|  |
| --- |
|  |
| Voto Electrónico |
| Etapa 2 |
|  |
| **Organización de Datos – Cátedra Servetto 2do cuatrimestre 2011** |
| **3/12/2011** |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | | Alfredo Scoppa | 89149 | | Cecilia khalil | 87996 | | Fernando Romera Ferrio | 88406 | | Juan Manuel Romera Ferrio | 88405 | |

Tabla de contenidos

[Diseño 3](#_Toc310596792)

[Introducción 3](#_Toc310596793)

[Diagrama de clases 3](#_Toc310596794)

[Algoritmo simétrico 4](#_Toc310596795)

[Vigenere 4](#_Toc310596796)

[Diagrama de clases 4](#_Toc310596797)

[Algoritmo asimétrico 5](#_Toc310596798)

[RSA 5](#_Toc310596799)

[Diagrama de clases 5](#_Toc310596800)

[Ataque al criptosistema RSA 6](#_Toc310596801)

[Método de factorización de números primos 6](#_Toc310596802)

[Ataque al criptosistema Vigenere 7](#_Toc310596803)

[Método de Kasiski 7](#_Toc310596804)

[Manual de Usuario 8](#_Toc310596805)

# Diseño

## Introducción

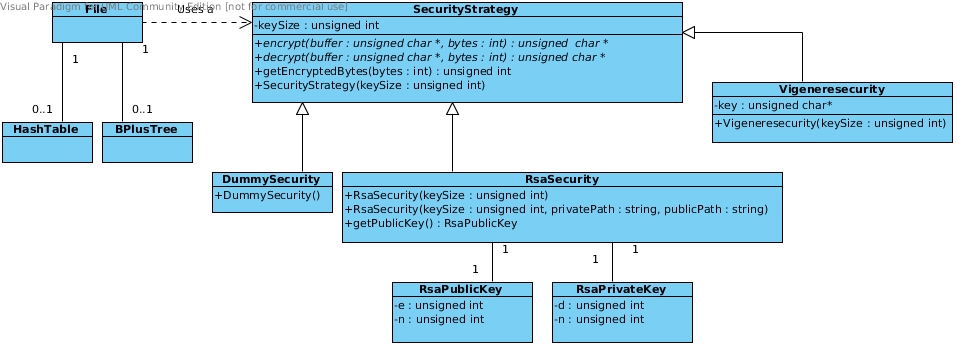
Se decidió optar por una estrategia que impacte lo menor posible en el modelo existente y que sea casi transparente para el mismo.

En definitiva, las estructuras de archivos existentes siguen dependiendo de las mismas clases pero son los archivos (clase File) los que ahora delegan en una estrategia de seguridad el resguardo de los datos.

Para tal objetivo se optó por usar una solución similar a la propuesta por el patrón Strategy, implementando las siguientes estrategias de seguridad:

* Simétrica: VigenereSecurity, para los archivos de reportes.
* Asimétrica: RsaSecurity, para los archivos que almacenan la información de votantes y administradores.
* Texto Plano: DummySecurity, para archivos de texto plano.

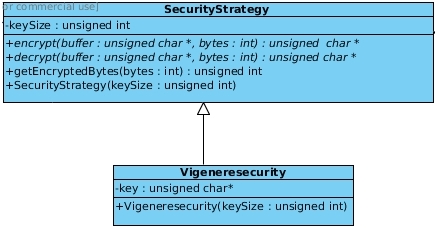
## Diagrama de clases



# Algoritmo simétrico

## Vigenere

## Diagrama de clases



# Algoritmo asimétrico

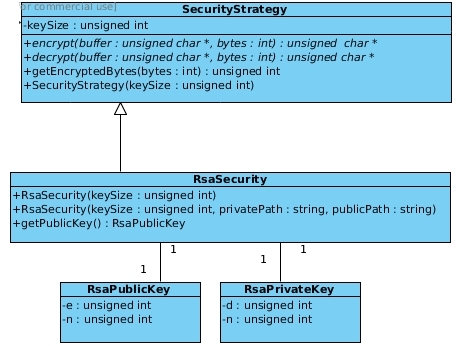
## RSA

Este algoritmo se implementó según lo visto en clase con algunas restricciones e hipótesis simplificadoras aplicadas para que su implementación sea más sencilla.

Primero está el factor del resguardo de las claves, las mismas se almacenan en el sistema de archivos del usuario y sin ninguna protección alguna. Sin embargo, se supone que la carpeta en la cual se almacena la clave privada (.forbiddenAccessFolder) es solo accesible por el dueño de la clave.

Finalmente, aunque parametrizable, el tamaño de las claves está limitado hasta los 26 bits.

## Diagrama de clases



# Ataque al criptosistema RSA

## Método de factorización de números primos

# Ataque al criptosistema Vigenere

## Método de Kasiski

# Manual de Usuario

Ver documento adjunto: ManualDeUsuario.pdf