Teacher Guide - Modulo Clock Thought Experiment

Thought Experiment - Clock as a one-way function

Any kind of encryption requires transforming information in a way that is hard to reverse without a key.

A “one-way function” is a math operation that is impossible to reverse or solve even if you know some of the inputs that went into it. But it’s not random. GIven the same inputs, it will produce the same result. There is just no way to reverse the process.

As an example, let’s do a thought experiment:

> *Imagine that you are a person who loses complete track of time when you close your eyes. When you open your eyes, a minute could have passed or an hour…or a day…or a week…or a year…you don’t know.*
>
> *So, now imagine a clock that reads 4:00.*

Show a clock of some kind that shows 4:00; here is an interactive one.

> *Now close your eyes and I’m going to add some time to the clock - I’m going to simulate that some amount of time is passing. Remember, with your eyes closed, any amount of time could be going by.*

Set the clock to show 3:00.

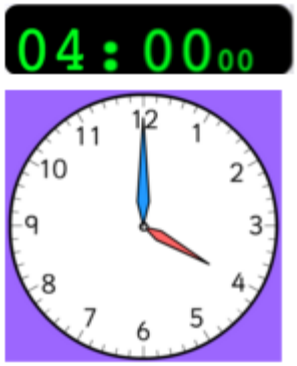
> *Now open your eyes, look at the clock and, without saying anything to anyone, write down how much time has passed.*

Wait a few seconds for students to write.

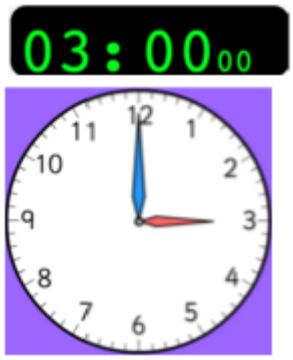
Prompt: So, how much time passed? What are the possibilities?

Let students share answers:

- There are an infinite number of possibilities, including: 11, 23, 35, 47 hours, etc. Or 1 day and 11 hours, and so on.
- If students want to know what you were thinking, make up something that no one has said yet, something like, “Oh, I was actually imagining that I was adding 13 years, 47 days and 11 hours.”



BEFORE: clock is showing 4:00.



AFTER: clock is showing 3:00.

Takeaway: Clock is a one-way function
There is no way to know the original input just from looking at the face of the clock. No matter what number you put into it, only numbers 1-12 can show afterward. Even if the number is 2,023,789 hours, if you wind the clock around, it will still come out as a number 1-12. We cannot know what the original number was that went into the clock.

Clock is a metaphor for modulo

Real cryptography uses this “clock” technique to obscure information, but with clocks that can have a wide range of possible values on their faces. **The operation is called modulo.** Modulo is a math operation that returns the *remainder* from dividing two integers. It is important for cryptography because it can act as a one-way function - the output obscures the input.

More points about the modulo operation can be found in the lesson plan.