai/riêng tư để giải quyết vấn đề phân phối khóa, mật mã khóa đối xứng vẫn được ưa chuộng trong các hệ thống yêu cầu tốc độ xử lý cao nhờ hiệu suất vượt trội [2][3].