Pseudo Random Functions

"If I had unlimited randomness...."

Imagine a large table: for every website in universe, I write down a randomly chosen password

Use a PRF: choose random λ-bit <u>seed</u> k

password for google.com is $F(k, \text{"google.com"})$

(only need to remember k)

Imagine Alice & Bob share HUGE database of OTP keys

Alice $\{m\}$ $\xrightarrow{\text{"I'm going to encrypt using OTP key @ position } i\text{"}}$ Bob

Using PRF, A & B share seed $\underline{k}$

$\xrightarrow{\text{I'm going to encrypt using PRF output @ } i}$

$F(k,i) \oplus m$

sneak preview of Chapter 8

---

example 6.2

even if G is secure PRG

$$F(k,x) = G(k) \oplus x$$

is <u>not</u> a secure PRF

Need to distinguish:

```
k ← {0,1}^λ

QUERY(x):
  ret G(k) ⊕ x
```

$\underbrace{G(k) \oplus x}_{F(k,x)}$

```
T = empty

QUERY(x):
  if T[x] undef
    T[x] ← {0,1}^out
  return T[x]
```

Obs: call QUERY on distinct inputs ⇒ get independent, random, unrelated outputs

⇒ should call QUERY on 2 things at least

```
A:
  z1 = QUERY(00··)
  z2 = QUERY(11···)
  ???
```

⇓ run this in presence of left library

```
A:
  z1 = QUERY(00··)
  //   = G(k) ⊕ 000··· = G(k)
  z2 = QUERY(11···)
  //   = G(k) ⊕ 111··· = ‾G(k)‾
  if z1 = ‾z2‾  return 1
        else    return 0
```

In presence of left library,

$\Pr[\text{out } 1] = 1$

In presence of right library,

z_1, z_2 uniform, indep.

$\Pr[\text{out } 1] = \frac{1}{2^{\text{output length}}}$

⇒ Advantage of A: $1 - \frac{1}{2^{\text{out length}}}$

not negligible ⇒ libraries are distinguishable

⇒ F not secure PRF