Story So Far:

Shannon's Pessimistic Thm

- Symmetric Key Crypto (Key Predetermined)
- Public Key Crypto (from scratch)

Sym. Key Crypto: → Ciphertext only attack

→ PRG based soln. $c := G(k) \oplus m$

→ PRG defn: $|P(A(G(U_n))=1) - P(A(U_{l(n)})=1)| \leq \text{negl}(n)$

→ PRG Construction: Heuristic (RC4)

Provably Secure (from 1-way permutation)

Candidate " " : DLP

→ Hard core predicate of 1-way fn.:

* PPTM A, $P[A(f(x)) = h(x)] \leq \frac{1}{2} + \text{negl}(n)$

→ MSB ($\log_g y \leq \frac{p-1}{2}$?) is a hardcore predicate for DLP

$DLP \leq_p$ MSB DLP

↳ Karp Reduction

- Need for Probabilistic Enc: No deterministic enc. scheme is CPA secure.
- CPA security defn: Oracle access to enc server
- PRF based soln.
- Defining PRF_D
- ∃ PRF ⇔ ∃ PRG
  - $F_k(x_0 x_1 .. x_{n-1}) = G_{x_{n-1}}(\cdots G_{x_1}(G_{x_0}(k))..)$
- CPA secure Enc $c := \langle r, F_k(r) \oplus m \rangle$

- Other modes of operation:

  CBC : $c_i := F_k(c_{i-1} \oplus m_i)$

  OFB : $r_i = F_k^{(i)}(r_0)$

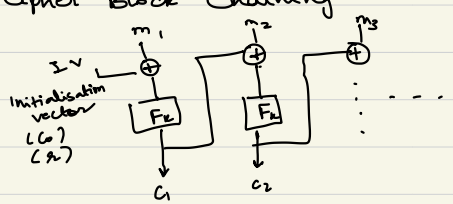
  Randomised counter : $r_i = F_k(r + i)$

- Malleability
- CCA Security: Oracle access to dec server
- MACS - defn
- CPA Security + MAC = CCA Security

CBCMAC:

$m_1, m_2 \cdots m_t$ are t blocks of messages with each block of length n, i.e $|m_i| = n$. $F_k: \{0,1\}^n \to \{0,1\}^n$ is a PRF.

Cipher Block Chaining:



$c := \langle c_1, c_2 \ldots c_t \rangle$

Not length doubling, total payload (ciphertext + IV) is $nt + n$

For an n bit message m, $F_{k_2}(m) = \sigma$ is a valid MAC

↳ mac key

Attempt 1:

For a longer message, divide into blocks, do CBC & $MAC_k(m_1 .. m_t) = c_t$

→ does not allow variable length queries

2^{nt} 2^n

Break:

$|m_0| = n$, $\sigma_0 = F_k(m_0)$

$|m_1| = 2n$, $\sigma_1 = F_k(c_{10} \oplus m_{11})$

$\hookrightarrow m_{10} . m_{11}$ $\quad = F_k(F_k(m_{10}) \oplus m_{11})$

$|m| = n$.

If $m_{11} = F_k(m_{10}) \oplus m$

where $m_{10} = m_0$,

$m_{11} = F_k(m_0) \oplus m = \sigma_0$

$\sigma_1 = F_k(\sigma_0 \oplus \sigma_0 \oplus m)$

$\sigma_1 = F_k(m)$

Fix 1: $k' = F_k(l)$

C_t using k': each message length has a different key

Fix 2: Prepend length: $m = m_1 \ldots m_t$

$m' = l\, m_1 \ldots m_k$

Fix 3: Use 2 keys k_1, k_2

Used for C_t ↙ $\quad$ ↘ $\sigma = F_{k_2}(C_t)$