Security Lock System

Assembly Language Implementation in 8086

System Overview

Purpose

A comprehensive security authentication system designed to protect bank employee access through ID verification and password management.

Core Features

- Employee ID validation
- Password authentication
- Account lockout protection
- Password change capability

System Architecture

Data Segment

Stores employee IDs, passwords, and attempt counters for 20 employees

Stack Segment

Allocated 256 bytes (100h) for temporary data storage and subroutine calls

Code Segment

Contains main program logic, authentication routines, and helper procedures

Key Configuration Constants

20

Maximum Employees

System supports up to 20 employee accounts IDs

3

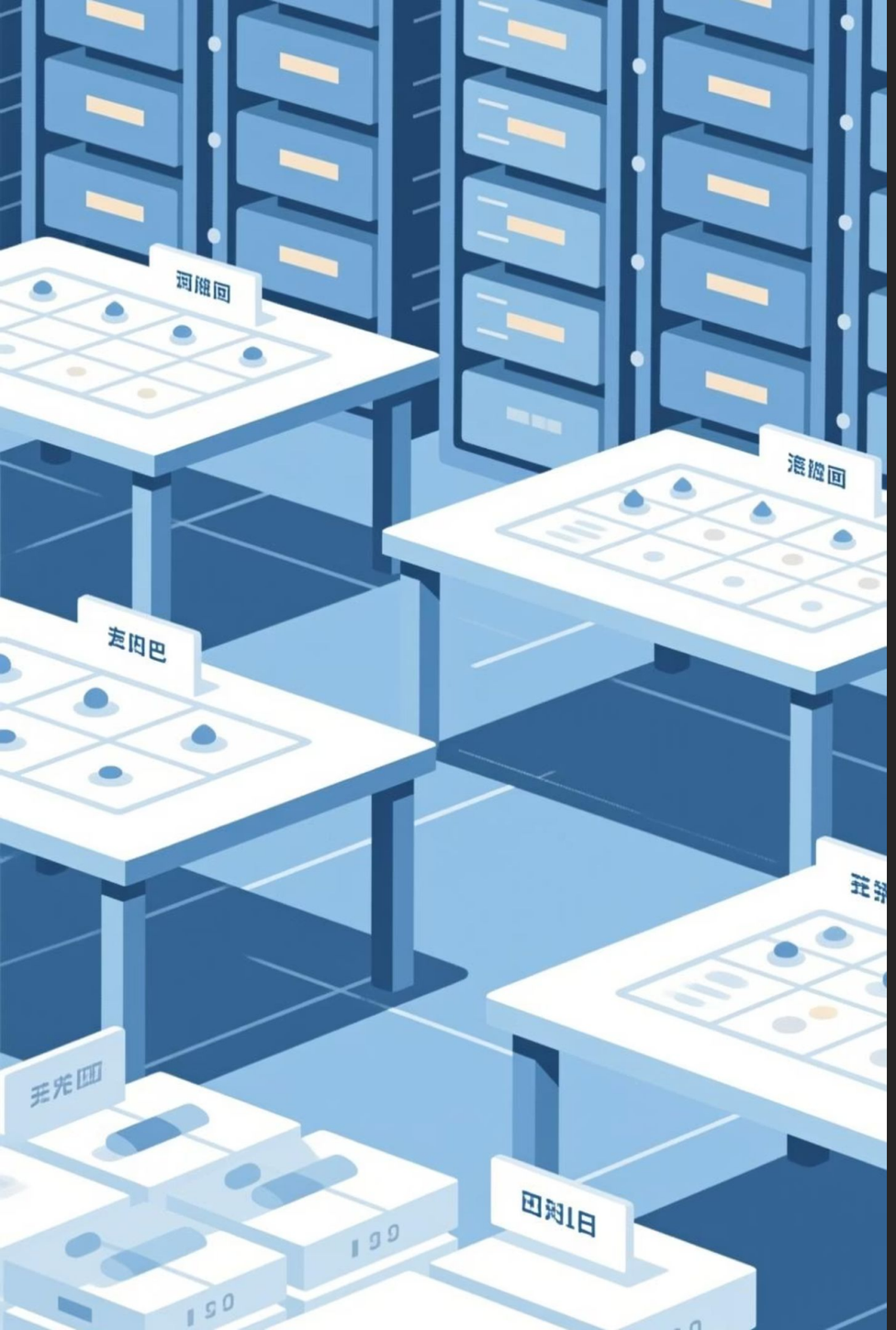
Login Attempts

Three failed password attempts trigger automatic account lockout

0-15

Password Range

Numeric passwords constrained to values between 0 and 15



Employee Data Structure

Employee ID Array

EmpTable stores 20 unique identifiers organized in three groups:

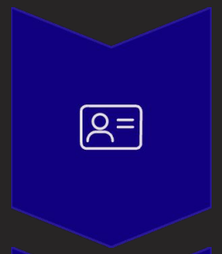
- 1001-1014: Department A
- 2001-2005: Department B
- 3001-3005: Department C

Password & Attempts

PassTable contains corresponding passwords (0-15) for each employee ID.

Attempts array tracks failed login counts, initialized to zero for all employees.

Authentication Flow

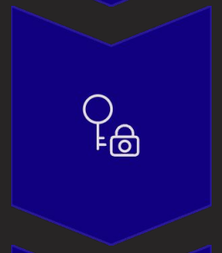


ID Verification

System prompts for employee ID and searches EmpTable using FindEmp procedure

Lockout Check

Validates current attempt count before allowing password entry

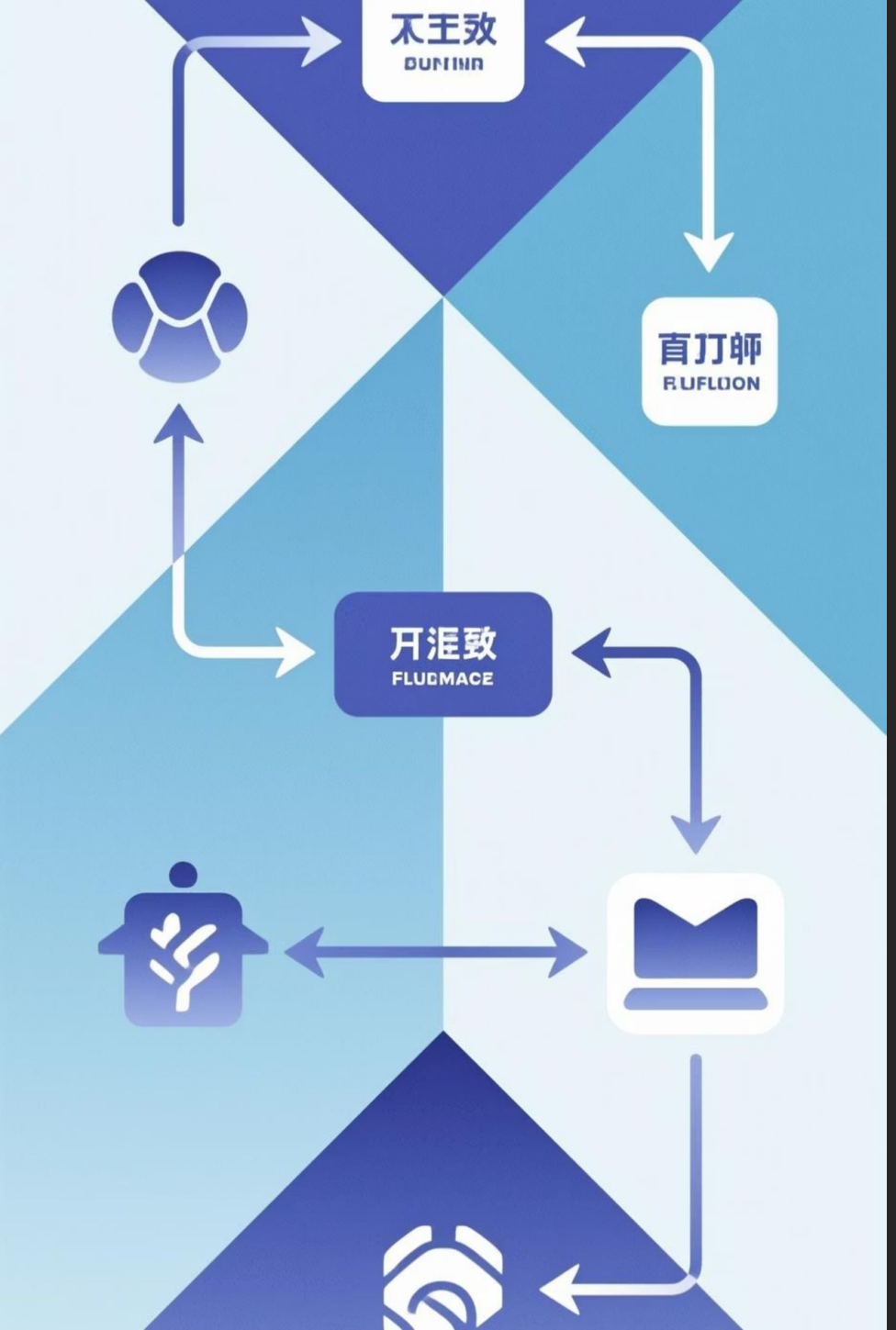


Password Validation

Compares entered password against PassTable entry for matched employee

Access Decision

Grants access on match, increments attempts on failure, locks after three attempts



Critical Procedures

1

SCAN_NUM

Reads numeric input from keyboard and converts ASCII characters to binary value stored in CX register.

2

FindEmp

Searches EmpTable array for matching ID. Returns employee index in BX register or sets zero flag if not found.

3

Main Loop

Continuously displays menu, processes authentication requests, and handles password change operations until program termination.

Security Features

Multi-Layer Protection

Attempt Tracking: Individual counter per employee prevents brute force attacks

Automatic Lockout: Account becomes inaccessible after three failed attempts

Attempt Reset: Successful login clears failed attempt counter to zero

Persistent Lock: Locked accounts require manual reset (not implemented in basic version)

Password Management

1

Post-Login Prompt

After successful authentication, system asks if user wants to change password

2

User Confirmation

Accepts 'Y' or 'y' input to proceed with password change operation

3

New Password Entry

Prompts for new password within valid range (0-15) using SCAN_NUM procedure

4

Update & Confirm

Replaces old password in PassTable and displays confirmation message

Implementation Highlights

Memory Efficiency

Compact data structures using byte arrays for passwords and word arrays for IDs minimize memory footprint.

DOS Integration

Leverages INT 21h BIOS interrupts for keyboard input (AH=01h) and display output (AH=09h).

Modular Design

Separate procedures for input scanning and employee lookup promote code reusability and maintainability.

Note: This assembly project demonstrates fundamental concepts including array manipulation, conditional branching, procedure calls, and interrupt handling in 8086 architecture.

Thank You

Presented by:

B. Kaivalya - AP23110011311

D. Gopika - AP23110011571

Y.L. Maheswari - AP23110011590

Ch. Himakshi - AP23110011596

P. Durga Sravanthi - AP23110011597