A cryptosystem is **unconditionally secure** if it cannot be broken, even with infinite computational resources. (There are other (weaker) types of security; we’ll talk about those later.)

A cryptosystem is unconditionally secure against a ciphertext-only attack if the ciphertext does not give any information about the plaintext (except its length). This is known as **perfect secrecy**.
One-time Pad

- plaintext: a binary string of length \( n \)
- key: a sequence of random bits of length \( n \)
- encryption: exclusive-OR of the plaintext and the key

- how to decrypt?
  \[ \text{XOR w. the key} \]
One-time Pad

- perfect secrecy? **YES**
  - if each bit of the key chosen independently, with 0/1 chosen with probability $\frac{1}{2}$

- encryption/decryption: [easy](#) hard?

- why not a standard cryptosystem?
  - requires a very large key that cannot be reused

Note: no perfect secrecy with shorter keys
Visual Cryptography

- a cool application of the one-time pad

- plaintext: each bit is represented as a pixel:
  0=black, 1=transparent

- key and ciphertext: each bit is represented by two subpixels:
  0=black/transparent, 1=transparent/black

- how to decrypt?
  put me on top of the other