One-Time Pad etc

Welcome to CS 427

Encryption scheme consists of 3 algorithms:

- KeyGen : outputs a key k
- Enc(k, m) : outputs a ciphertext c (ctxt)
  - plaintext (ptxt)
- Dec(k, c) : outputs plaintext

$\mathcal{K}$ = key space

$\mathcal{C}$ = ciphertext space

$\mathcal{M}$ = ptxt space

Correctness property:

$$\forall\, m \in \mathcal{M},\ k \in \mathcal{K} \ : \quad \text{Dec}(k, \text{Enc}(k, m)) = m$$

"correctness" = something that doesn't involve Adversaries

"security" = " " does " "

One-time Pad (1882):

- $\mathcal{K} = \mathcal{C} = \mathcal{M} = \underbrace{\{0,1\}}_{\text{set of } \lambda\text{-bit strings}}{}^{\lambda}$ ~ lambda = length of a key
- KeyGen: choose $\boxed{k \leftarrow \{0,1\}^\lambda}$ uniformly at random
- Enc$(k, m) = k \oplus m$
- Dec$(k, c) = k \oplus c$

XOR (addition mod 2)

$0 \oplus 0 = 0$

$0 \oplus 1 = 1$

$1 \oplus 0 = 1$

$1 \oplus 1 = 0$

Correctness:

$$\begin{array}{rl} m = & 011010 \\ \oplus\ k = & 010101 \\ \hline Enc(k,m) = c = & 001111 \\ \oplus\ k = & 010101 \\ \hline = Dec(k,c) = & 011010 \end{array}$$

$$\begin{aligned} Dec(k, Enc(k,m)) &\stackrel{?}{=} m \\ &= Dec(k,\ k \oplus m) \\ &= k \oplus (k \oplus m) \\ &= (k \oplus k) \oplus m \\ &= 00\cdots00 \oplus m \\ &= m \end{aligned}$$

Talk about security

goal: protect against an Adversary who

... sees ctxt

... doesn't know key

... ~~shouldn't learn~~ ptxt should learn no info about ptxt

what about an Adv who learns partial info about ptxt?

e.g.: learns the 1st bit of ptxt

learns whether ptxt is encoding of prime #

Formal Definition (take 1):

Idea: Adv sees ctxt, which is a sample from some distribution

more specifically, a sample from

$$\boxed{\begin{array}{l} \underline{mydist(m):} \\ \quad k \leftarrow \{0,1\}^\lambda \\ \quad \text{return } k \oplus m \end{array}}$$

Claim: $\forall m \in \mathcal{M}$, $\underbrace{mydist(m)}_{\text{a probability distribution}}$ is the uniform distribution on $\{0,1\}^\lambda$

Pf: Uniform dist. assigns prob. $1/2^\lambda$ to each outcome $c \in \{0,1\}^\lambda$

pick arbitrary $m, c \in \{0,1\}^\lambda$, then it suffices to show $\Pr[\text{mydist}(m) = c] = 1/2^\lambda$

$$\text{mydist}(m) = c \iff k \oplus m = c \qquad m, c \text{ fixed}$$
$$\iff k = m \oplus c$$

i.e, there is unique k that causes $\text{mydist}(m) = c$ but k chosen uniformly, so this particular $k = m \oplus c$ chosen w/prob. $1/2^\lambda$ $\blacksquare$

Formal Def (take 2):

Idea: Define 2 libraries, same interface

```
Query(m):
    k <- {0,1}^λ
    return k ⊕ m
```

$\mathcal{L}_{otp\text{-}real}$

```
Query(m):
    c <- {0,1}^λ
    return c
```

$\mathcal{L}_{otp\text{-}rand}$

Adv is an arbitrary calling program

Claim: $\forall A$ (adversary)

$$\Pr[\underbrace{A \diamond \mathcal{L}_{otp\text{-}real}}_{\text{"A linked to this library"}} \Rightarrow 1] = \Pr[A \diamond \mathcal{L}_{otp\text{-}rand} \Rightarrow 1]$$