Parameter Values are Keys to Cryptographic Locks

Think of the values as parameters
and define a class of functions:

$$\mathbf{PRNG_{M,A,D}(x) = floor\ [\ (M\ x + A)\ /\ D\ ]\ mod\ 256}$$

Parametric functions (NOT the one above)

- **can be designed** in **such** a way
- **that one can only invert** the function
- **IF one knows the** values of the **parameters**.

One can thus think of these values

- as **the "key" to a cryptographic lock**
- implemented by the function.