

HỆ MÃ RSA VÀ CHỮ KÝ SỐ

Người hướng dẫn: **TS. Vũ Thành Nam**

Sinh viên: **Nguyễn Minh Quân**

Lớp: **KSTN Toán Tin-K61**

Cơ sở thực tập: **Tổng công ty Công nghệ và Giải pháp CMC**

Hà Nội, 7/2020

Công việc được giao

- Các kiến thức cơ sở của bảo mật: Hệ mã RSA, chữ ký số, thiết bị chữ ký số HSM,...
- Chương trình: Thiết kế ngôn ngữ C# và từ khóa: signature, hash, namespace: system.security,...
- Kết quả: Báo cáo, code và môi trường.
- Phát triển: Ký PDF, ký mobile.

Quá trình thực tập

- Lập kế hoạch công việc, đặc tả các yêu cầu.
- Tìm tài liệu và nghiên cứu về lý thuyết.
- Xây dựng các thuật toán cơ bản.
- Lựa chọn môi trường, xây dựng chương trình.
- Xây dựng giao diện của chương trình.
- Kiểm tra, chỉnh sửa và tối ưu.
- Viết báo cáo thu hoạch.

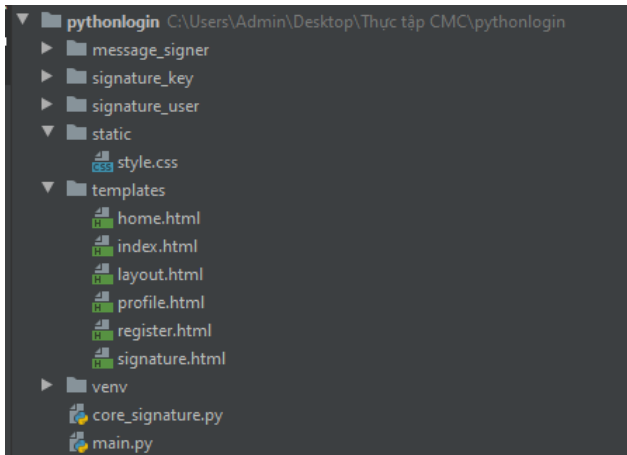
Công việc hoàn thành

- Tìm hiểu và xây dựng các thuật toán trong mật mã khóa công khai RSA.
- Tìm hiểu chữ ký số, thiết bị HSM.
- Xây dựng được chương trình thực hiện được các chức năng cơ bản: giao diện của người dùng, sinh khóa, tạo chữ ký và xác thực chữ ký số.

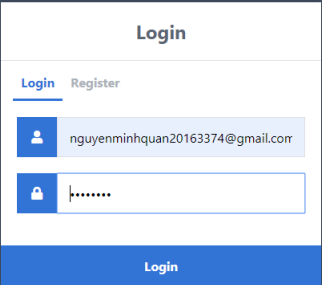
Cài đặt và kết quả

Công cụ	Chú thích	Pha sử dụng
Python	Ngôn ngữ lập trình	
Flask	Thư viện của python	API
RSA	Thư viện của python	CORE
HTML, CSS	Thiết kế giao diện	Giao diện của sản phẩm
MySQL	Hệ cơ sở dữ liệu	Lưu trữ thông tin người dùng

Cài đặt và kết quả



Đăng nhập và đăng ký



The image shows a login form centered on a dark blue background. The form has a white header with the title "Login". Below the header, there are two tabs: "Login" (active) and "Register". The form contains two input fields: the first is for an email address, with the placeholder text "nguyenminhquan20163374@gmail.com", and the second is for a password, represented by a series of dots. At the bottom of the form is a blue button labeled "Login".

Trang chủ người dùng

RSA DIGITAL SIGNATURE

[Home](#) [Profile](#) [Signature](#) [Logout](#)

Profile Information

Username: Nguyen Minh Quan

Password: nmq123987

Email: nguyenminhquan20163374@gmail.com

Sinh cặp khóa bí mật, khóa công khai

Generate RSA Key Size

☒ 512 bit ☐ 1024 bit ☐ 2048 bit ☐ 4096 bit

Public Key:

```
b'-----BEGIN RSA PUBLIC KEY-----  
\nMIGJAoGBAIt4AnhWgiVKITksBjYju9NBxmDVOX3/l9Qt4aozy5pm  
kSqlU9z3ZIMU\ynsr5x2yLyVfufqbWPHbjpgpr1mwUAB5xxJF9F5WV3  
ndqvNhThDtl+ceaoBPHOBvR\yn4QJzhKAVMv7FG7tqST+LG98CEQ  
MKVvqJenL9UwDt5+AweAUjotpAgMBAAE=\n-----END RSA
```

Generate Key

Private Key:

```
b'-----BEGIN RSA PRIVATE KEY-----  
\nMIICYAIBAAKBgQCLeAJ4Vol1Sok5LAY2l7vTQV5g1Tl9/5fUleGqM  
8uaZPeqpVPc\yn925DFLK+cdisl8X7n6m1jx246YKa9ZsFAAecVyRfReV  
ld53arzYU4Q7S/qHmqATX\ynzgXr0eEcC4ZAFtl+XRu7akk/xvfAhEDC  
laqlXjS/VIsA7efgMHgFl6LaQIDAQAB\nAoGAe6yQ7CsyTZVp9+O9llc
```

Khởi tạo chữ ký số

Hash Function

☐ SHA-256 ☒ SHA-384 ☐ SHA-512

Message Send:

Viện Toán Ứng dụng và Tin học Đại Học Bách Khoa Hà Nội

Create Signature

Provide Signature Value:

```
b'=\x19\xfc\x15\xa7\xd0\n\n\xc5G\xa0\xa1\x8f\x15\xe4\xa2\xf2\x80\xc3\x93\xc4\xb1\xc6\x12\x13\xdf\x90\x90\x85,P\xad\xec3\xdc\x9d\xee\x1a\xa0\xd3't\xa3\x0e\xc7\x08\xdc2\xdb\x96\xe3\xed\x8a<\xb1\xd5ak\xac\x9e\x85=\xde\xf8\xbc\xbd\x7\xd7=\t\o\x1a\x95\xa9\x8f\x9b\x6(\xca)\t\x90\x8em\x92^xe1\x9fu\x80\xc5\x9b\x9f\x9c2\xbe\xa6\xaf\x
```

Xác thực chữ ký số

Message Receive:	Signature Verify:
<div>Viện Toán Ứng dụng và Tin học Đại Học Bách Khoa Hà Nội</div>	
<div>Verify Signature</div>	

Activate Windows
Go to Settings to activate Windows.