

Project Name:

Phone Unlock Using Pattern Predictor

Members:

Naghul Varshan N

Sahith M

Yamuna Shri vardhini T V

Procedure:

This Python program generates a random, valid phone unlock pattern just like the one you use on an Android 3×3 lock screen.

It follows the same rules your phone uses — you can't skip over a dot unless you've already touched it, and you can't revisit a dot that's already part of the pattern.

Step-by-Step explanation:

Importing Libraries

NumPy: Helps store and handle the (x, y) positions of each dot on the screen.

Matplotlib: Used to draw the grid and visually connect the dots.

Random: Chooses random valid moves to form the pattern.

Defining Jump Rules (jumps dictionary)

Some moves require an “in-between” dot to be used first.

For example, moving from 0 to 2 directly requires dot 1 to be already part of the pattern.

Checking Valid Moves (is_valid_move)

Makes sure the next dot:

Hasn't been used before.

Doesn't break the jump rules.

Generating a Pattern (generate_random_pattern)

Starts from a random dot.

Adds valid next moves until the desired pattern length is reached or no moves are possible.

Drawing the Pattern (draw_pattern)

Place dots in a 3×3 grid.

Colors the dots light gray, numbers them, and draws red lines between them in the order they're touched.

The starting dot is highlighted in green.

Execution

A pattern of length 5 is created.

The program prints the sequence of dots and displays the pattern visually.

How It Is Used:

This tool can be applied in:

Security research – Simulating and testing different unlock patterns.

UI design – Building gesture-based authentication systems.

Data generation – Creating datasets for AI models that learn and predict patterns.

It ensures that every pattern follows the same restrictions as an actual Android lock screen.

Conclusion:

This code successfully produces and displays realistic, valid unlock patterns for a 3×3 Android grid.

By respecting Android's rules, it becomes a useful resource for education, security research, and user interface development.

It can even be extended into a pattern prediction model for deeper security analysis.