Proyecto 2: Administrador Seguro de Contraseñas en Haskell

Portada

Proyecto 2: Administrador Seguro de Contraseñas
Curso: Lenguajes de Programación
Paradigma Funcional
Integrantes:

- Daniel Alemán
- Luis Meza

Índice

Enlace de GitHub

Repositorio del Proyecto

Descripción del Proyecto

Este proyecto es un administrador de contraseñas de línea de comandos implementado en Haskell. Permite a los usuarios gestionar credenciales de manera segura mediante una interfaz de terminal, con las siguientes características:

- Registro e inicio de sesión protegidos por PIN
- Almacenamiento cifrado de contraseñas en archivos locales
- Visualización segura y organizada de credenciales
- Operaciones completas de gestión (agregar, modificar, eliminar)
- Funcionalidad para copiar credenciales al portapapeles

El sistema está diseñado siguiendo el paradigma funcional, aprovechando las ventajas de Haskell en seguridad, inmutabilidad y manejo de efectos secundarios controlados.

Requisitos

- Haskell Stack
- GHC >= 9.0 (Stack lo instalará automáticamente)
- Dependencias (incluidas en el archivo .cabal):
  - directory: para manejo de directorios y archivos
  - process: para interacción con el portapapeles
  - bytestring: para el manejo eficiente de datos binarios
  - text: para manipulación de texto
  - base64-bytestring: para codificación Base64
  - split: para procesamiento de cadenas

Instalación

1. **Clonar el repositorio**:

```
git clone https://github.com/DanielAR27/Proyecto2-Lenguajes
cd Proyecto2-Lenguajes
```

2. **Compilar el proyecto**:

```
stack build
```

3. **Ejecutar el programa**:

```
stack exec admin
```

4. **Ubicación de datos**:

   El programa almacena sus datos en la carpeta `src/data/` que se crea automáticamente durante la primera ejecución.

Manual de Usuario

Menú Principal

Al iniciar el programa, se mostrará el siguiente menú:

```
================================================
=       ADMINISTRADOR SEGURO DE CONTRASEÑAS     =
================================================
=                                               =
=  1. Registrarse                               =
=  2. Iniciar Sesión                            =
```

```
=  3. Salir                                          =
=                                                    =
======================================================
```

Registro de Usuario

1. Seleccione la opción `1` en el menú principal.
2. Ingrese un nombre de usuario (sin espacios).
3. Ingrese un PIN numérico (solo números).
4. El sistema confirmará el registro exitoso.

Iniciar Sesión

1. Seleccione la opción `2` en el menú principal.
2. Ingrese su nombre de usuario.
3. Ingrese su PIN.
4. Si las credenciales son correctas, accederá al menú de gestión de contraseñas.

Salir del sistema

1. Seleccione la opción `3` en el menú principal.
2. Se le preguntará si está seguro de salir, escriba en la consola `s` para confirmar su decisión. En caso rechazarla escriba `n` en su lugar.
3. El programa terminará exitosamente.

Gestión de Contraseñas

Una vez iniciada sesión, tendrá acceso a las siguientes opciones:

```
======================================================
=            GESTIÓN DE CONTRASEÑAS                  =
======================================================
=  1. Ver contraseñas                                =
=  2. Agregar contraseña                             =
=  3. Modificar contraseña                           =
=  4. Eliminar contraseña                            =
=  5. Copiar usuario al portapapeles                 =
=  6. Copiar contraseña al portapapeles              =
=  7. Cerrar sesión                                  =
======================================================
```

Ver Contraseñas

Al seleccionar esta opción, se mostrará una tabla con todas las contraseñas guardadas:

- **ID**: Número identificador de la contraseña
- **Título**: Nombre del servicio o sitio

- **Usuario**: Usuario parcialmente oculto (Ej: "Ju*n")
- **Contraseña**: Completamente oculta con asteriscos

Agregar Contraseña

1. Ingrese el título (sitio o servicio).
2. Ingrese el nombre de usuario.
3. Ingrese la contraseña.
4. Confirme la operación.

Modificar Contraseña

1. Seleccione el ID de la contraseña a modificar.
2. Ingrese los nuevos datos (deje en blanco para mantener el valor actual).
3. Confirme los cambios.

Eliminar Contraseña

1. Seleccione el ID de la contraseña a eliminar.
2. Confirme la eliminación.

Copiar Usuario/Contraseña

1. Seleccione el ID de la credencial.
2. El sistema copiará el usuario o la contraseña al portapapeles.

Cerrar Sesión

Seleccione la opción `7` para volver al menú principal.

Arquitectura Lógica

Organización de Módulos

```
Proyecto2-Lenguajes/
├── src/
│   ├── /data              -- Almacenamiento de credenciales cifradas
│   ├── Main.hs            -- Punto de entrada y control principal
│   ├── UI.hs              -- Interfaz de usuario en terminal
│   ├── User.hs            -- Gestión de usuarios y autenticación
│   ├── Password.hs        -- Operaciones sobre contraseñas
│   ├── FileManager.hs     -- Manejo de persistencia
│   ├── Crypto.hs          -- Sistema de cifrado
│   └── Types.hs           -- Definiciones de tipos de datos
├── Proyecto2-Lenguajes.cabal -- Archivo de configuración del proyecto
├── README.md              -- Documentación del proyecto
├── LICENSE                -- Licencia del software
├── Setup.hs              -- Script de configuración para Cabal
```

```
├── stack.yaml            -- Configuración de Stack
└── stack.yaml.lock       -- Archivo de bloqueo de dependencias
```

Componentes Clave

- **Sistema de Cifrado**: Implementado en `Crypto.hs`, utiliza una combinación de Base64 y cifrado César para proteger la información sensible.
- **Gestión de Usuarios**: Manejado por `User.hs`, controla el registro e inicio de sesión con validación de PIN.
- **Persistencia**: Implementada en `FileManager.hs`, maneja la lectura y escritura de archivos cifrados, incluyendo manejo de errores y recuperación.
- **Gestión de Contraseñas**: Implementada en `Password.hs`, proporciona todas las operaciones CRUD para las contraseñas.
- **Interfaz de Usuario**: Dividida entre `Main.hs` y `UI.hs`, maneja la interacción con el usuario y el flujo del programa.

Funcionamiento

Flujo Principal

1. **Inicio**: El programa inicia mostrando el menú principal.
2. **Registro/Login**:
    - Al registrarse, se crea un archivo cifrado para el usuario con su PIN.
    - Al iniciar sesión, se valida el PIN contra el almacenado.
3. **Gestión de Contraseñas**:
    - Cada contraseña se almacena como una entrada en el archivo del usuario.
    - Las operaciones (agregar, modificar, eliminar) actualizan el archivo cifrado.
4. **Seguridad**:
    - Toda la información se almacena cifrada, nunca en texto plano.
    - El PIN nunca se muestra en pantalla al introducirlo.
    - Las contraseñas se muestran ocultas en la interfaz.

Sistema de Cifrado

El sistema utiliza un enfoque de dos etapas:

1. **Cifrado César**: Desplaza cada carácter por un valor fijo.
2. **Codificación Base64**: Convierte los datos binarios resultantes a formato Base64.

La combinación de estas técnicas proporciona un nivel básico de seguridad para proteger la información sensible.

Persistencia

- Cada usuario tiene su propio archivo de contraseñas cifrado.
- La primera línea del archivo contiene el PIN cifrado.
- Las líneas siguientes contienen las entradas de contraseñas, cada una cifrada individualmente.
- Se utiliza un archivo temporal para el usuario actualmente en sesión.

Este diseño permite mantener las contraseñas seguras incluso si el archivo es accedido por terceros.