Example: Encrypting a Document with a Key

Let's say that you have **a document D** (a bunch of bits) that you want **to keep secret**.

You **create a "key,"**

- which defines a specific function, and
- **apply** that function **to the bits in D to produce** another bunch of bits, **E**.
- E looks like random bits.
- Then you throw away D (don't lose the key!).