

A blue parallelogram and a light green parallelogram are positioned on the left side of the slide, overlapping each other and the dark background. The blue shape is on the left, and the green shape is to its right, partially overlapping it.

# Obfuscation: Week Two

Caleb Parten and Carlo Velarde



# Overview

- Testing different obfuscation methods
- Analysis
- New prompting

# Testing Obfuscation Methods

- Dead code obfuscation
- Naming obfuscation
- What did we test for?
  - Equality
  - Correct implementation

```
let name = "carlo"  
console.log(name)
```

obfuscation

Fail

```
let 01_2zd = "carlo"  
console.log(name)
```

```
let name = "Carlo"  
console.log(name)
```

obfuscation

Success

```
function foo(name){  
  return name + "  
  Velarde"};  
  
let name = "Carlo"  
foo(name)  
  
console.log(name)
```



# Testing Parameters

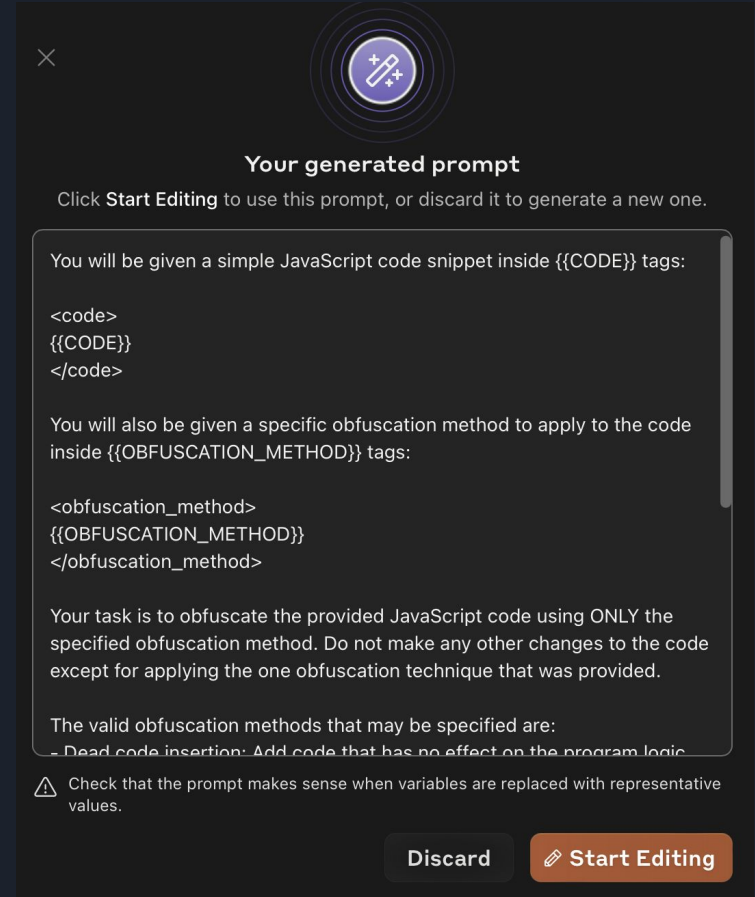
- Equality
  - Should compile and output
  - Output must be direct match
- Correct implementation
  - Must use specified obfuscation method
  - Mixing obfuscation methods == False
  - Output can be off
- Successful obfuscation
  - True for equality AND True for implementation

# Completed Table

obfuscate output	obfuscation type	equal	implemented obfuscation
Area of circle: 78.53981633974483	Dead Code Obfuscation	FALSE	TRUE
10 kilometers is 6.21371 miles	Dead Code Obfuscation	TRUE	TRUE
Error: Command '['node', '-e', 'const str	Dead Code Obfuscation	FALSE	TRUE
Error: Command '['node', '-e', 'const str	Dead Code Obfuscation	FALSE	TRUE
Error: Command '['node', '-e', 'const str	Dead Code Obfuscation	FALSE	FALSE
Square root: 4	Dead Code Obfuscation	FALSE	FALSE
Error: Command '['node', '-e', 'const per	Dead Code Obfuscation	FALSE	TRUE
Current date and time: Tue Jun 11 2024	Dead Code Obfuscation	FALSE	TRUE
Maximum: 10	Dead Code Obfuscation	TRUE	FALSE
10 kilometers is 6.21371 miles	Dead Code Obfuscation	TRUE	TRUE
Hypotenuse: 5	Dead Code Obfuscation	TRUE	TRUE
Fixed number: 3.14	Dead Code Obfuscation	TRUE	TRUE
First character: J	Dead Code Obfuscation	TRUE	TRUE
Perimeter of rectangle: 30	Dead Code Obfuscation	TRUE	TRUE

# Anthropic Prompting

- Anthropic is by the company of Claude 3
- Allows for advanced prompting
- Gives LLMs best chance of success





# Analysis

Out of 373 JavaScript snippets:

- Correct implementation:
  - 248 passed and 125 failed.
- Correct output:
  - 221 passed and 152 failed.
- Correct output & implementation:
  - 155 passed and 218 failed.
- Correct output but failed implementation:
  - 66 passed
- Wrong output but correct implementation:
  - 93 passed



# Findings

- Output and implementation
  - More failed
- More accuracy with naming obfuscation
- Occasionally mixed obfuscation methods