Functions that Generate a Few Values Easy to Predict

Now we can think about cryptography.

If I tell you H(x) = 123, can you tell me x?

It’s not obvious

- how to invert the function
- (not too hard for an expert,
- but not obvious to most people).

But **H(x) has only 256 values**, so one can use a computer to guess and check pretty quickly.