PRPs & Chosen Plaintext Attacks

Monday, September 13, 2021 3:56 PM

Pseudorandom Permutations

- PRF: $F_2: K \times D \to C$

- PRP is a PRF that's also a permutation : $F_2: K \times D \to D$

  $\forall x.\ F^{-1}(k, F(k,x)) = x$

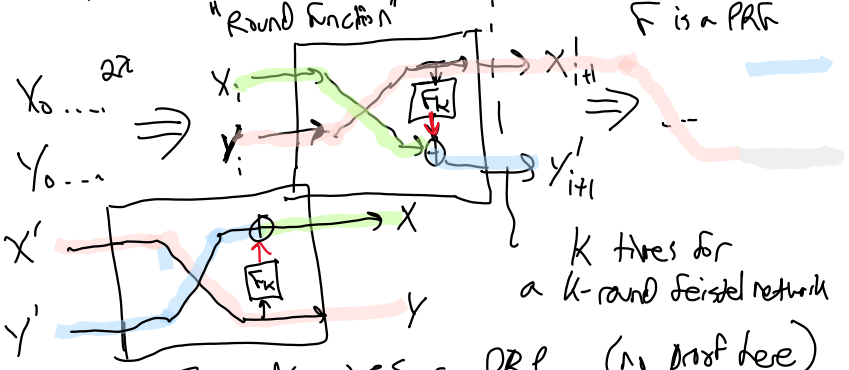
Enc: 

Dec: 

Feistel Network: Any PRF to a PRF

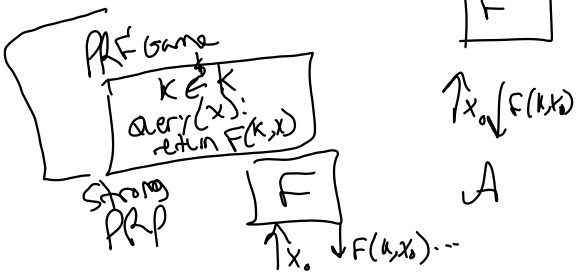
"Round function"

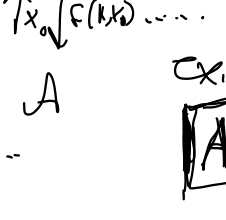
F is a PRF



k times for a k-round feistel network

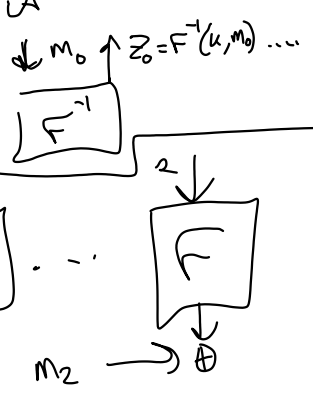
- 3 rounds gives a PRP (no proof here)
- 4 rounds gives a ~~strong~~ PRP





Ex. of PRP

128 b.t., 256-bit ... ?



Chosen Plaintext Attacks

Multimessage security

k — "All $m_1 \dots m_q$ chosen up front"

Alice $m_1, m_2 \dots$ — $c_1, c_2 \dots$ → Bob $m_1', m_2' \dots$

$c_1 \dots$

$\mathcal{A}$

$\forall m_L', m_R'$
m_L^2, m_R^2
$\vdots$
$m_L^{q(\lambda)}, m_R^{q(\lambda)}$

$k \xleftarrow{\$} Gen()$
for $i \in 1 \dots q(\lambda)$:
  $Enc(k, m_L^i)$
  $\dots$

$\approx$

$\dots$
$Enc(k, m_R)$

0 0
0 1

Alice $m_1, m_2 \dots$ — $c_1 \dots c_i$ → Bob

$\mathcal{A}$

"m_{i+1} might depend on $c_1, \dots c_i$"

IND-CPA — "indistinguishability under chosen plaintext"

Left side

$c_L^1 \dots c_L^i$

m_L^{i+1}, m_R^{i+1} — $\mathcal{A}$

$\forall \mathcal{A}$.

O_L:
$k \xleftarrow{\$} Gen()$
Query(m_L, m_R):
return $c = Enc(k, m_L)$

$\approx$

O_R $k \leftarrow Gen$
Query(m_L, m_R):
return $c = Enc(k, m_R)$

$\mathcal{A}^{O_L.query} \approx \mathcal{A}^{O_R.query}$

Alternate equivalent defn's

Phase 1. $\mathcal{A}$ chooses $m_1, \ldots m_q$ and learns $c_1, \ldots c_q$

Phase 2. $\mathcal{A}$ chooses a pair of m_L, m_R and receives c_L or c_R and has to guess which

---

Q for next time:

Give a multimessage secure Enc scheme that is NOT CPA-secure.

Real vs Random multimessage:

$k \leftarrow Gen()$

$Query(m_1, \ldots m_q)$:

// $Enc(k, m_i)$

$\approx$

$k \leftarrow Gen()$

$Query(m_1, \ldots m_q)$:

// $m_i \xleftarrow{\$} M$

$Enc(k, m_i)$