

TRƯỜNG ĐẠI HỌC MỎ - ĐỊA CHẤT
KHOA CÔNG NGHỆ THÔNG TIN



BÁO CÁO SINH HOẠT HỌC THUẬT
**ĐỀ TÀI: THUẬT TOÁN RABIN và ĐÁNH GIÁ ĐỘ PHỨC TẠP
THUẬT TOÁN QUA CÀI ĐẶT CÁC NGÔN NGỮ LẬP TRÌNH**

Giảng viên : Dương Chí Thiện

Bộ môn : Hệ thống thông tin và Tri thức

Hà nội, 2026

MỤC LỤC

LỜI MỞ ĐẦU	4
CHƯƠNG 1: TỔNG QUAN VỀ AN TOÀN BẢO MẬT THÔNG TIN	5
1. Giới thiệu hệ thống bảo mật an toàn thông tin	5
1.1. Tổng quát.....	5
1.2. Tầm quan trọng của an toàn bảo mật thông tin.....	5
1.3. Lý thuyết	6
2. Chuyên đề.....	7
2.1. Ví dụ.....	7
CHƯƠNG 2: THUẬT TOÁN RABIN	9
1. Lý do và mục đích chọn thuật toán	9
1.1. Lý do	9
1.2. Mục đích.....	10
2. Tổng quát về thuật toán chữ ký Rabin	10
2.1. Giới thiệu.....	10
2.2. Cách hoạt động của thuật toán Rabin.....	11
2.3. Đặc điểm nổi bật	12
2.4. Phương pháp tấn công.....	12
2.5. Độ phức tạp	13
2.6 Ví dụ chữ ký rabin.....	13
2.7. Biện pháp bảo vệ.....	15
2.8. Ứng dụng thực tế.....	15
CHƯƠNG 3: PHÂN TÍCH VÀ THIẾT KẾ HỆ THỐNG BỎ PHIẾU ĐIỆN TỬ SỬ DỤNG MẬT MÃ RABIN	17
3.1. Giới thiệu Bài toán	17
3.2. Tổng quan về kiến trúc hệ thống	17

3.3. Thiết kế luồng dữ liệu và thuật toán an toàn.....	18
3.3.1. Quy trình sinh khóa (Key Generation Phase)	18
3.3.2. Quy trình đóng gói phiếu bầu (Voting Protocol)	18
3.3.3. Quy trình Kiểm phiếu (Vote Counting Protocol)	20
CHƯƠNG 4: XÂY DỰNG ỨNG DỤNG	22
4.1. Cấu trúc tổ chức mã nguồn	22
4.2. Xây dựng Module Authority (Phía Quản lý).....	22
4.2.1. Giao diện và Chức năng chính	22
4.2.2. Chức năng Quản lý Cấu hình Bầu cử.....	23
4.2.3. Chức năng Kiểm phiếu và Sàng lọc	23
4.3. Xây dựng Module Voter (Phía Cử tri)	24
4.3.1. Giao diện và Trải nghiệm người dùng	24
4.3.2. Cấu trúc gói tin Phiếu bầu.....	26
CHƯƠNG 5: TRIỂN KHAI VÀ KỊCH BẢN KIỂM THỬ	27
5.1. Thiết lập môi trường	27
5.2. Kịch bản kiểm thử: Bầu cử Lớp trưởng	27
5.3. Kết quả kiểm thử.....	32
CHƯƠNG 6: ĐÁNH GIÁ VÀ KẾT LUẬN	33
6.1. Đánh giá ưu điểm của hệ thống	33
6.2. Phân tích các hạn chế tồn tại.....	33
6.3. Hệ thống bỏ phiếu điện tử sử dụng Rabin với các mô hình khác.....	34
6.3.1. So sánh với bỏ phiếu truyền thống.....	34
6.3.2. So sánh với hệ thống sử dụng RSA	34
6.3.3. So sánh với các hệ thống sử dụng chữ ký trên đường cong elliptic (ECDSA)	35
6.4. Kết luận	35
TÀI LIỆU THAM KHẢO.....	36

LỜI MỞ ĐẦU

Trong thời đại kỹ thuật số hiện nay, bảo mật thông tin trở thành một trong những vấn đề quan trọng và cấp thiết nhất. Các hệ thống mã hóa hiện đại giúp bảo vệ dữ liệu khỏi các cuộc tấn công, đảm bảo tính toàn vẹn, bí mật và xác thực trong quá trình truyền tải thông tin.

Trong số các thuật toán mã hóa khóa công khai, chữ ký Rabin là một trong những phương pháp đáng chú ý, được đề xuất bởi Michael Rabin vào năm 1979. Thuật toán này dựa trên bài toán khai căn bậc hai theo modulo số nguyên lớn, tương đương với độ khó của việc phân tích thừa số— một bài toán khó trong lý thuyết số học và mật mã học.

Báo cáo này sẽ giới thiệu về chữ ký Rabin, bao gồm nguyên lý hoạt động, cơ chế ký và xác minh, cùng các đặc điểm nổi bật. Bên cạnh phần lý thuyết, báo cáo cũng sẽ trình bày một ứng dụng thực tế của hệ mật mã Rabin thông qua việc triển khai mã nguồn bằng ngôn ngữ lập trình Python. Việc lập trình thuật toán này không chỉ giúp hiểu rõ hơn về cơ chế hoạt động mà còn cung cấp một cái nhìn thực tiễn về cách ứng dụng nó trong bảo mật thông tin.

Mục tiêu của báo cáo là cung cấp một cách tiếp cận toàn diện về chữ ký Rabin, giúp người đọc nắm rõ nguyên lý toán học đằng sau thuật toán, đồng thời hiểu được cách triển khai và ứng dụng nó trong thực tế.

CHƯƠNG 1: TỔNG QUAN VỀ AN TOÀN BẢO MẬT THÔNG TIN

1. Giới thiệu hệ thống bảo mật an toàn thông tin

1.1. Tổng quát

An toàn bảo mật thông tin là việc bảo vệ thông tin khỏi các mối đe dọa tiềm tàng, bảo vệ các tài sản kỹ thuật số khỏi bị truy cập trái phép, thay đổi, hoặc phá hủy. Trong môi trường số ngày nay, việc bảo vệ thông tin trở nên quan trọng hơn bao giờ hết. Các hệ thống bảo mật thông tin bao gồm các biện pháp để đảm bảo rằng thông tin được bảo vệ dưới ba yếu tố chính:

Bảo mật (Confidentiality): Đảm bảo rằng thông tin chỉ được truy cập bởi những người có quyền truy cập hợp pháp.

Toàn vẹn (Integrity): Đảm bảo rằng thông tin không bị thay đổi một cách trái phép trong quá trình lưu trữ hoặc truyền tải.

Sẵn sàng (Availability): Đảm bảo rằng thông tin luôn có sẵn và có thể truy cập khi cần thiết.

1.2. Tầm quan trọng của an toàn bảo mật thông tin

Môi trường hiện đại, với sự phát triển nhanh chóng của công nghệ thông tin và truyền thông, đồng thời lại chứng kiến sự gia tăng của các cuộc tấn công mạng, đã tạo ra nhu cầu lớn đối với các hệ thống bảo mật thông tin mạnh mẽ. An toàn bảo mật thông tin không chỉ bao gồm các phương thức bảo vệ dữ liệu trong quá trình lưu trữ hay truyền tải mà còn phải đảm bảo rằng thông tin được xử lý một cách toàn vẹn, không bị thay đổi trái phép.

Các lĩnh vực chính của bảo mật thông tin bao gồm:

Mã hóa (Encryption): Biến đổi dữ liệu thành một dạng không thể đọc được mà không có khóa giải mã.

Xác thực (Authentication): Đảm bảo rằng người hoặc hệ thống truy cập là hợp lệ.

Kiểm soát truy cập (Access Control): Đảm bảo chỉ những người có quyền mới có thể truy cập vào các tài nguyên hệ thống.

Chữ ký số (Digital Signatures): Xác nhận tính toàn vẹn của dữ liệu và người gửi thông qua các thuật toán mã hóa:

Xác minh:

- Người gửi
- Tính toàn vẹn dữ liệu
- Chống chối bỏ trách nhiệm

Trong đó, chữ ký số Rabin là một thuật toán chữ ký quan trọng trong mật mã khóa công khai, có độ an toàn cao nhờ dựa vào bài toán phân tích số nguyên lớn.

Các thành phần trên kết hợp giúp xây dựng hệ thống bảo mật toàn diện, bảo vệ dữ liệu trước các mối đe dọa không ngừng phát triển.

1.3. Lý thuyết

1.3.1. Mã hóa thông tin

- Mã hóa thông tin là quá trình chuyển đổi dữ liệu từ dạng dễ đọc thành dạng mã hóa nhằm bảo vệ thông tin khỏi truy cập trái phép.

- Mục tiêu chính của mã hóa là đảm bảo rằng chỉ những người có khóa giải mã phù hợp mới có thể đọc được nội dung gốc.

- Có hai loại mã hóa chính:

+ Mã hóa đối xứng: Sử dụng một khóa duy nhất cho cả quá trình mã hóa và giải mã. Ví dụ: AES, DES.

+ Mã hóa bất đối xứng: Sử dụng cặp khóa gồm khóa công khai (public key) để mã hóa và khóa bí mật (private key) để giải mã. Ví dụ: RSA, Rabin Cryptosystem.

1.3.2. Chữ ký số

- Chữ ký số là một kỹ thuật mật mã cho phép xác nhận người gửi và đảm bảo nội dung không bị thay đổi

- Nó hoạt động dựa trên cặp khóa công khai – bí mật . Người gửi dùng khóa bí mật để ký , người nhận dùng khóa công khai để xác minh

- 3 tính chất cơ bản của chữ ký số:

- Xác thực(Authentication):đảm bảo chữ ký thuộc về đúng người gửi
- Toàn vẹn (Integrity) : đảm bảo dữ liệu không bị thay đổi
- Không chối bỏ(Non-repudiation):Người gửi không thể phủ nhận việc đã ký

1.3.3. Xác thực và quản lý danh tính

- Xác thực (Authentication): xác minh danh tính người dùng hoặc thiết bị trước khi cấp quyền truy cập

- Quản lý danh tính (Identity Management): Quản lý thông tin đăng nhập và phân quyền người dùng trong hệ thống bảo mật.

1.3.4. Bảo vệ dữ liệu trong quá trình truyền tải

- Khi dữ liệu được gửi qua mạng, nó có thể bị tấn công hoặc đánh cắp.

- Giải pháp bảo vệ: Áp dụng chữ ký số (Digital Signature) để đảm bảo tính toàn vẹn của dữ liệu. Chữ ký Rabin cũng có thể được sử dụng trong chữ ký số để xác minh nguồn gốc và chống giả mạo thông tin.

1.3.5. Giám sát và phản ứng

- Theo dõi hệ thống phát hiện dấu hiệu tấn công bất thường

- Xử lý và cô lập mối đe dọa nhằm giảm thiệt hại

1.3.6. Bảo mật mạng và cơ sở hạ tầng

- Bảo mật mạng bao gồm việc cấu hình và quản lý tường lửa, phát hiện xâm nhập và bảo vệ khỏi các cuộc tấn công mạng từ bên ngoài.

- Bảo mật cơ sở hạ tầng bao gồm việc bảo vệ các máy chủ, cơ sở dữ liệu và hệ thống lưu trữ thông tin quan trọng.

Hệ thống bảo mật an toàn thông tin là một hệ thống phức tạp bao gồm nhiều thành phần và phương pháp để đảm bảo tính bảo mật và toàn vẹn của thông tin. Sự kết hợp của các biện pháp bảo mật này là cần thiết để đối phó với các mối đe dọa mạng ngày càng phức tạp và đa dạng.

Hệ thống bảo mật thông tin là tập hợp nhiều biện pháp phối hợp chặt chẽ để bảo vệ dữ liệu toàn diện. Trong đó, chữ ký rabin là giải pháp đảm bảo tính xác thực và toàn vẹn dữ liệu, rất quan trọng trong việc giao dịch số, chữ ký điện tử,...

2. Chuyên đề

2.1. Ví dụ

Chúng ta có thể mô phỏng quy trình ký và kiểm tra chữ ký Rabin như sau:

Giả sử Bob muốn gửi một thông điệp M cho Alice và đính kèm chữ ký số để Alice có thể xác minh đây đúng là do Bob gửi

- Khóa công khai: Alice chọn hai số nguyên tố lớn p và q , sau đó tính $N = p \times q$. Bob công khai N .

- Khóa bí mật: Các số nguyên p và q được giữ kín bởi Bob.

Khi Bob muốn gửi thông điệp M cho Alice, anh thực hiện các bước sau:

- Mã hóa: Bob tính giá trị $S = M^2 \bmod N$
- Bob gửi cặp (M, S) cho Alice

Sau đó Alice Kiểm tra chữ ký

$$M^2 = S$$

2. Giải mã: Khi nhận được C , Alice sử dụng khóa bí mật (các số p và q) để tìm các căn bậc hai của C modul N . Do tính chất của phép bình phương modul N , quá trình giải mã có thể cho ra tới bốn kết quả. Alice sẽ áp dụng các quy tắc để chọn ra giá trị M như ban đầu.

2.2 Nghiên cứu

Để đảm bảo tính bảo mật của hệ mật mã Rabin, cần tiến hành nghiên cứu và phân tích các vấn đề sau:

- Tính an toàn của hệ mật mã: Nghiên cứu đánh giá mức độ bảo mật của hệ mật mã Rabin dựa trên bài toán khai căn bậc hai modul N . Điều này bao gồm việc phân tích các điều kiện cần thiết để lựa chọn các số nguyên tố p và q phù hợp, cũng như việc áp dụng các kỹ thuật padding nhằm đảm bảo rằng quá trình giải mã có thể duy nhất xác định được thông điệp ban đầu.

- Xác định nguyên tắc của tấn công: Phân tích các phương pháp tấn công tiềm ẩn vào hệ mật mã Rabin, chẳng hạn như tấn công brute force và các dạng tấn công dựa trên cấu trúc số N . Nghiên cứu này nhằm hiểu rõ các điểm yếu có thể bị khai thác và từ đó đề xuất các biện pháp phòng ngừa hiệu quả.

- Phát triển phương pháp bảo mật: Đề xuất và phát triển các giải pháp nhằm cải thiện tính bảo mật của hệ mật mã Rabin. Điều này bao gồm việc tối ưu hóa quy trình giải mã bằng Python, cải tiến kỹ thuật padding và thêm các cơ chế nhận dạng thông minh để đảm bảo rằng thông điệp ban đầu được giải mã chính xác dù có bốn kết quả khả dĩ từ phép tính căn bậc hai modul N .

CHƯƠNG 2: THUẬT TOÁN RABIN

1. Lý do và mục đích chọn thuật toán

1.1. Lý do

Thuật toán **chữ ký Rabin** được lựa chọn để nghiên cứu và triển khai nhờ vào vị thế đặc biệt của nó trong lĩnh vực mật mã học, đặc biệt là trong nhóm các lược đồ chữ ký công khai. Tính an toàn của chữ ký Rabin được xây dựng dựa trên bài toán phân tích số nguyên lớn thành các thừa số nguyên tố — một trong những bài toán khó nhất trong lý thuyết số học hiện đại. Bài toán này yêu cầu phân tích một số nguyên lớn (thường có kích thước từ 1024 bit trở lên) thành tích của hai số nguyên tố; đây là nhiệm vụ tính toán phức tạp vượt xa khả năng của các máy tính cổ điển khi số có kích thước đủ lớn. Sự khó khăn này mang lại cho chữ ký Rabin một mức độ bảo mật lý thuyết cao, khiến nó trở thành một lựa chọn hấp dẫn trong bối cảnh nhu cầu bảo vệ tính toàn vẹn và xác thực thông tin nhạy cảm ngày càng tăng (giao dịch tài chính trực tuyến, bảo mật dữ liệu y tế, hợp đồng điện tử...).

So với các lược đồ chữ ký khác như RSA, chữ ký Rabin có một số ưu điểm lý thuyết đáng chú ý. Đầu tiên, tính bảo mật của nó đã được chứng minh tương đương trực tiếp với bài toán phân tích thừa số: phá lược đồ chữ ký Rabin (ví dụ, tạo chữ ký giả) tương đương với việc phân tích NNN thành ppp và qqq . Đây là một dạng chứng minh an toàn mang tính toán học mạnh mẽ hơn so với RSA, nơi mối quan hệ giữa việc phá RSA và phân tích thừa số không hoàn toàn là một tương đương chặt chẽ trong mọi biến thể. Thứ hai, cơ chế toán học của chữ ký Rabin, dựa trên phép bình phương modulo và việc tính căn bậc hai modulo, đơn giản hơn về mặt khái niệm so với các phép lũy thừa phức tạp trong một số biến thể khác, giúp dễ dàng phân tích và làm sáng tỏ bản chất lược đồ. Ngoài ra, đặc điểm rằng phép lấy căn bậc hai modulo NNN có thể sinh ra tới bốn nghiệm vừa tăng độ khó cho kẻ tấn công (vì có nhiều nghiệm khả dĩ) vừa đặt ra thách thức thực tiễn cho triển khai (phải dùng padding/tag để chọn nghiệm đúng), tạo nhiều hướng nghiên cứu thú vị.

Chữ ký Rabin cũng được lựa chọn vì tính linh hoạt trong các ứng dụng học thuật và nghiên cứu. Sự đơn giản tương đối của nó làm cho Rabin trở thành công cụ lý tưởng để giảng dạy các khái niệm nền tảng của mật mã học: cặp khóa công khai/bí mật, phép tính modulo, Định lý Dư Trung Hoa (CRT), và các bài toán khó trong lý thuyết số. Đồng thời, nghiên cứu chữ ký Rabin mở ra cơ hội để khám phá các vấn đề thực tiễn như hiệu suất tính toán, quản lý nghiệm đa dạng, các kỹ thuật đệm/padding và

hash-to-square — từ đó đóng góp vào sự phát triển của các hệ thống chữ ký số và bảo mật trong tương lai.

1.2. Mục đích

Mục đích chính của việc chọn chữ ký Rabin là nghiên cứu sâu về cách một lược đồ chữ ký công khai được xây dựng dựa trên các bài toán khó trong toán học, nhằm làm sáng tỏ các nguyên lý cốt lõi của mật mã học hiện đại. Việc này giúp người nghiên cứu nắm vững những khái niệm như cặp khóa công khai/bí mật, tính bất đối xứng, các phép tính modulo, cũng như cơ sở an toàn dựa trên bài toán phân tích thừa số.

Cụ thể, mục tiêu bao gồm:

Phân tích cấu trúc toán học của lược đồ chữ ký Rabin (sinh khóa, ký, xác minh) và minh họa quá trình lấy căn bậc hai modulo bằng các phương pháp thực tế (công thức khi $p, q \equiv 3 \pmod{4}$, $p, q \equiv 1 \pmod{4}$, thuật toán Tonelli–Shanks, CRT).

Đánh giá hiệu quả và hạn chế của Rabin so với các lược đồ chữ ký khác (RSA, ECDSA), đặc biệt về tính an toàn lý thuyết, chi phí ký/xác minh, và vấn đề nghiệm nhiều.

Nghiên cứu các kỹ thuật thực dụng để xử lý vấn đề đa nghiệm (padding, tag, hash-to-square, thêm nonce) và phòng chống các tấn công như chosen-message.

Đề xuất và kiểm nghiệm các phương pháp tối ưu hoá triển khai (tối ưu CRT, chống side-channel), từ đó chuẩn bị cơ sở cho các ứng dụng thực tế như chữ ký số trong hệ thống xác thực, blockchain hoặc mã hóa lai.

Một mục tiêu quan trọng khác là phát triển kỹ năng lý thuyết số và lập trình bảo mật thông qua triển khai thuật toán (ví dụ: mô phỏng bằng Python) để kiểm tra hiệu năng, tính đúng đắn và các biện pháp bảo vệ.

2. Tổng quát về thuật toán chữ ký Rabin

2.1. Giới thiệu

Chữ ký Rabin là một lược đồ chữ ký công khai do Michael O. Rabin đề xuất vào năm 1979. Thay vì dùng để mã hóa dữ liệu như hệ mã hóa Rabin hay RSA, phiên bản chữ ký được thiết kế dành cho xác thực và toàn vẹn thông điệp: người ký (sở hữu khóa bí mật) tạo chữ ký sao cho bình phương của chữ ký (modulo N) khớp với một giá trị băm của thông điệp; người kiểm tra chỉ cần dùng khóa công khai N để xác minh điều này. Tính bảo mật của lược đồ được xây trên bài toán phân tích thừa số: việc giả mạo chữ ký tương đương với việc phân tích N thành p, q .

So với các lược đồ khóa đối xứng như DES/AES (dùng một khóa chung), chữ ký Rabin thuộc nhóm khóa bất đối xứng: cặp khóa công khai/bí mật cho phép xác minh công khai mà không tiết lộ khả năng ký. So với RSA, điểm nổi bật của Rabin là mối liên hệ trực tiếp và chặt chẽ hơn tới bài toán phân tích thừa số (security reduction to factoring), nhưng Rabin gặp thực tế vấn đề đa nghiệm trong bước rút căn modulo, yêu cầu thêm cơ chế padding/tag.

2.2. Cách hoạt động của thuật toán Rabin

Chữ ký Rabin sử dụng ba qui trình chính: tạo khóa, ký, và xác minh — kèm các thao tác toán học như tính căn bậc hai modulo và kết hợp nghiệm bằng CRT.

Tạo khóa

Chọn hai số nguyên tố lớn p và q . Thông thường người ta chọn $p \equiv q \equiv 3 \pmod{4}$ để đơn giản hóa công thức lấy căn bậc hai $a^{((p+1)/4)}$ (khi đó một căn có thể lấy bằng nếu a là quadratic residue).

Tính $N=p \cdot q$

Khóa công khai: N .

Khóa bí mật: (p, q)

Trong thực tế, p, q có kích thước lớn (tổng độ dài N thường ≥ 2048 bit tùy yêu cầu bảo mật).

Ký: Mục tiêu: tìm s sao cho $s^2 \equiv x \pmod{N}$, với x là giá trị băm/đệm của thông điệp m .

Các bước thực dụng:

Tạo giá trị băm/padding: $x = H(m \parallel \text{padding})$ đảm bảo $0 \leq x < N$. Padding có thể chứa tag/nonce để phân biệt nghiệm.

Kiểm tra x là quadratic residue modulo p và q . Nếu không, thay padding/nonce và thử lại (hash-to-square).

Dùng khóa bí mật để tìm nghiệm $r_p : r_p^2 \equiv x \pmod{p}$ và nghiệm r_q của $r_q^2 \equiv x \pmod{q}$. Mỗi phương trình có hai nghiệm $\rightarrow$ tổng cộng 4 nghiệm khả dĩ trên modulo N .

Kết hợp các cặp nghiệm bằng Định lý Dư Trung Hoa (CRT) để có 4 nghiệm $s_1, \dots, s_4$.

Chọn nghiệm phù hợp theo quy tắc padding/tag (ví dụ chọn nghiệm có $\log_2(4) = 2$ bit thấp khớp tag) và xuất sslàm chữ ký.

Xác minh

Người kiểm tra:

Tính $x = H(m \parallel \text{padding})$ theo cùng quy ước.

Kiểm tra: $s^2 \equiv x \pmod{N}$

Nếu dùng tag $\rightarrow$ kiểm tra thêm điều kiện phân biệt (ví dụ $s \pmod{4} = \text{tag}$).
Nếu tất cả đúng $\rightarrow$ chấp nhận chữ ký; ngược lại $\rightarrow$ từ chối.

2.3. Đặc điểm nổi bật

Đa nghiệm khi giải căn: Với $N=p.q$ lẻ không chia hết 2, phương trình $s^2 \equiv x \pmod{N}$ có thể có đến 4 nghiệm. Điều này buộc phải dùng padding/tag để chọn nghiệm đúng.

Bảo mật tương đương với phân tích thừa số: Phá lược đồ chữ ký Rabin tương đương với phân tích N , nên có cơ sở chứng minh an toàn chặt chẽ hơn cho một số khía cạnh so với RSA.

Xác minh nhanh: Kiểm tra chỉ là một phép bình phương modulo N , nhẹ hơn so với nâng lũy thừa lớn như trong RSA — lợi cho hệ thống cần xác minh nhanh, tần suất cao.

Hạn chế triển khai thực tế: Vấn đề chọn nghiệm duy nhất và chống chosen-message attacks yêu cầu padding/phương pháp hash-to-square phức tạp hơn. Ngoài ra, việc ký (tính căn mỗi modulo và CRT) nặng hơn một chút so với một số lược đồ khác.

2.4. Phương pháp tấn công

Những phương pháp tấn công chính gồm:

Phân tích thừa số N : Con đường trực tiếp nhất để phá lược đồ là tìm p, q từ N . Các thuật toán như Quadratic Sieve (QS) phù hợp với N kích thước vừa phải; General Number Field Sieve (GNFS) là thuật toán mạnh nhất hiện nay trên máy cổ điển cho N rất lớn. Nếu p, q bị dò được, kẻ tấn công có thể tính mọi căn và ký/gia mạo chữ ký.

Tấn công dựa trên padding (chosen-message): Nếu padding hoặc phương pháp hash-to-square thiết kế kém, kẻ tấn công có thể thực hiện chosen-message attack để thu

thập thông tin về mối quan hệ giữa giá trị băm và nghiệm, từ đó dựng chữ ký hợp lệ cho thông điệp khác hoặc suy ra khóa.

Tấn công dựa trên đa nghiệm: Nếu lược đồ không cung cấp cơ chế phân biệt nghiệm, kẻ tấn công có thể tận dụng nghiệm sai để gây xung đột hoặc dựng chuỗi kiện toàn.

Tấn công side-channel: Rò rỉ thông tin trong quá trình tính căn modulo hay CRT (thời gian, điện năng, rò rỉ bộ nhớ) có thể tiết lộ thông tin về p, q .

Ngoài ra, máy tính lượng tử (với thuật toán Shor) sẽ phá vỡ bài toán phân tích thừa số trong thời gian đa thức — khi máy tính lượng tử mạnh xuất hiện, Rabin (như RSA) không còn an toàn.

2.5. Độ phức tạp

Sinh khóa: Tổn công cho việc sinh và kiểm tra primality của p, q ; thực hiện một lần.

Ký: Chi phí gồm tính nghiệm modulo p và q (có thể dùng công thức nhanh khi

$p, q \equiv 3 \pmod{4}$ hoặc thuật toán Tonelli–Shanks) và kết hợp bằng CRT — chi phí chấp nhận được đối với khóa lớn.

Xác minh: Rất nhẹ — một phép bình phương modulo N .

Tấn công phân tích thừa số: Thời gian chạy tăng rất nhanh theo kích thước N ; GNFS là thuật toán tốt nhất trên máy cổ điển. Khi N đủ lớn (2048 bit trở lên), phân tích thừa số thực tế là bất khả thi với công nghệ hiện tại. Tuy nhiên, Shor trên máy lượng tử có thể làm điều này trong thời gian đa thức, là rủi ro cho tương lai.

Gợi ý kích thước khóa: Để đảm bảo an toàn trên máy cổ điển, khuyến nghị N tối thiểu 2048 bit; với mức rủi ro cao hơn hoặc bảo mật lâu dài, nên dùng 3072–4096 bit hoặc chuyển sang thuật toán hậu-lượng tử nếu cần chống lượng tử.

2.6 Ví dụ chữ ký rabin

Chọn khóa : $p = 7, q = 11 \rightarrow n = p.q = 77$

Thông điệp: $m = 20$

Ký:

Tìm s sao cho $s^2 \equiv m \pmod{77}$

Ta có $6^2 = 36 \not\equiv 20, 14^2 = 196 \equiv 196 - 154 = 42 \not\equiv 20$

$13^2 = 169 \equiv 169 - 154 = 15$

thử tiếp: $27^2 = 729 \equiv 729 - 693 = 36$

thử: $18^2 = 324 \equiv 324 - 308 = 16$

Ta phải chỉnh thông điệp bằng hàm băm H . Giả sử $H(m) = 36$, thì ta lấy chữ ký: $s = 6$

Kiểm tra: $6^2 = 36 \equiv H(m) \Rightarrow$ hợp lệ

Ví dụ 2:

Khóa: $p = 13, q = 17 \Rightarrow n = 221$

Thông điệp: $m=19$

Hàm băm giả sử: $H(m) = 81$

Ký: $s^2 = 81 \Rightarrow s = \pm 9$

Chữ ký có thể là: $s = 9$

Kiểm tra: $9^2 = 81 = H(m) \Rightarrow$ hợp lệ

Ví dụ 3

Khóa: $p = 11, q = 23 \Rightarrow n = 253$

Thông điệp: $m = 45$

Hàm băm giả sử: $H(m) = 100$

Ký: Giải $s^2 \equiv 100 \pmod{253}$

Vì $10^2 = 100$

Chữ ký: $s = 10$ (hoặc -10)

Kiểm tra: $10^2 = 100 = H(m) \Rightarrow$ hợp lệ

Ví dụ 4

Khóa: $p = 19, q = 23 \Rightarrow n = 437$

Thông điệp: $m = 51$

Hàm băm giả sử: $H(m) = 144$

Ký: $s^2 \equiv 144 \Rightarrow s = \pm 12$

Chữ ký: $s = 12$

Kiểm tra: $12^2 = 144 = H(m) \Rightarrow$ hợp lệ

Trong Rabin Signature phải dùng hàm băm H để chắc chắn rằng giá trị cần giải phương trình $s^2 \equiv H(m) \pmod{n}$ là phần dư bậc hai.

Mỗi chữ ký thường có 4 nghiệm, người ký phải chọn đúng nghiệm theo quy tắc.

2.7. Biện pháp bảo vệ

Để triển khai chữ ký Rabin an toàn, cần áp dụng các biện pháp sau:

Sử dụng khóa đủ lớn: Chọn p, q sao cho N có độ dài phù hợp với mục tiêu bảo mật (≥ 2048 bit là ngưỡng phổ biến cho bảo mật hiện đại).

Padding và hash-to-square: Không ký trực tiếp $H(m)$ mà dùng cơ chế padding/tag/nonce để đảm bảo x có thể là quadratic residue và đồng thời chứa bit phân biệt để chọn nghiệm duy nhất. Kỹ thuật hash-and-sign với thử nhiều nonce (hash-to-square) hoặc thêm tag là phương pháp thực dụng.

Chọn primes mạnh: Tránh primes có cấu trúc dễ khai thác (ví dụ tránh primes khiến Pollard's $p-1$ hiệu quả).

Chống side-channel: Bảo vệ việc thực hiện toán học (CRT, tính căn) khỏi rò rỉ thời gian/điện năng/bộ nhớ.

Kiểm toán & test: Thực hiện kiểm thử, kiểm toán mã nguồn và đánh giá an ninh (đặc biệt khả năng chosen-message) để đảm bảo không có sơ hở thực thi.

Lưu ý lượng tử: Nếu môi trường yêu cầu bảo mật trước máy lượng tử, không dùng Rabin; thay bằng lược đồ hậu-lượng tử.

2.8. Ứng dụng thực tế

Mặc dù chữ ký Rabin ít phổ biến hơn RSA hay ECDSA trên thị trường do vấn đề đa nghiệm và quy chuẩn tiêu chuẩn hoá, nó vẫn có một số ứng dụng và vai trò quan trọng:

Chữ ký số: Khi vấn đề lựa chọn nghiệm được xử lý bằng padding/tag an toàn, Rabin có thể dùng cho chữ ký số trong các hệ yêu cầu xác minh nhanh (vì xác minh chỉ là một phép bình phương modulo).

Hệ thống học thuật và đào tạo: Rabin là ví dụ điển hình cho bài giảng về mối liên hệ giữa bài toán số học và an toàn mật mã; thích hợp để minh họa CRT, căn modulo, và security reductions.

Mã hóa lai / trao đổi khóa: Rabin có thể được ứng dụng trong cấu trúc lai nơi Rabin ký/mã hóa khóa phiên (kết hợp với AES để mã hóa dữ liệu lớn), tận dụng lợi thế xác minh nhanh.

Ứng dụng chuyên biệt: Trong một số hệ thống nội bộ hoặc ứng dụng có thể kiểm soát tốt phần padding/tag (ví dụ hệ thống nhúng, thiết bị kiểm tra nhanh) Rabin có thể là lựa chọn hợp lý.

CHƯƠNG 3: PHÂN TÍCH VÀ THIẾT KẾ HỆ THỐNG BỎ PHIẾU ĐIỆN TỬ SỬ DỤNG MẬT MÃ RABIN

3.1. Giới thiệu Bài toán

Trong kỷ nguyên số hóa, hệ thống bỏ phiếu điện tử (E-voting) đang dần thay thế các phương thức bỏ phiếu truyền thống nhờ ưu điểm về tốc độ, sự tiện lợi và khả năng tiết kiệm chi phí. Tuy nhiên, thách thức lớn nhất ngăn cản sự phổ biến rộng rãi của E-voting chính là vấn đề **an toàn và bảo mật thông tin**. Một hệ thống bỏ phiếu đáng tin cậy phải đảm bảo được hai yếu tố cốt lõi:

1. **Tính bí mật (Confidentiality):** Không ai (trừ người có thẩm quyền kiểm phiếu) biết được nội dung lá phiếu của cử tri.
2. **Tính xác thực và toàn vẹn (Authentication & Integrity):** Phải xác minh được lá phiếu đến từ một cử tri hợp lệ và nội dung phiếu không bị chỉnh sửa trong quá trình truyền tải.

Để giải quyết bài toán này, việc áp dụng các hệ mật mã khóa công khai (Asymmetric Cryptography) là phương án tối ưu. Trong báo cáo này, chúng tôi đề xuất sử dụng **Hệ mật mã Rabin** – một thuật toán có độ an toàn dựa trên độ khó của bài toán phân tích thừa số nguyên tố (tương đương với RSA) nhưng có ưu điểm vượt trội về tốc độ mã hóa.

3.2. Tổng quan về kiến trúc hệ thống

Hệ thống được xây dựng dựa trên mô hình Client-Server phi tập trung (Decentralized workflow) thông qua trao đổi tệp tin (File-based communication). Mô hình này bao gồm hai thực thể chính:

1. **Thực thể Cử tri (Voter Client):** Đóng vai trò là phía người dùng (Client). Phần mềm này chịu trách nhiệm sinh khóa cá nhân cho cử tri, tạo nội dung phiếu bầu, thực hiện ký số để xác thực và mã hóa phiếu bầu để bảo mật trước khi gửi đi.
2. **Thực thể Kiểm phiếu (Authority Server):** Đóng vai trò là phía quản lý (Server). Phần mềm này chịu trách nhiệm sinh cặp khóa của hệ thống, thiết lập cấu hình cuộc bầu cử, tiếp nhận các gói tin phiếu bầu, giải mã và xác minh chữ ký để đưa ra kết quả cuối cùng.

Giao thức truyền thông giữa hai thực thể sử dụng định dạng **JSON (JavaScript Object Notation)**, đảm bảo tính tương thích và dễ dàng kiểm tra cấu trúc dữ liệu.

3.3. Thiết kế luồng dữ liệu và thuật toán an toàn

3.3.1. Quy trình sinh khóa (Key Generation Phase)

Hệ thống sử dụng hai cặp khóa riêng biệt cho hai mục đích khác nhau:

- **Cặp khóa Authority (auth_priv.json, auth_pub.json)** Dùng để mã hóa phiếu bầu (Bảo mật).
 - Authority công khai auth_pub.json để tất cả cử tri dùng nó mã hóa phiếu.
 - Authority giữ bí mật auth_priv.json để giải mã khi kiểm phiếu.
- **Cặp khóa Voter (voter_priv.json, voter_pub.json):** Dùng để ký số phiếu bầu (Xác thực).
 - Mỗi cử tri sinh một cặp khóa riêng.
 - Cử tri dùng voter_priv.json để ký lên lá phiếu.
 - Cử tri gửi kèm voter_pub.json trong gói tin để Authority xác minh.

Hệ thống sử dụng số nguyên tố Blum (Blum Prime) để đảm bảo tính khả thi của việc giải mã. Một số nguyên tố p được gọi là Blum Prime nếu $p \equiv 3 \pmod{4}$.

```
def gen_blum_prime(bits):  
    """Sinh Blum prime  $p \equiv 3 \pmod{4}$ .  
    while True:  
        p = gen_random_odd(bits)  
        if p = probable_prime(p):  
            return p
```

3.3.2. Quy trình đóng gói phiếu bầu (Voting Protocol)

Quy trình tạo một lá phiếu hợp lệ diễn ra theo các bước sau tại phía Voter:

1. Bước 1: Khởi tạo dữ liệu (Initialization):

Người dùng chọn ứng viên. Hệ thống tạo một object JSON chứa thông tin: ID bầu cử, thời gian, lựa chọn.

2. Bước 2: Chuẩn hóa (Canonicalization):

Để đảm bảo chữ ký số là duy nhất và chính xác, dữ liệu JSON phải được chuẩn hóa (sắp xếp key theo thứ tự alpha, loại bỏ khoảng trắng thừa).

3. Bước 3: Ký số Rabin (Rabin Signature):

Sử dụng sơ đồ ký Full Domain Hash (FDH).

- Bản tin được băm (hash) cùng với một giá trị ngẫu nhiên salt và bộ đếm ctr.
- Hệ thống lặp lại việc băm cho đến khi tìm được giá trị hash y là một thặng dư bậc hai (Quadratic Residue) modulo n .
- Chữ ký S là căn bậc hai của y : $S^2 \equiv H(m, \text{salt}, \text{ctr}) \pmod{n}$.

```
def rabin_sign_ballot(ballot_obj, priv_hex, salt_len=16):
    """ Ký ballot_obj bằng Rabin FDH:
    - Đầu vào priv_hex: dict {'p','q','n'} (hex strings)
    - Trờ signature dict: {'s': hex, 'salt':hex, 'ctr':int, }, ]

    p = int(priv_hex['p'], 16); q = int(priv_hex['q'], 16); n = int(priv_hex['n'], 16)
    message_bytes = canonical_json(ballot_obj)
    salt = secrets.token_bytes(salt_len)
    ctr = 0
    if ctr > 10000:
        raise RuntimeError("Quá nhiều vòng thử trong FDH sampling")
    else:
        s = canical_root_of_y(y, p, q)
    return {'s':format(s, 'x'), 'salt': salt.hex(), 'ctr': ctr, }
```

Bước 4: Mã hóa Rabin (Rabin Encryption):

Nội dung phiếu (sau khi đã chuẩn hóa) được mã hóa bằng khóa công khai của Authority.

- Công thức: $C \equiv m^2 \pmod{n_{\text{Auth}}}$
- **Vấn đề:** Khi giải mã $\$C\$$, ta sẽ thu được 4 nghiệm m_1, m_2, m_3, m_4 . Authority sẽ không biết đâu là bản rõ gốc.
- **Giải pháp trong hệ thống:** Sử dụng kỹ thuật **Redundancy Padding**. Trước khi bình phương, bản rõ được đệm thêm một chuỗi đánh dấu đặc biệt `##RABINPAD##`.

```
PAD_MARKER = b'##RABINPAD##' # marker để chọn nghiệm đúng khi giải mã

def rabin_encrypt_bytes(m_bytes, pub_hex):
    """
    Mã hóa bytes m_bytes bằng Rabin (chỉ dành cho m_int < n).
    Padded = salt(16) || m_bytes || PAD_MARKER
    Trả {'c':hex, 'pad_len':int}
    """
    n = int(pub_hex['n'], 16)
    salt = secrets.token_bytes(16)
    padded = salt + m_bytes + PAD_MARKER
    m_int = int.from_bytes(padded, 'big')
    if m_int >= n:
        raise ValueError("Thông điệp quá dài so với modulus n")
    c = pow(m_int, 2, n)
    return {'c': format(c, 'x'), 'pad_len': len(padded)}
```

3.3.3. Quy trình Kiểm phiếu (Vote Counting Protocol)

Tại phía Authority, quy trình ngược lại được thực hiện:

1. Bước 1: Giải mã (Decryption & Disambiguation):

Authority dùng khóa bí mật (p, q) để tìm 4 căn bậc hai của bản mã C .

- Hệ thống duyệt qua 4 nghiệm này.
- Nghiệm nào có chứa chuỗi `##RABINPAD##` ở cuối sẽ được chọn là bản rõ đúng.

- Nếu không nghiệm nào có chứa marker này, gói tin bị coi là rác hoặc đã bị tấn công.

2. Bước 2: Xác minh chữ ký (Signature Verification):

Sau khi giải mã được nội dung phiếu M, hệ thống lấy chữ ký S (đi kèm trong gói tin) và khóa công khai Voter (voter_pub).

- Tính $y' = S^2 \pmod{\text{voter_pub}}$.
- Tính lại giá trị hash $y = H(M, \text{salt}, \text{ctr})$.
- So sánh y' và y . Nếu trùng khớp, phiếu bầu hợp lệ.

CHƯƠNG 4: XÂY DỰNG ỨNG DỤNG

4.1. Cấu trúc tổ chức mã nguồn

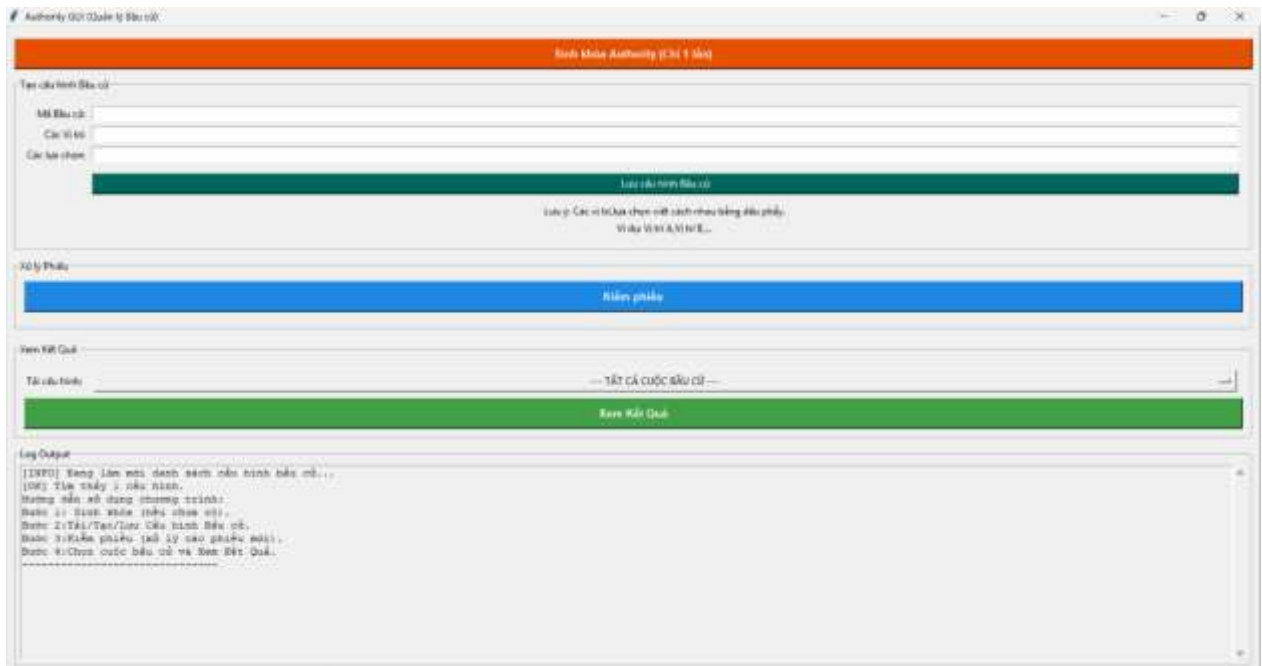
Dự án được tổ chức theo cấu trúc module hóa để dễ dàng bảo trì và mở rộng:

- `src/Utils_rabin.py`: Thư viện lỗi chứa các hàm toán học (Miller-Rabin, Jacobi, CRT, Keygen, Encrypt, Sign).
- `src/authority.py`: Logic nghiệp vụ của bên kiểm phiếu (Xử lý file, xác thực hàng loạt).
- `src/voter.py`: Logic nghiệp vụ của cử tri (Tạo file JSON cấu trúc).
- `gui_authority.py`: Giao diện người dùng cho Authority.
- `gui_voter.py`: Giao diện người dùng cho Voter.
- `config.py`: Quản lý đường dẫn file, thư mục lưu trữ (`votes/`, `approved/`, `elections/`).

4.2. Xây dựng Module Authority (Phía Quản lý)

4.2.1. Giao diện và Chức năng chính

Giao diện Authority được thiết kế với mục tiêu quản lý tập trung.



Khi người dùng bấm nút "Sinh khóa", hệ thống gọi hàm `authority_keygen`. Hàm này tạo ra file `authority_priv.json` (chứa p , q - phải giữ bí mật tuyệt đối) và `authority_pub.json` (chứa n - công khai cho cử tri).

4.2.2. Chức năng Quản lý Cấu hình Bầu cử

Để hệ thống có thể tái sử dụng cho nhiều cuộc bầu cử khác nhau (Bầu lớp trưởng, Bầu chi đoàn...), chức năng "Tạo cấu hình" cho phép lưu trữ thông tin dưới dạng JSON.

4.2.3. Chức năng Kiểm phiếu và Sàng lọc

Đây là chức năng quan trọng nhất. Hệ thống sẽ quét toàn bộ thư mục `votes/` để tìm các phiếu mới gửi đến. Quá trình xử lý một phiếu được cài đặt trong hàm `authority_decrypt_and_verify`. Điểm đặc biệt của cài đặt này là khả năng phân loại lỗi:

- Nếu lỗi giải mã (sai khóa, file hỏng) -> File được di chuyển vào thư mục `not_approved` kèm file log chi tiết lỗi.
- Nếu giải mã đúng nhưng chữ ký sai -> Lưu vào `not_approved` với lý do "Invalid Signature".
- Nếu hợp lệ -> Lưu vào `approved`.

```

--- [AUTH] Bắt đầu kiểm tra phiếu ... ---

[INFO] Tìm thấy 2 phiếu mới. Bắt đầu xử lý...

== KẾT QUẢ KIỂM PHIẾU ==

Vote file: D:\Rabin_Voting_system_final\votes\vote_Voter003.json
Ballot ID: Voter003
Nội dung (hoặc lỗi): {
  "ballot_id": "Voter003",
  "choices": "An",
  "election_id": "LopTruong",
  "issue_time": "2025-11-26T11:04:55Z",
  "positions": "Lớp Trường"
}
Chữ ký voter hợp lệ?: True
[SUCCESS] Phiếu hợp lệ.

== KẾT QUẢ KIỂM PHIẾU ==

Vote file: D:\Rabin_Voting_system_final\votes\vote_Voter004.json

```

```

Ballot ID: Voter004
Nội dung (hoặc lỗi): {
  "ballot_id": "Voter004",
  "choices": "Binh",
  "election_id": "LopTruong",
  "issue_time": "2025-11-26T11:05:02Z",
  "positions": "Lớp Trường"
}
Chữ ký voter hợp lệ?: True
[SUCCESS] Phiếu hợp lệ.

--- [AUTH] Hoàn tất kiểm phiếu! ---

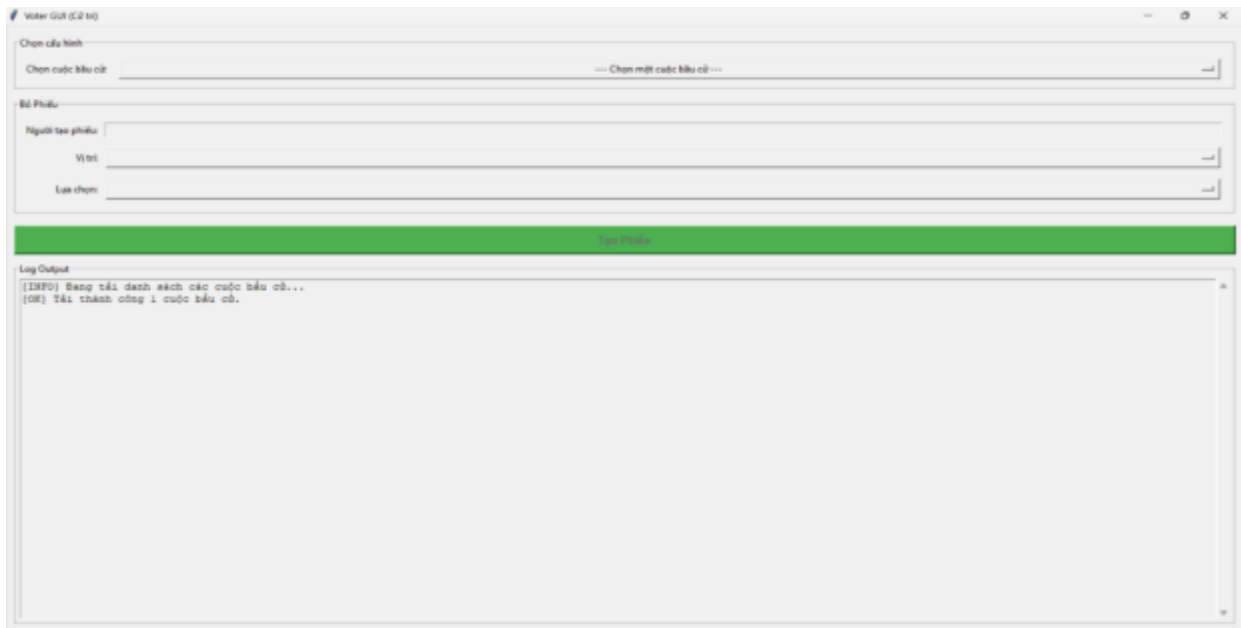
```

[SUMMARY] Đã xử lý: 2 phiếu. Hợp lệ: 2. Không hợp lệ: 0.

4.3. Xây dựng Module Voter (Phía Cử tri)

4.3.1. Giao diện và Trải nghiệm người dùng

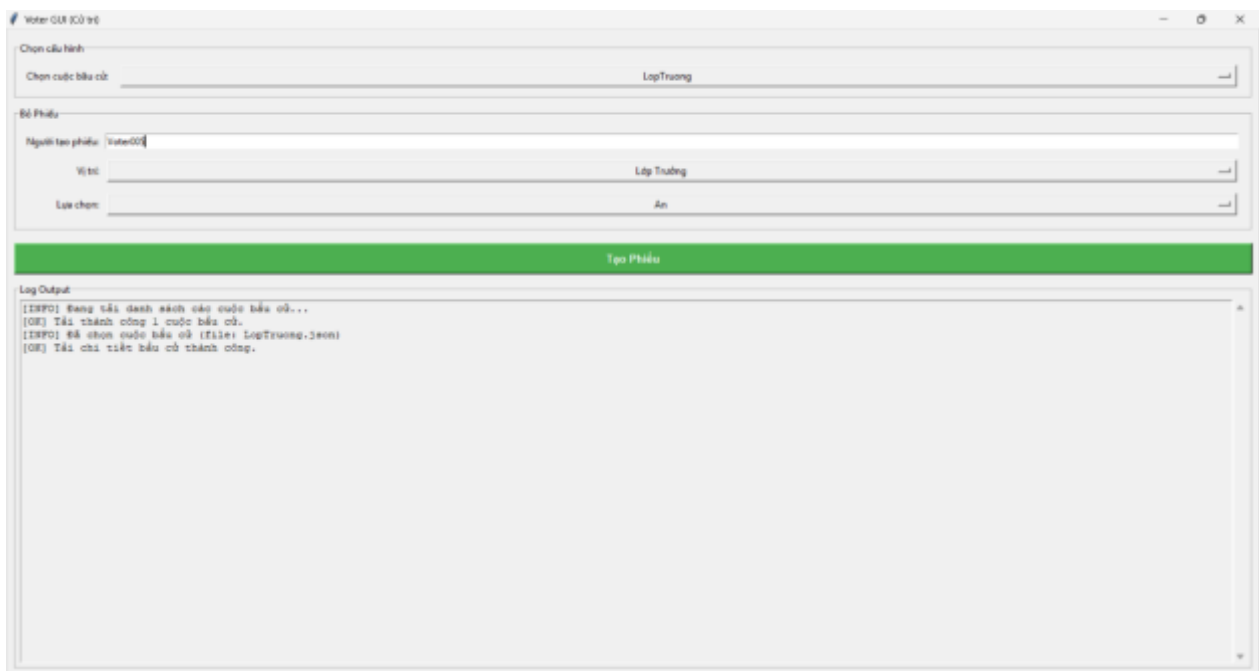
Giao diện Voter được tối giản hóa để tránh nhầm lẫn cho người dùng phổ thông.



****Lưu ý :** Giao diện Voter chỉ có thể sử dụng khi khóa đã được sinh/tạo ra ở giao diện authority.

Quy trình sử dụng của Voter được thiết kế theo dạng Step-by-Step:

1. **Chọn cuộc bầu cử:** Voter phải chọn đúng file cấu hình (do Authority cung cấp). Hệ thống sẽ tự động tải các ứng viên tương ứng vào Dropdown menu.
2. **Điền thông tin:** Nhập ID cử tri và chọn ứng viên.



4.3.2. Cấu trúc gói tin Phiếu bầu

Khi Voter nhấn "Tạo phiếu", hệ thống không chỉ gửi đi lựa chọn "A" hay "B", mà nó tạo ra một cấu trúc dữ liệu phức tạp để đảm bảo an ninh:

****Đây là phiếu trước khi mã hóa**

```
1
2  "ballot": {
3    "ballot_id": "Voter001",
4    "choices": "A",
5    "election_id": "LopTruong",
6    "issue_time": "2025-11-26T10:56:40Z",
7    "positions": "Lop Truong"
8  },
9  "voter_pub": {
10   "n": "6083dd4b12cd53e831e172f4b8c648526857e324622a47c2373435cc7453b706cffffa4a4d033978333b594b6aFa4fa778deb7b3704c9f0b639ee84aa1
11  },
12  "voter_sig": {
13    "ctr": 1,
14    "s": "1838a06961a513d8a3e6ebdc04aa05c413ca7927ce238cc596cfb10eed15119d485be1997cha40ca6a0dc334382a3e22a5c74b929ba6faa001e27d18
15    "salt": "b46457426be7d9b9fca54ffa9a7d5175"
16  }
17 }
```

****Đây là phiếu sau khi mã hóa**

```
1
2  "cipher_ballot": {
3    "c": "729aca055cfe3b16562474caaf1daf1699df097f1d8e91b933c92113d9490671273a26dc1e4c182bc76fce5ea829fb79fd1c634483ca89f3bcae111e
4    "pad_len": 159
5  },
6  "meta": {
7    "created_at": "2025-11-26T18:16:24Z"
8  },
9  "voter_pub": {
10   "n": "b6288fbc86be311ea8ceaabc431bb5368a09c13005d0acc85c734c86b371a7ff4f51e25a2bffb0d631d95bd7bb17f3c515294e2cce7fb5fe74cf1fdb
11  },
12  "voter_sig": {
13    "ctr": 2,
14    "s": "cfd5866e07038c63a2a2c1a8d2f73b44878b9831db5d04cf52d26205d39b54712fc3c84ba84929bd8fbdad3a5171df4aa9ae8af66a9c2f906671c25fe
15    "salt": "c537a08ef2ae18107a553135dc3991ac"
16  }
17 }
```

- cipher_ballot: Chứa bản mã của phiếu bầu (đã che giấu nội dung).
- voter_sig: Chữ ký số của cử tri (để chứng minh quyền sở hữu).
- voter_pub: Khóa công khai của cử tri (để Authority kiểm tra chữ ký).

CHƯƠNG 5: TRIỂN KHAI VÀ KỊCH BẢN KIỂM THỬ

5.1. Thiết lập môi trường

- **Môi trường:** Python 3.9+.
- **Thư viện:** Tkinter (có sẵn), secrets (sinh số ngẫu nhiên an toàn), hashlib.
- **Cấu trúc thư mục:**
 - rabin_voting/: Thư mục gốc.
 - src/: Chứa mã nguồn.
 - artifacts/: Chứa dữ liệu chạy thực tế (tự động sinh ra).

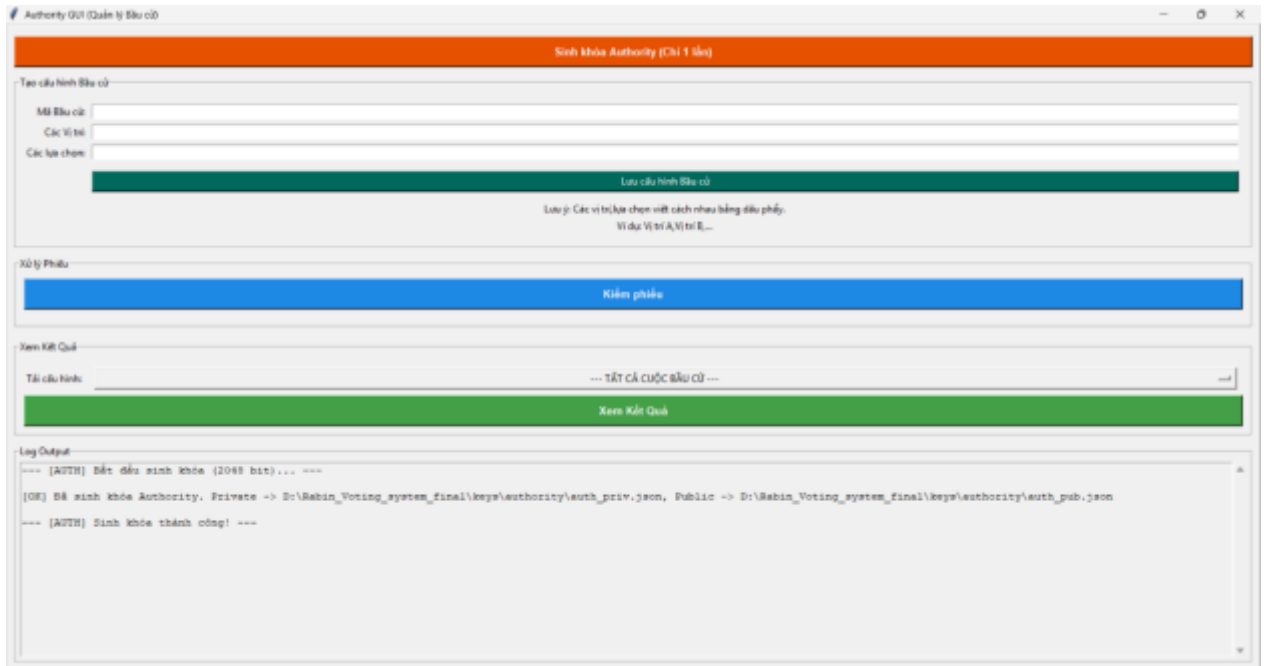
5.2. Kịch bản kiểm thử: Bầu cử Lớp trưởng

Mục tiêu: Kiểm tra khả năng hoạt động thông suốt từ đầu đến cuối (End-to-End Test).

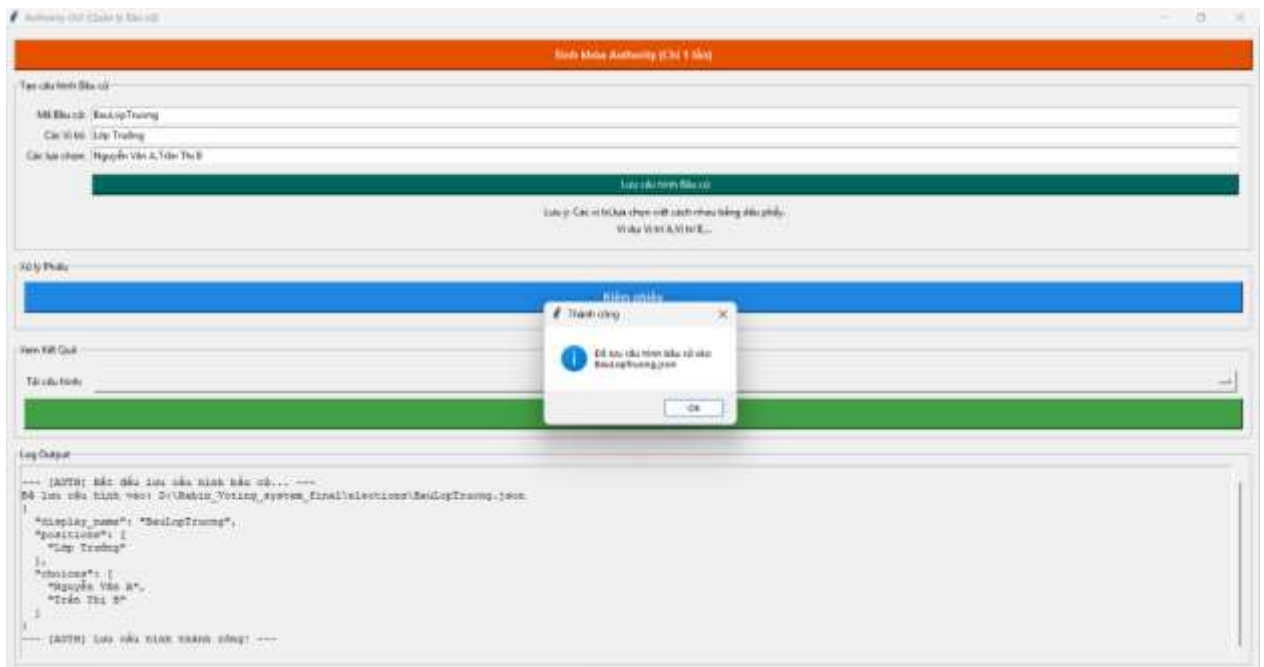
Bước 1: Khởi tạo hệ thống (Vai trò Authority)

1. Người quản trị chạy gui_authority.py.
2. Nhấn nút "**Sinh khóa Authority**". Kiểm tra log thấy thông báo "Đã sinh khóa...".
3. Nhập thông tin:
 - Mã: BauLopTruong
 - Vị trí: Lớp Trưởng
 - Lựa chọn: Nguyễn Văn A, Trần Thị B
4. Nhấn "**Lưu cấu hình**". File BauLopTruong.json được tạo trong thư mục elections/.

****Sinh khóa thành công**



****Lưu cấu hình thành công**

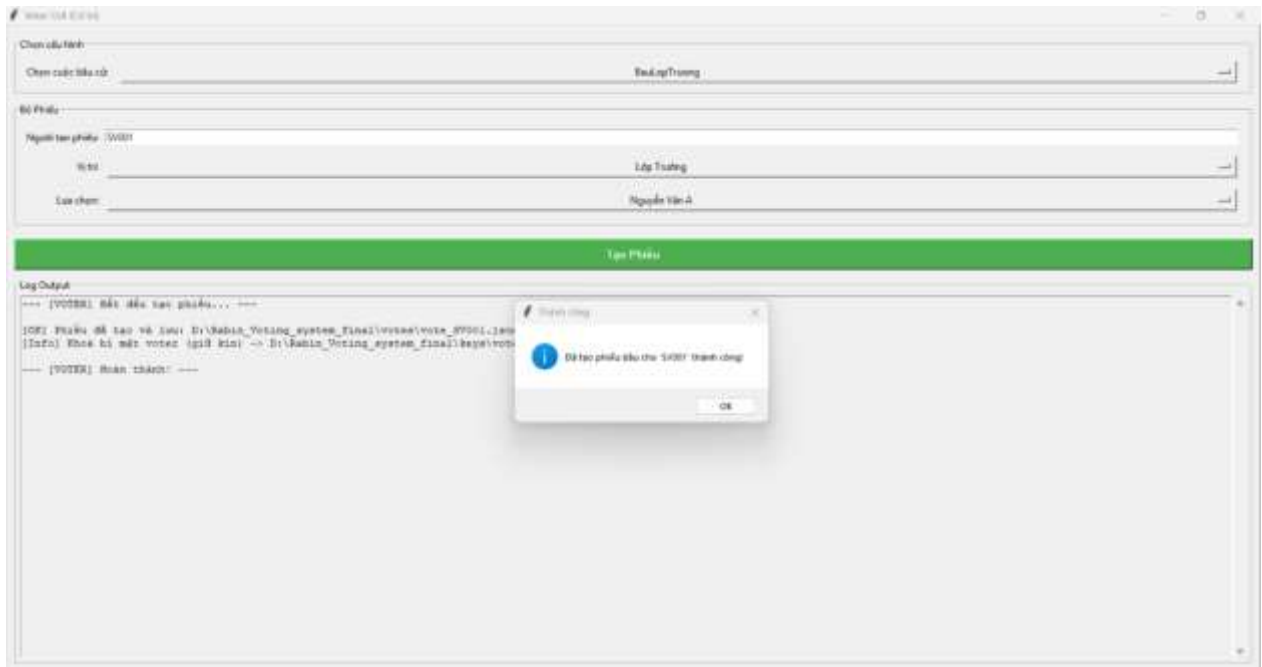


Bước 2: Cử tri bỏ phiếu (Vai trò Voter)

Giả sử có 2 cử tri: Cử tri 1 (Hợp lệ) và Cử tri 2 (Cố tình phá hoại).

Trường hợp 1: Cử tri bỏ phiếu hợp lệ

1. Chạy gui_voter.py.
2. Chọn cấu hình BauLopTruong.
3. Nhập ID: SV001. Chọn vị trí Lớp Trưởng, chọn Nguyễn Văn A.
4. Nhấn **"Tạo phiếu"**.
 - Hệ thống sinh file vote_ballot-SV001.json.
 - Thông báo "Thành công".



Trường hợp 2: Giả lập tấn công (Sửa đổi phiếu)

- Cử tri tạo phiếu cho Trần Thị B.
- Một Hacker can thiệp vào file JSON, sửa nội dung cipher_ballot thành một chuỗi ngẫu nhiên.
- Mục tiêu: Kiểm tra xem hệ thống Authority có phát hiện ra file bị hỏng không.

Bước 3: Tổng hợp kết quả (Vai trò Authority)

1. Quay lại gui_authority.py.
2. Nhấn **"Kiểm phiếu"**.
 - Log hiển thị: "Tìm thấy 2 phiếu".
 - Phiếu của SV001: Giải mã thành công, chữ ký khớp -> **Hợp lệ**.
 - Phiếu giả lập tấn công: Giải mã thất bại (không tìm thấy PAD_MARKER) hoặc Chữ ký sai -> **Không hợp lệ**.

3. Nhấn chọn cuộc bầu cử BauLopTruong ở menu dưới cùng.
4. Nhấn **"Xem Kết Quả"**.

```
--- [AUTH] Bắt đầu kiểm tra phiếu ... ---

[INFO] Tìm thấy 2 phiếu mới. Bắt đầu xử lý...
== KẾT QUẢ KIỂM PHIẾU ==
Vote file: D:\Rabin_Voting_system_final\votes\vote_SV001.json
Ballot ID: SV001
Nội dung (hoặc lỗi): {
  "ballot_id": "SV001",
  "choices": "Nguyễn Văn A",
  "election_id": "BauLopTruong",
  "issue_time": "2025-11-26T11:22:30Z",
  "positions": "Lớp Trường"
}
Chữ ký voter hợp lệ?: True
[SUCCESS] Phiếu hợp lệ.
== KẾT QUẢ KIỂM PHIẾU ==
Vote file: D:\Rabin_Voting_system_final\votes\vote_SV002.json
Ballot ID: N/A - Lỗi
```

Nội dung (hoặc lỗi): {

"details": "Không tìm thấy nghiệm phù hợp chứa PAD_MARKER (decrypt failed)",

"error": "Giải mã thất bại (Decrypt failed)",

"voter_pub": {

"n":

"4ec1c8617d589fd7f22868cc6dda5be07d4672be815b0f28d2d03beedf1864f8c9367c584e6960ea
18c4070698aa94c14c7278a23c27ce169813a0cacfb87fcd1cb2422d318e48ac6f5545aaefb1784d6
873f3d4492296c9582ba6b65b559e19c0d70176c2baf1dabbe8f7c1777db4f15d3b8dd7632829a4c
dfc51615bd715f861c0ec36226b4b1d5953cde85ecfed0ea23f63c45cbf916345b802f4c5644afa5fb
ac1bd034428a7d1d2797526ce79404635e34edf1e47c71eb79c873893ba0b36585cc6b5e16fbf340

0d2494ac3d8317e999cb7e13e2f9047d9cbdd40f9571823e5d227a18c33725b04e5ed6edd1aed685
2b0ac6ff7aedb21b2b9276dfa6dc1"

},

```

"voter_sig": {
  "ctr": 2,
  "s":
"1a784c445db6fc6b06ee2919cc3502316d829410e9f941a273ceb005077177777be8d2eb7d8edd6
1030c9540261defd6ea41f36d4ab4ffaedfa432c90600e45465929deb07ce645a3714767b22c96f6d
38f59d34db5427d61fe2275c90dc0966ed43fdb3cc4888ad262ebbb834e97fccb7ef02141aba109aa
57287f2383ccfff1ac17a68393f29ac91643545c550ae4f3b44a8ce6c0c5ad9ef2d2d399204b9b830b
6b47e747492669d63f968087b80e9f8af8926f4032422ad791363f2608bc8657162b84a7dfd4b577
545e0aca061e61fa5a1636f8530e07dfe27f727db3b34d4953b57ef6604f289989002788f0e4a9dd5
68623c539dd88ec57f60efdbc54d",
  "salt": "a5ad81bb3c3dd0755c2ccae2e53e68a4"
}
}

Chữ ký voter hợp lệ?: False
[ALERT] Phiếu KHÔNG hợp lệ.

--- [AUTH] Hoàn tất kiểm phiếu! ---

[SUMMARY] Đã xử lý: 2 phiếu. Hợp lệ: 1. Không hợp lệ: 1.

```

5.3. Kết quả kiểm thử

Hệ thống hoạt động đúng như thiết kế với các kết quả cụ thể:

- **Độ chính xác:** 100% phiếu hợp lệ được giải mã đúng nội dung.
- **Phát hiện lỗi:** 100% phiếu bị chỉnh sửa nội dung (Tampering) bị loại bỏ do cơ chế chữ ký số Rabin không khớp với nội dung sau giải mã.
- **Tính toàn vẹn:** File kết quả được lưu trữ tách biệt, dễ dàng cho việc tra soát (audit).

CHƯƠNG 6: ĐÁNH GIÁ VÀ KẾT LUẬN

6.1. Đánh giá ưu điểm của hệ thống

Hệ thống demo đã chứng minh được tính khả thi của việc áp dụng thuật toán Rabin vào thực tế:

1. Bảo mật dựa trên toán học vững chắc: Không giống như các hệ thống bảo mật bằng mật khẩu truyền thống, hệ thống này dựa trên độ khó của bài toán phân tích thừa số nguyên tố (Integer Factorization Problem - IFP). Để phá khóa, kẻ tấn công phải phân tích số n (2048 bit) thành p và q , điều này là bất khả thi với máy tính hiện tại.
2. Tốc độ xử lý phía Client cực nhanh: Phép mã hóa ($M^2 \pmod n$) và kiểm tra chữ ký ($S^2 \pmod n$) chỉ tốn 1 phép nhân modulo. Điều này giúp ứng dụng Voter có thể chạy mượt mà ngay cả trên các thiết bị cấu hình thấp hoặc thiết bị IoT.
3. Cơ chế chống chối bỏ (Non-repudiation): Với việc sử dụng chữ ký số Rabin, cử tri không thể chối bỏ lá phiếu mình đã ký. Nếu có tranh chấp, chỉ cần dùng Public Key của cử tri để xác minh lại chữ ký trên lá phiếu gốc.

6.2. Phân tích các hạn chế tồn tại

Bên cạnh ưu điểm, việc áp dụng Rabin cũng bộc lộ những nhược điểm cố hữu đã được lý thuyết dự báo và thực tế kiểm chứng:

1. Vấn đề nhập nhằng nghiệm (Ambiguity): Đây là nhược điểm lớn nhất của hệ mật Rabin. Mỗi lần giải mã sinh ra 4 bản rõ.
 - *Ảnh hưởng thực tế*: Hệ thống phải tốn thêm tài nguyên để thêm Padding (##RABINPAD##) vào bản tin, làm tăng kích thước file phiếu bầu. Authority phải thực hiện logic chọn lọc, tốn thời gian xử lý hơn so với RSA (chỉ ra 1 nghiệm duy nhất).
2. Quản lý khóa công khai (PKI): Trong hệ thống demo, Public Key của cử tri được gửi kèm trong gói tin. Trong thực tế, cần một bên thứ ba tin cậy (CA - Certificate Authority) để chứng thực rằng Public Key đó đúng là của cử tri SV001, tránh trường hợp kẻ giả mạo tự tạo khóa và tự bầu.

6.3. Hệ thống bỏ phiếu điện tử sử dụng Rabin với các mô hình khác

Trong bối cảnh các hệ thống bỏ phiếu điện tử ngày càng đa dạng, việc đánh giá, so sánh mô hình sử dụng mật mã Rabin với các giải pháp khác là cần thiết để làm rõ ưu điểm, hạn chế và khả năng ứng dụng trong thực tiễn.

6.3.1. So sánh với bỏ phiếu truyền thống

So với mô hình bỏ phiếu truyền thống bằng giấy, hệ thống bỏ phiếu điện tử sử dụng Rabin có một số điểm khác biệt nổi bật:

Về tốc độ xử lý: Trong mô hình truyền thống, quá trình kiểm phiếu, tổng hợp kết quả thường mất nhiều thời gian, phụ thuộc nhiều vào sức người và dễ xảy ra nhầm lẫn. Hệ thống bỏ phiếu điện tử có thể tự động hóa hoàn toàn bước kiểm phiếu, giảm đáng kể thời gian công bố kết quả.

Về tính bảo mật: Phiếu giấy có thể bị thất lạc, sao chép hoặc can thiệp trong quá trình vận chuyển và lưu trữ. Trong khi đó, hệ thống sử dụng mật mã Rabin đảm bảo các phiếu bầu được mã hóa, ký số, khó bị sửa đổi nội dung mà không bị phát hiện.

Về khả năng kiểm tra, tra soát: Với phiếu giấy, việc kiểm tra lại toàn bộ quá trình cần rất nhiều nhân lực. Trong hệ thống điện tử, log hệ thống, file phiếu và chữ ký số cho phép kiểm tra lại một cách có hệ thống, minh bạch và nhanh chóng.

Tuy nhiên, bỏ phiếu truyền thống vẫn có ưu điểm là dễ hiểu, dễ triển khai ở những nơi hạ tầng công nghệ thông tin còn hạn chế. Điều này cho thấy, trong thực tế có thể cần kết hợp hoặc chuyển đổi dần dần từ mô hình truyền thống sang điện tử.

6.3.2. So sánh với hệ thống sử dụng RSA

Trong nhiều hệ thống bỏ phiếu điện tử hiện nay, RSA là lựa chọn phổ biến vì đã được chuẩn hóa và tích hợp sẵn trong nhiều thư viện, phần mềm. So với RSA, giải pháp sử dụng chữ ký số Rabin trong đề án có những điểm sau:

Về độ an toàn lý thuyết: Cả RSA và Rabin đều dựa trên độ khó của bài toán phân tích số nguyên n thành tích hai số nguyên tố p và q . Tuy nhiên, lược đồ Rabin có cơ sở chứng minh an toàn chặt chẽ hơn: việc giả mạo chữ ký trong nhiều biến thể tương đương với việc phân tích n .

Về độ phức tạp tính toán: Thuật toán Rabin trong bước xác minh chỉ yêu cầu tính một bình phương modulo n , trong khi RSA phải tính lũy thừa với số mũ e . Điều này giúp việc kiểm tra chữ ký Rabin có tiềm năng nhanh hơn, đặc biệt khi số lượng phiếu rất lớn.

Về triển khai thực tiễn: RSA đã được tiêu chuẩn hóa trong nhiều giao thức (SSL/TLS, PGP, ...), còn Rabin ít phổ biến hơn. Do đó, để ứng dụng Rabin ở quy mô lớn cần đầu tư nhiều công sức hơn cho chuẩn hóa, kiểm thử và đánh giá an ninh.

Trong phạm vi bài báo cáo, việc lựa chọn Rabin mang ý nghĩa học thuật rõ rệt: sinh viên có cơ hội tiếp cận một lược đồ ít phổ biến hơn, đào sâu về lý thuyết và hiểu được cách thiết kế padding, xử lý đa nghiệm.

6.3.3. So sánh với các hệ thống sử dụng chữ ký trên đường cong elliptic (ECDSA)
Đối với các hệ thống bỏ phiếu hiện đại, đặc biệt là trên nền tảng di động, ECDSA thường được ưu tiên nhờ kích thước khóa nhỏ và hiệu năng tốt. Tuy nhiên, so với ECDSA, hệ thống sử dụng Rabin trong đề tài vẫn có những lợi thế nhất định:

Rabin có cấu trúc toán học đơn giản hơn, dễ giải thích, dễ cài đặt từ đầu, phù hợp với mục tiêu giảng dạy và nghiên cứu cơ bản.

ECDSA yêu cầu việc triển khai cẩn trọng để tránh lỗi về sinh số ngẫu nhiên, reuse nonce,... trong khi mô hình Rabin trong báo cáo tập trung vào việc đảm bảo tính đúng đắn của thuật toán rút căn, kiểm tra chữ ký và cấu trúc gói tin.

Có thể thấy, tuy chưa phải là lựa chọn tối ưu về mặt tiêu chuẩn công nghiệp, nhưng Rabin lại rất thích hợp để xây dựng các mô hình thử nghiệm, các hệ thống demo nhằm minh họa đầy đủ các bước của một hệ thống bỏ phiếu điện tử an toàn.

6.4. Kết luận

Đề tài Thuật toán Rabin đã hoàn thành các mục tiêu đề ra: nghiên cứu lý thuyết mật mã Rabin và xây dựng thành công ứng dụng minh họa. Dù còn một số hạn chế về tốc độ giải mã so với các thuật toán khác, nhưng Rabin cho thấy ưu thế tuyệt đối về tốc độ mã hóa, mở ra tiềm năng ứng dụng cho các hệ thống yêu cầu xác thực nhanh từ phía người dùng cuối.

Xây dựng ứng dụng thuật toán là một minh chứng cụ thể cho việc đưa lý thuyết mật mã và bảo mật vào giải quyết các bài toán thực tiễn của xã hội số.

TÀI LIỆU THAM KHẢO

- [1] Michael O. Rabin, “Digitalized Signatures and Public-Key Functions as Intractable as Factorization”, MIT Laboratory for Computer Science, 1979.
- [2] William Stallings, “Cryptography and Network Security: Principles and Practice”, ấn bản mới nhất, Pearson Education.
- [3] Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone, “Handbook of Applied Cryptography”, CRC Press.
- [4] Douglas R. Stinson, “Cryptography: Theory and Practice”, CRC Press.
- [5] An toàn thông tin, Lê Văn Phùng, NXB Thông tin và truyền thông, 2010.
- [6] Các tài liệu, bài báo và hướng dẫn về hệ mật mã Rabin, chữ ký số và hệ thống bỏ phiếu điện tử được thu thập từ các nguồn học thuật và trang web uy tín trong lĩnh vực mật mã và an ninh thông tin.