MPIN Validation Project Report

1. Introduction

This project aims to evaluate the strength of MPINs (Mobile Personal Identification Numbers) by identifying commonly used patterns and those derived from user demographics. It consists of five parts, each building upon the previous, to create a robust PIN validation framework.

2. Problem Statement

Many users choose MPINs that are guessable. These include:

- Commonly used numbers like 1234, 0000, or 1111
- Personal demographic combinations such as:
    - Date of Birth (DOB)
    - Wedding Anniversary
    - Spouse's DOB

This project attempts to detect such weaknesses and classify the MPINs as **WEAK** or **STRONG**.

3. Project Breakdown

Part	Description
A	Detects if a 4-digit MPIN is commonly used
B	Adds demographic-based validation for 4-digit MPINs
C	Enhances Part B to provide detailed **reasons** for weakness
D	Extends validation to **6-digit MPINs**
E	A **test suite** with 20+ test cases covering all edge and normal cases

4. Key Features

- Detection of patterns (sequential, repeated, palindromes, etc.)
- User demographic pattern extraction (DOB, anniversary, spouse DOB)
- Full explanation for why a PIN is weak
- Support for both 4-digit and 6-digit MPINs
- Unit testing with unittest to ensure functionality

5. Tools Used

- Python 3.x
- Colab Notebooks
- unittest for test coverage

6. Learning Outcomes

- Applied **pattern recognition** logic
- Integrated **real-life user behavior** into algorithm design
- Practiced writing **modular**, **scalable**, and **testable** Python code
- Understood the importance of **user education** in cybersecurity

7. Conclusion

This project simulates a real-world FinTech scenario, where user PINs need to be verified for security. By adding layers of validation and explanation, the solution not only detects weak MPINs but educates users about **why** they are weak.