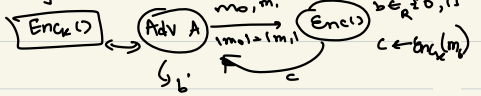
Review:

- No deterministic encryption scheme is CPA secure
- Need for probabilistic encryption
- CPA security:



One time Pad is CPA secure.

Consider the scheme $G(k) \oplus m$ which is not CPA secure, to make it CPA secure, either i) use different key everytime (needs secure channel)

ii) Create a very large $G(k)$ & use diff. bits of key to mimic 1 time pad.

$G(k)_{0..l} \oplus m_l$, $G(k)_{l+1..2l} \oplus m'_l$

but it doesn't fit definition of Enc scheme since Enc needs 3 inputs: m, k, index

→ Sender & receiver need to maintain index & has to be synchronised

If no history, choose start point randomly, but this has overhead of calculating $G(k)$ till the s^{th} bit.

Stream Cipher: PRG which starts from specified index

Block Cipher: Use blocks instead of bits

Pseudo Random Functions:

$f: \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$

Key (seed) s — Index x

If PRF is truly random, it is equivalent to one time pad

$c = \langle x, f(k,x) \oplus m \rangle$

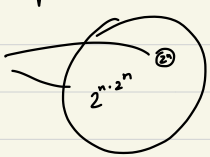
For each block choose a random x for encryption

Truly random functions:

$f_k: \{0,1\}^n \to \{0,1\}^n$

There are $2^{n \cdot 2^n}$ functions of this form. The key must have $\log(2^{n \cdot 2^n})$ bits $= n \cdot 2^n$ bits

Fixing key as n bits, a PRF is such that no PPTM adversary A can distinguish b/w the set of 2^n fns. indexed by n bits & $2^{n \cdot 2^n}$ fns of the truly random functions.



PRF:

$F_k: \{0,1\}^n \to \{0,1\}^n$

$c = \langle x, F_k(x) \oplus m \rangle$

A fn. $F_k: \{0,1\}^n \to \{0,1\}^n$ is said to be a PRF if $\forall$ PPTM A

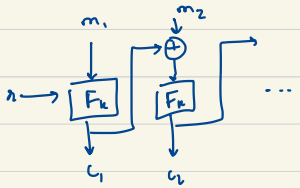
$$\left| P\left[A^{f_k}(1^n) = 1\right] - P\left[A^{F_k}(1^n) = 1\right] \right| \leq negl(n)$$

(f_k: oracle to Truly Random; F_k: oracle to Pseudo Random)

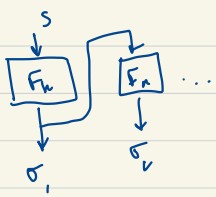
Cannot give all pairs of input-output as it is of 2^n size (exponential input cannot be handled by PPTM). Instead, give access to the function, considering it produces instantaneous output, called an oracle TM.

DES, AES are purported to be PRFs of a special kind

Theorem: Existence of PRF $\iff$ PRG



Cipher Block Chaining mode



$r_i = F_k^{(i)}(s)$

Output feedback mode

Popular, efficient (since only 1 r is sent, as $r_i = F_k(r_{i-1})$)

Browsers use Randomized Counter Mode

$r_i = F_k(r_0 + i)$

PRG $\to$ PRF:

If given a length doubling PRG: $G: \{0,1\}^n \to \{0,1\}^{2n}$

$G(s) = G_0(s) G_1(s)$ where G_0, G_1 are length preserving functions

$F_k(r_0 r_1 r_2 \ldots r_{n-1})$

$G_r(k)$

$G_0(k)$ $G_1(k)$

Choose $G_{r_0}(k)$ then do $G_{r_1}(G_{r_0}(k))$

...

at the end, n bit string $G_{r_0 r_1 \ldots r_{n-1}}(k)$

Using hybrid argument, if A can distinguish b/w truly random k (first row) & pseudo-random $G_{r_0 r_1 \ldots r_{n-1}}(k)$, then A should be able to distinguish b/w 2 $G_{r_0 r_1 \ldots r_i}(k)$, $G_{r_0 r_1 \ldots r_i r_{i+1}}(k)$, which means that G is not a PRG.