Pseudorandom Functions and Permutations

Pseudorandom Functions (PRF) defined over (K, X, Y)

$$F: K \times X \to Y$$

s.t. "eff" algo exists to eval $F(k, x)$

Pseudorandom Permutation (PRP) defined over (K, X):

$$E: K \times X \to X$$

s.t. 1. "eff" algo exists to eval $E(k, x)$

2. $E(k, \cdot)$ is one-to-one

3. Exists "eff" inversion algo $D(k, x)$

Same as block cipher

Ex. AES128: $K \times X \to X$ where $k = x = \{0,1\}^{128}$

DES: $K \times X \to X$ where $X = \{0,1\}^{64}$, $K = \{0,1\}^{56}$

3DES: $K \times X \to X$ where $X = \{0,1\}^{64}$, $K = \{0,1\}^{168}$

PRP $\subseteq$ PRF; a PRP is a PRF where $X = Y$ and is efficiently invertible

Secure PRFs

Let $F: K \times X \to Y$ be PRF

→ Let Funs$[X, Y]$: set of all functions from X to Y

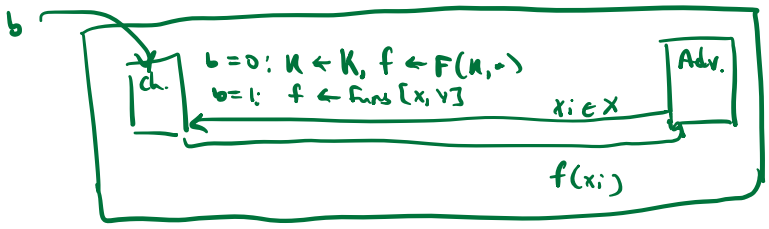
→ Let $S_F = \{F(k, \cdot) \text{ s.t. } k \in K\} \subseteq \text{Funs}(X, Y)$

Intuition: PRF is secure if

→ random fn in Funs$[X, Y]$ is indistinguishable from random fn in S_F

Formally!

For $b = 0, 1$ define $EXP(b)$ as



Def. F is a secure PRF if for all "eff" A:

$$Adv_{PRF}[A, F] = |Pr[EXP(0) = 1] - Pr[EXP(1) = 1]|$$

is negligible.

Ex. Let $K = X = \{0,1\}^n$

Consider: $F(k, x) = k \oplus x$ over (K, X, X)

$F(x)$ is insecure! Why:

Adversary A: 1. Choose arbitrary $x_0 \neq x_1 \in X$
2. query for $y_0 = f(x_0)$ and $y_1 = f(x_1)$
3. Output '0' if $y_0 \oplus y_1 = x_0 \oplus x_1$, else '1'

2-time pad attack

$Pr[EXP(0) = 0] = 1$

$Pr[EXP(1) = 0] = 1/2^n$

$\Rightarrow Adv_{PRF}[A, F] = 1 - \frac{1}{2^n}$ (not negligible)

Secure PRP: Same, except replace $Funs[X, Y]$ w/ $Perms[X]$

all permutations over X

Ex AES, 3DES, ...

AES256 PRP assumption:

For all A s.t. time(A) $< 2^{80}$: $Adv_{PRP}[A, AES256] < 2^{-40}$

Any Secure PRP is also a secure PRF

PRP-PRF switching lemma:

Let E be PRP over (K, X)

Then for any q-query adversary A:

$$|Adv_{PRF}[A,E] - Adv_{PRP}[A,E]| < q^2/2|X|$$

$|X|$ very large: $Adv_{PRP}[A,E]$ negligible $\Rightarrow$ $Adv_{PRF}[A,E]$ negligible

Using PRPs and PRFs

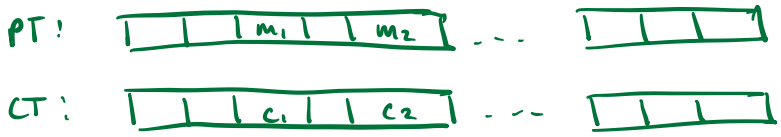
Goal: build "secure" encryption from a PRP

Security parameters:

1. What "power" does adversary have?
   - → sees one CT (one-time key)
   - → sees many PT|CT pairs (many-time key, CPA)
2. What "goal" is adv trying to achieve?
   - → fully decrypt challenge ciphertext
   - → learn none about PT from CT (semantic security)

Incorrect use of a PRP

Electronic Codebook (ECB)



Problem:

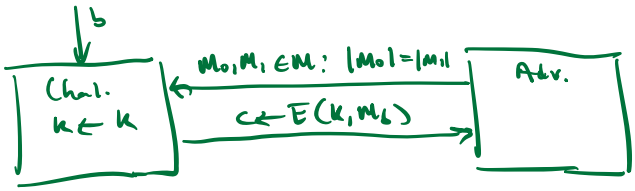
- If $m_1 = m_2$ then $c_1 = c_2$; can recover info about PT from this (i.e. length of words in sentence)

Model of operation for one-time use key

ex. encrypted email

$\mathcal{E} = (E, D)$: cipher defined over $(\mathcal{K}, \mathcal{M}, \mathcal{C})$

For $b = 0, 1$ define $EXP(b)$ as



Def. $\mathcal{E}$ is sem. sec. for one-time key if for all eff. A

$$Adv_{SS}[A, \mathcal{E}] = \left| Pr[EXP(0) = 1] - Pr[EXP(1) = 1] \right|$$

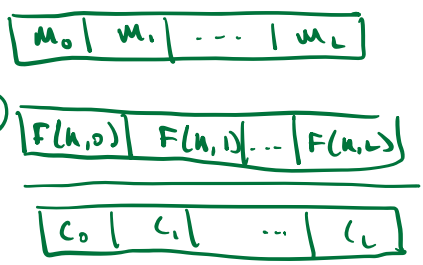
is negligible

$\Rightarrow$ No efficient adversary learns info about PT from single CT

Examples of sem. sec. systems

1. $Adv_{SS}[A, OTP] = 0$ for all A
2. Deterministic counter mode from a PRF F

$\rightarrow E_{DETCTR}(k, m) =$



Stream cipher built from PRF (e.g. AES)