

LAPORAN PROJECT AKHIR
CRYPTOGRAPHY



DISUSUN OLEH:

RAFLI

F1D022022

TEKNIK INFORMATIKA
UNIVERSITAS MATARAM
2025/2026

SISTEM LOGIN CUSTOM MENGGUNAKAN TEKNIK CRYPTOGRAPHY DENGAN GUI MODERN (PYQT5)

1. Pendahuluan

Pada era digital saat ini, autentikasi pengguna menjadi aspek penting dalam sistem keamanan aplikasi. Salah satu metode yang digunakan untuk melindungi kredensial pengguna adalah teknik kriptografi. Dalam project ini, dikembangkan sistem login custom berbasis Python dengan antarmuka pengguna grafis (GUI) menggunakan PyQt5.

Tujuan dari project ini adalah merancang dan membangun sistem login yang aman, dengan menyimpan data password dalam bentuk hash menggunakan algoritma bcrypt, serta menyajikan antarmuka modern dan fungsional.

2. Perancangan Sistem

- **Fitur Utama:**
 - a. **Registrasi:** Pengguna membuat akun dengan username dan password
 - b. **Login:** Pengguna memasukkan kredensial untuk diverifikasi
 - c. **Selamat Datang:** Halaman setelah login berhasil menampilkan nama pengguna
 - d. **Logout:** Kembali ke halaman login
- **Alur Kerja Sistem:**
 - a. Pengguna membuka aplikasi dan melihat halaman Login
 - b. Jika belum memiliki akun, pengguna dapat berpindah ke halaman Registrasi
 - c. Saat registrasi:
 - Password dikonversi ke byte, diberi salt otomatis, lalu di hash menggunakan bcrypt
 - Username dan hash password disimpan ke database SQLite
 - d. Saat login:
 - Username dicocokkan dengan data di database
 - Password yang dimasukkan akan diverifikasi dengan hash dari database menggunakan `bcrypt.checkpw()`
 - Jika cocok, pengguna diarahkan ke halaman selamat datang
 - Jika tidak cocok, muncul notifikasi gagal login

- e. Di halaman selamat datang, terdapat tombol Keluar untuk kembali ke halaman login
- Struktur GUI:
Aplikasi terdiri dari tiga halaman dalam QStackedWidget:
 - LoginPage: untuk masuk
 - RegisterPage: untuk daftar
 - HomePage: untuk tampilan selamat datang

3. Struktur Database (SQLite)

Kolom	Tipe	Keterangan
id	INTEGER PRIMARY KEY	ID unik (otomatis)
username	TEXT NOT NULL UNIQUE	Nama pengguna
password_hash	TEXT NOT NULL	Password yang sudah di-hash (bcrypt)

4. Teknik Cryptography Yang Digunakan

Sistem ini menggunakan teknik hashing dan salting dari library bcrypt, sebagai standar keamanan login

- a. **Hashing:** Mengubah password menjadi bentuk acak yang tidak bisa dibalik
- b. **Salting:** Menambahkan string acak (salt) sebelum hashing, untuk mencegah serangan tabel hash (rainbow table)
- c. Library **bcrypt** sudah menggabungkan hashing dan salting dalam satu proses

Library Tambahan:

- bcrypt: Untuk hashing dan verifikasi password
- sqlite3: Untuk menyimpan dan membaca data pengguna
- PyQt5: Untuk membangun GUI

5. Fungsi - Fungsi

- a. `init_db()`
 - Membuat database dan tabel users jika belum ada
- b. `LoginPage`
 - `login()`: Mengecek username & password, lalu memverifikasi password menggunakan `bcrypt.checkpw()`
- c. `RegisterPage`

- `register()`: Meng-hash password dan menyimpan data ke database. Dan menangani error duplikat username

d. `HomePage`

- `set_username()`: Menampilkan teks "Selamat datang [username]"
- `logout()`: Kembali ke halaman login (index 0 dari `QStackedWidget`)

e. `main()`

- Menginisialisasi aplikasi, database, dan tampilan GUI
- Menentukan urutan halaman yang akan ditampilkan dalam `QStackedWidget`

6. Source Code

a. Registrasi (Hashing Password):

```
password_bytes = pw.encode()
hashed = bcrypt.hashpw(password_bytes, bcrypt.gensalt())
```

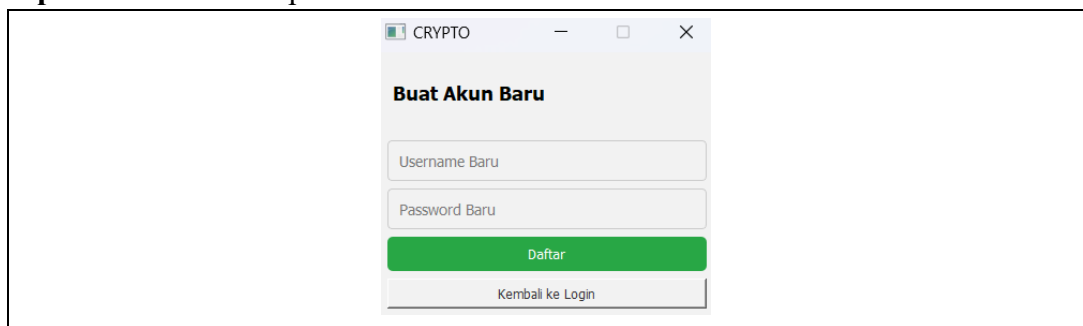
b. Login (Verifikasi Hash):

```
if bcrypt.checkpw(pw.encode(), result[0]):
    self.home_page.set_username(uname)
    self.stacked_widget.setCurrentIndex(2)
```

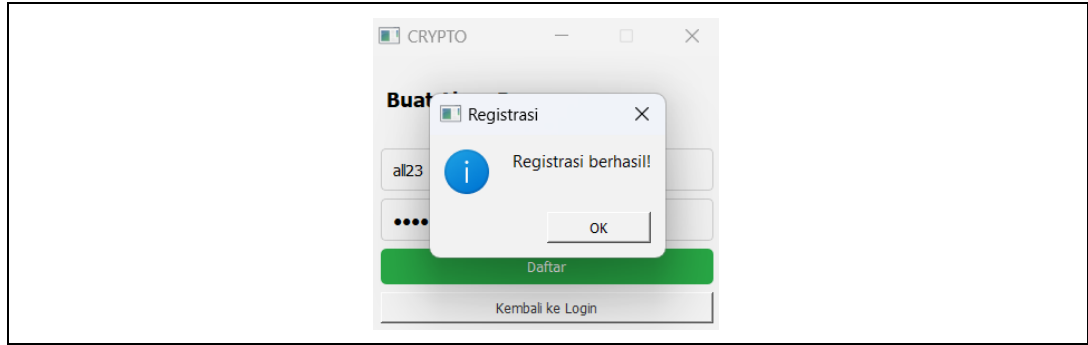
7. Hasil dan Pengujian

a. Pengujian 1: Registrasi

- **Input:** username dan password

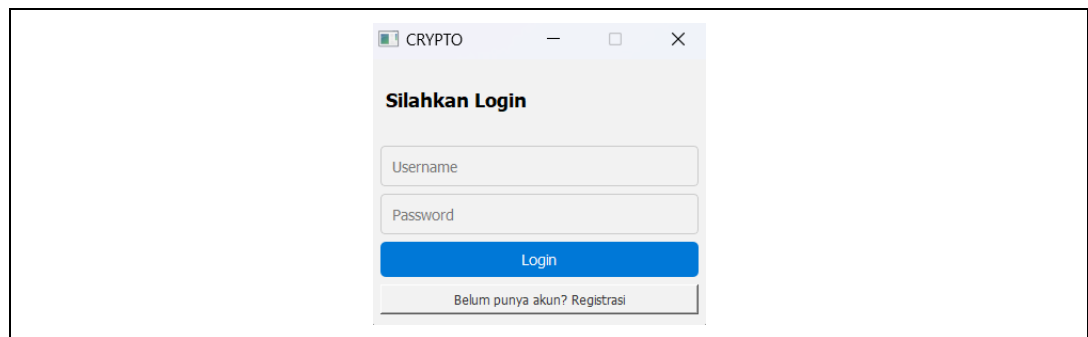


- **Output:** Registrasi berhasil, data disimpan di database dalam bentuk hash

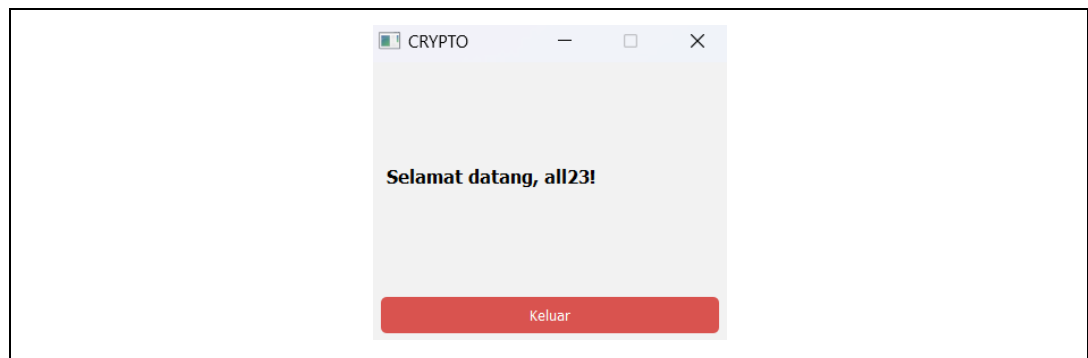


b. Pengujian 2: Login

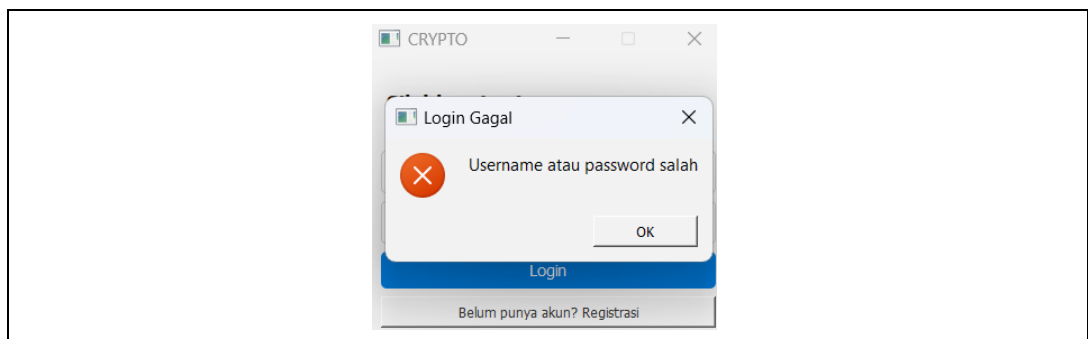
- **Input:** username dan password yang telah di registrasi sebelumnya



- Masuk ke halaman selamat datang

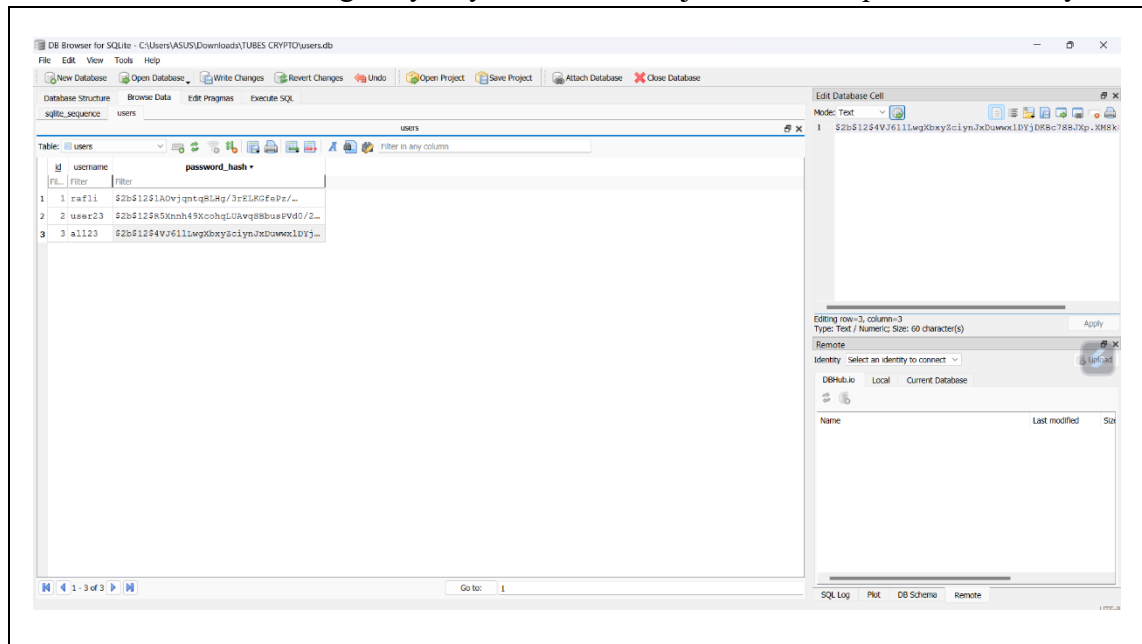


- **Input password salah** → muncul notifikasi gagal login



c. Hasil Hash di Database:

all23: \$2b\$12\$4VJ61lLwgXbxyZciynJxDuwwx1DYjDKBc7SBJXp.XMSk8OuFRyBsu



8. Kesimpulan

Sistem login yang dikembangkan dalam project ini telah berhasil diimplementasikan menggunakan Python dengan antarmuka pengguna modern berbasis PyQt5. Dalam sistem ini, teknik cryptography seperti hashing dan salting diterapkan menggunakan algoritma bcrypt untuk menjaga kerahasiaan data pengguna, khususnya dalam penyimpanan kata sandi. Kata sandi tidak disimpan dalam bentuk aslinya, melainkan dalam bentuk hash yang tidak dapat dikembalikan, sehingga lebih terlindungi dari ancaman seperti pencurian data atau serangan rainbow table. Pemanfaatan database SQLite juga mendukung penyimpanan data secara lokal dengan struktur tabel yang sederhana dan efisien. Fitur login dan registrasi berjalan lancar, serta mampu memberikan respons yang sesuai terhadap input pengguna. Dengan desain kode yang terstruktur dan tampilan yang mudah digunakan, sistem ini memiliki potensi untuk dikembangkan lebih lanjut, seperti dengan menambahkan fitur validasi password yang lebih kuat, pencatatan aktivitas pengguna, atau pembatasan percobaan login. Secara keseluruhan, sistem ini telah memenuhi kebutuhan dasar dalam hal keamanan dan fungsionalitas autentikasi pengguna.

DAFTAR PUSTAKA

<https://pypi.org/project/bcrypt/>

<https://docs.python.org/3/library/sqlite3.html>

<https://doc.qt.io/qtforpython/>

<https://id.wikipedia.org/wiki/Kriptografi>