Exam Review

HW3 due today, exam Monday

Exam structure:

- Some short answer (understand classic constructions)
- ~4 problems similar to HW (smaller in scope)
  ex: proof?, attack

Shamir SSS:

t-out-of-n

Dealer: secret $m \in \mathbb{Z}_p = \{0, \dots, p-1\}$

choose poly of deg $t-1$

$$f(x) = \underset{\underset{m}{\parallel}}{f_0} + \underline{f_1} x + \underline{f_2} x^2 + \cdots \underline{f_{t-1}} x^{t-1}$$

chosen uniformly from $\mathbb{Z}_p$

give $f(1)$ to user 1
$f(2)$ to user 2
⋮

Reconstruct: given $(i, f(i))$ for <u>any</u> t users can recover f, hence $f(0) = \underline{m}$

PRG:

$$G : \{0,1\}^\lambda \longrightarrow \{0,1\}^{\lambda + \ell}$$

PRF:

Given k, PRF defines exponentially large pseudorandom string

PRF gives random access to string

OR: for k chosen uniformly, PRF(k, *) looks like $R : \{0,1\}^{in} \to \{0,1\}^{out}$ chosen randomly

CPA attack:

insecure

```
Enc(k, m):
    $r \leftarrow \{0,1\}^\lambda$
    $x = F(k, r)$
    $y = F(k, r) \oplus m$
    return $(x, y)$
```

Secure!

```
    ⋮
    return $(r, y)$
```

Attack: (CPA)

choose $m_L \neq m_R$ arbitrarily

$(x, y) = \text{CHALLENGE}(m_L, m_R)$

return $y \oplus m_L \overset{?}{=} x$

in left world

$x = F(k, r)$

$y = F(k, r) \oplus m_L$

$y \oplus m_L = F(k, r)$

$= x$

$\Rightarrow$ Always says true

Right world

$x = F(k, r)$

$y = F(k, r) \oplus m_R$

$$y \oplus m_L = \underbrace{F(k, r) \oplus \underbrace{m_R \oplus m_L}_{\neq 0}}_{\neq F(k, r)}$$

$\Rightarrow$ Always says false