



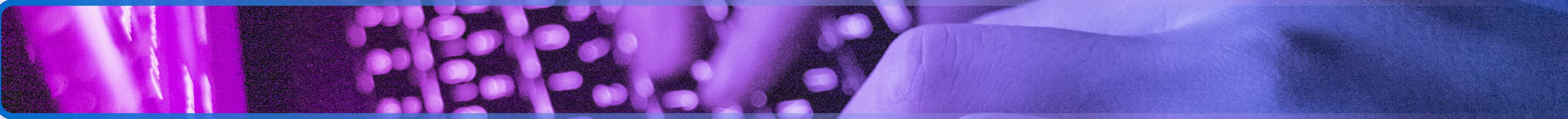
Kelompok 15

Perancangan

Sistem Digital



Anggota kelompok



Abyan Ammar
Zaki

Joshua Richardo
Riangkamang

Muhammad
Hashif Jade

Toriq Fathoni
Dezi



Latar Belakang Pemilihan Ide



Masalah Problem

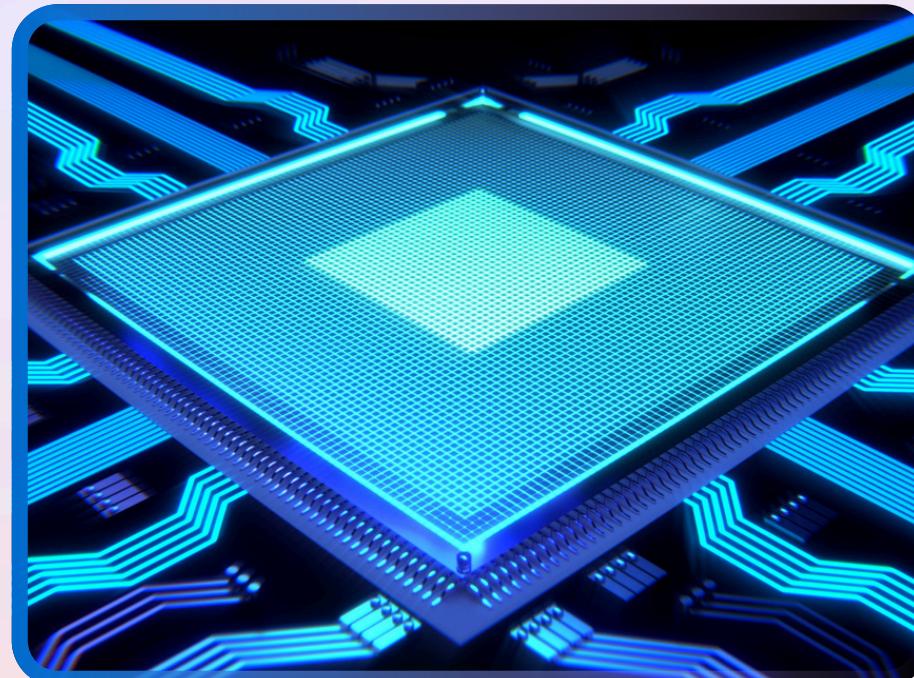


Masalah :

Kemajuan teknologi yang semakin pesat membuat keamanan perangkat konvensional lebih rentan dibobol karena AI dapat menganalisis pola dengan cepat.



Solusi Solution



● **Solusi :**

Meningkatkan keamanan dengan teknik hashing SHA-3 untuk penyimpanan password.

Algoritma enkripsi ini akan diimplementasikan di hardware.

Hashing ? SHA 3? Apa itu?

Hashing adalah proses mengubah data menjadi serangkaian karakter unik menggunakan fungsi hash yang menghasilkan nilai hash.

SHA merupakan singkatan dari Secure Hash Algorithm. SHA-3 merupakan salah satu jenis fungsi hash yang berfungsi untuk mengubah data agar keamanan data dapat terjaga.





Bagaimana Cara Kerjanya?

Pada prototype yang kami buat, password asli tidak disimpan sebagai plaintext, melainkan dalam bentuk hash SHA-3.

Cara kerjanya, sistem akan melakukan hashing terhadap input user dan membandingkannya dengan hash yang tersimpan secara hardcode. Jika password cocok, maka kunci akan terbuka, sedangkan jika berbeda, maka kunci tidak akan terbuka.





Detail Proyek



Spesifikasi Proyek

Prototype yang kami bangun didalam proyek ini mengimplementasi setidaknya 7 modul dari 8 modul yang telah dipelajari selama satu semester ini

Modul yang kami implementasikan diantaranya : modul 2, modul 3, modul 4, modul 5, modul 6, modul 7, modul 8



Modul 2 : Dataflow Style



Kecepatan

Berfungsi untuk efisiensi dan kecepatan pemrosesan program



Hardware

Berfungsi sebagai koneksi hardware antar modul

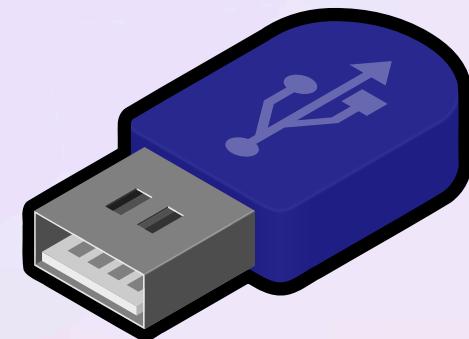


Penggabungan

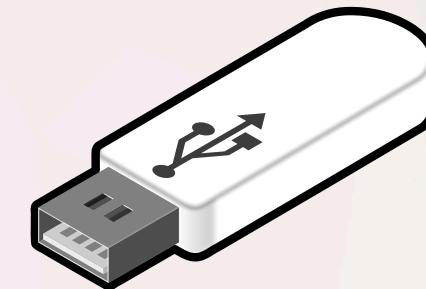
Berfungsi untuk menggabungkan PIN user dengan padding SHA3 secara paralel



Modul 3 : Behavioral Style



Berfungsi sebagai pengelola state SHA 3



Berfungsi sebagai control flow validation pada lock controller



Berdungsi sebagai sequential test scenario untuk program pada testbench



Proyek yang kami buat menggunakan testbench untuk memverifikasi kinerja dari proyek yang telah kami buat. Testbench yang kami buat dapat mengecek kedua kondisi yaitu kondisi dimana pin yang dimasukkan benar dan kondisi dimana pin yang dimasukkan salah.

Modul 4 Testbench



Modul 5 Structural Programming



Structural programming, dalam proyek ini, berfungsi sebagai pemisah antara SHA engine dan lock controller. Implementasi ini memudahkan kami dalam pembuatan dan penggerjaan proyeknya dengan kerjasama tim. Selain itu, pengimplementasian modul ini memudahkan jika ingin meng-upgrade logika SHA 3 menjadi SHA - 256 di kemudian hari dan membuat kode menjadi reusable.



Modul 6 Looping

Looping digunakan untuk mengacak password input dengan fungsi Theta (xor), Rho (memutar bit pada setiap blok untuk menyebarkan data). Dengan menggunakan proses looping, hasil akhir dari password input akan menjadi pola data yang jauh berbeda dari input aslinya.

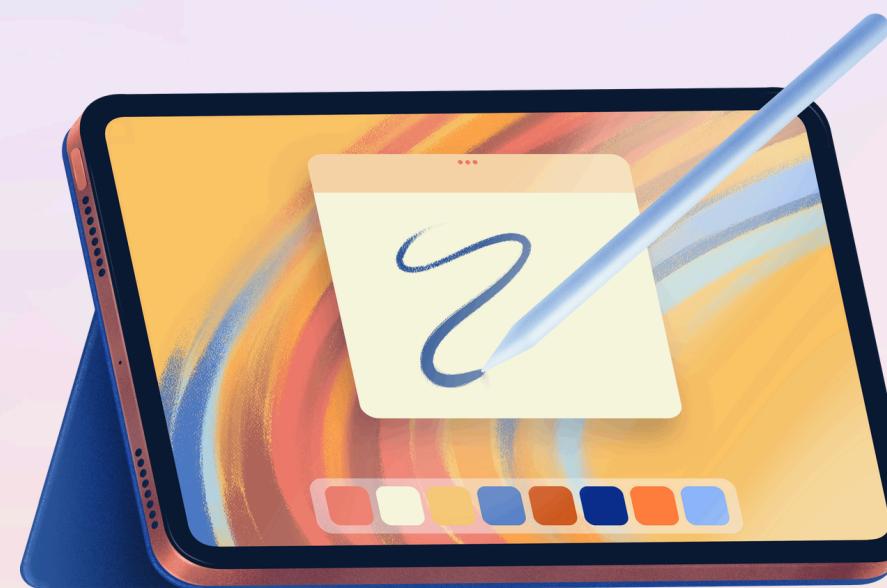


Modul 7

Function, Procedure, Impure Function

Implementasi

Proyek kami menggunakan Function untuk mempermudah operasi Bitwise Rotation pada algoritma Keccak pada modul *sha3_256_core.vhd*





Modul 8

FSM

FSM diimplementasikan untuk mengurutkan alur state pada algoritma Keccak





Thank You.
Thank You.
Thank You.