Review: PRG + 2 relaxations → Security against eavesdropper ; PRG ⇔ One way fns ; Discrete logarithm Problem (DLP)

$y = f(x) = g^x \bmod p$ DLP : Find x

Reduction to MSB DLP : DLP $\leq_p$ MSB-DLP (Existence of ✓)

Find MSB of x

If efficient algo for MSB-DLP exists, then efficient algo for DLP exists. (MSB of x is the hardest bit to find, but it is one of the hardcore predicates for DLP)

Theorem : LSB-DLP has a polynomial time soln.

Proof : Given g, p & $g^x \bmod p$, LSB(x) i.e. even or odd is solvable in polynomial time. (Shows need for hardcore predicate)

Fermat's Little Theorem

If p is prime, $\forall\ a \in [1, \ldots p-1]$,

$a^{p-1} \bmod p = 1$ (a & p are coprime)

Proof : $a \in [1 \ldots p-1]$

Let $i \neq j \wedge i, j \in [1 \ldots p-1]$ and $ia = ja \pmod p$

$\Rightarrow$ p divides $ia - ja$ $\quad p \mid ia - ja$

$\Rightarrow$ $p \mid (i-j)a$ but $i-j$ & $a \in [1 \ldots p-1]$

$\Rightarrow$ $a, 2a, 3a, 4a \ldots (p-1)a \bmod p$ are distinct & is a permutation of $1, 2, 3 \ldots p-1$

Product of $a, 2a, 3a \ldots (p-1)a \bmod p = a^{p-1}(p-1)!$

$1, 2, 3 \ldots p-1 \bmod p = (p-1)!$

$\Rightarrow a^{p-1} \bmod p = 1$

$g^{p-1} \bmod p = 1$

If $x^2 \equiv 1 \pmod p$, then $p \mid x^2 - 1$

$\Rightarrow p \mid (x+1)(x-1)$

either $x+1 = 0$ or p

$x-1 = 0$ or p

x is 1 or $p-1$

$\Rightarrow g^{\frac{p-1}{2}} \bmod p = p-1$

(since g is generator & g^{p-1} is already 1)

If $y = g^x \bmod p$,

$y^{\frac{p-1}{2}} \bmod p = g^{\frac{x(p-1)}{2}} \bmod p$

$= (p-1)^x \bmod p$

$= \begin{cases} 1 & \text{if } x \text{ is even} \\ -1 & \text{if } x \text{ is odd} \end{cases}$

Given y, calculate $y^{\frac{p-1}{2}}$ & conclude if x is even or odd in $O(\log(\frac{p-1}{2}))$ time

---

Can we use this to solve DLP in polynomial time?-

Let $y = g^x \bmod p$.

Find $lsb(x) = l$

$\rightarrow$ If $l == 0$:

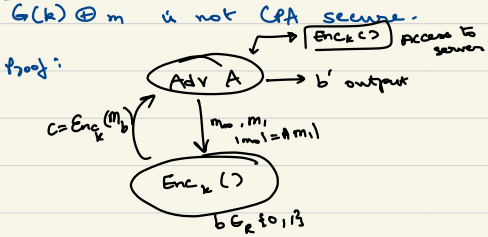
$y \leftarrow \sqrt{y} = g^{x/2} \bmod p$

else, $l == 1$:

$y \leftarrow \sqrt{yg^{-1}}$ (same as $\sqrt{y-1}$

Thm:
$G(k) \oplus m$ is not CPA secure.

Proof:



$P[b = b'] \leq \frac{1}{2} + negl(n)$

$y = g^x \bmod p$

$\sqrt{y}$ — $g^{x/2} \bmod p$ ans 1

— $g^{\frac{x}{2} + \frac{p-1}{2}} \bmod p$ ans $z = -$ ans 1

The positive root is the one we need to use & to decide which is the +ve root, we need to know MSB ($> \frac{p-1}{2}$ or $< \frac{p-1}{2}$).

Thus, DLP cannot be solved using only LSB-DLP.

PRG:

$G(k) = \sigma_1 \sigma_2 \sigma_3 \ldots$

$\sigma_i = h(f^i(k))$

Ex: $f(x) = g^x \bmod p$

$G(k)$ (The PRG) has to be as fast as the fast insecure channel if PRG is run online to use full bandwidth of the fast insecure channel

---

Thm: No deterministic encryption scheme is CPA secure.

Use encryption servers to get ciphertext of m_0 & m_1 as c_0 & c_1. Compare $c = Enc_k(m_b)$ with c_0 & c_1 to decide b' with probability 1.

→ CPA security needs probabilistic encryption.

Probabilistic Encryption

Choose a random nonce (number used once)

$c = \langle r \in_R \{0,1\}^n, Enc_k(r) \oplus m \rangle$

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