CAS CS538 Problem Set 3

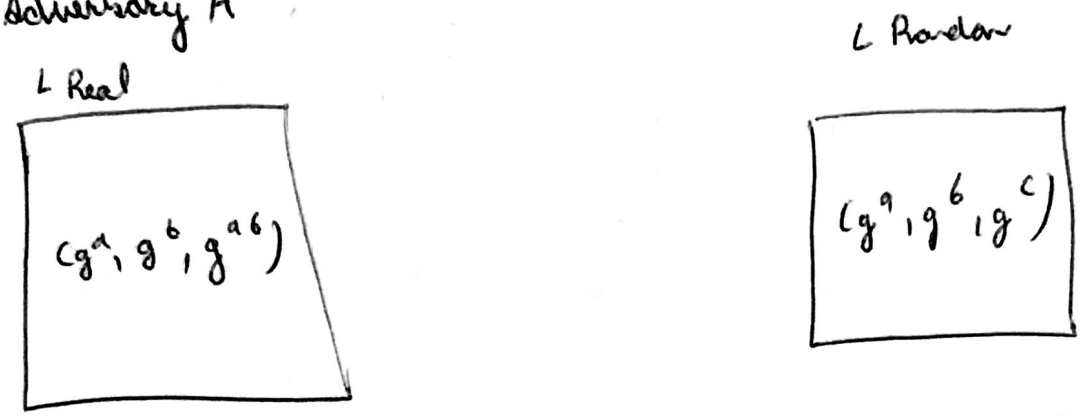
Riken Mahajan

Collabration with Biken Mahanjan

Problem 1.

Squares modulo-p test = $O(\lambda^3)$

Adversary A



Adversary A can use Euler's criterion to distinguish the library. He can use Euler's criterion in the following way:

$$\beta = g^x$$

apply

$$\beta^{\frac{(p-1)}{2}} \equiv_p g^{x\frac{(p-1)}{2}}$$
$$\equiv_p (-1)^x$$

Hence

If $\beta^{\frac{(p-1)}{2}} \equiv_p 1$ then x is even

else x is odd.

So, he has power to see if x is even or odd.

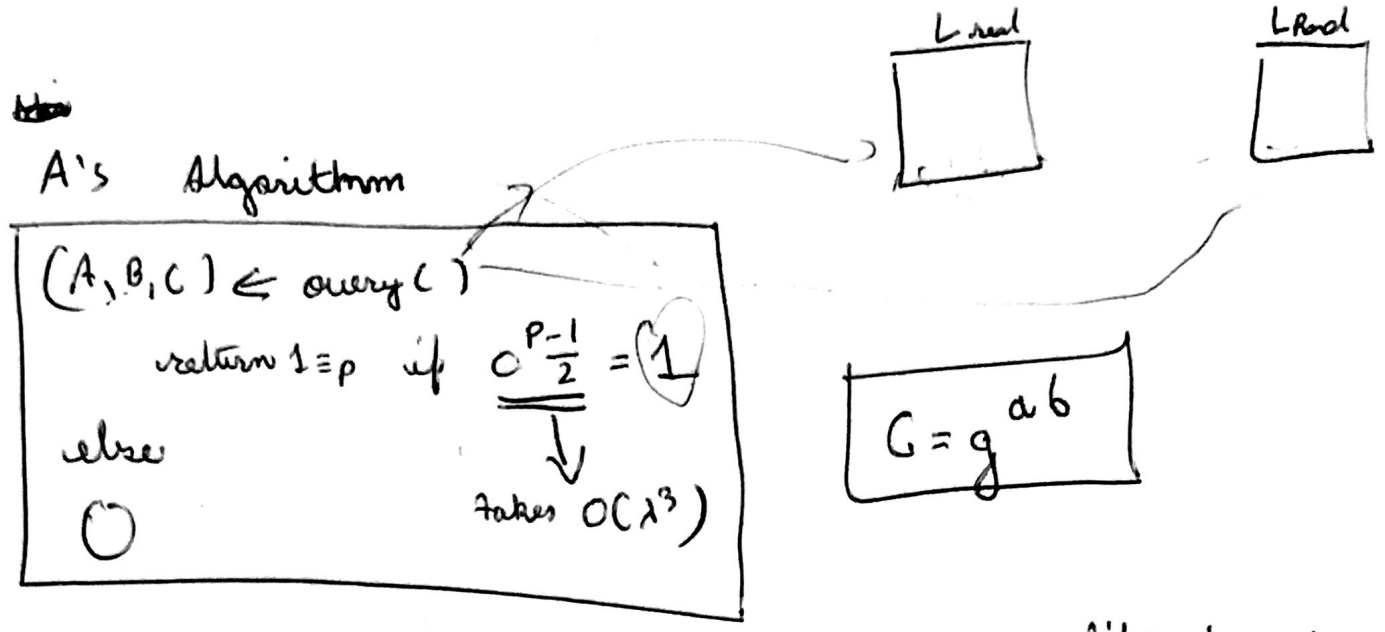
This is useful to distinguish Real from Random because of the following:

$\Rightarrow$ g^{ab} is $\frac{3}{4}$ even whereas g^c from random is $\frac{1}{2}$ times even

g^{ab} g^c

Now if he builds an algorithm to exploit this he can distinguish Real and Random.

P.T.O



If he links with both real and random libraries, he can distinguish them.

$$Pr[A \diamond L_{real} \to 1] = Pr[ab = even] = \frac{3}{4}$$

$$Pr[A \diamond L_{random} \to 1] = Pr[C = even] = \frac{1}{2}$$

$$Pr[A \diamond L \to 1] - Pr[A \diamond L_{random} \to 1]$$

$$= \frac{3}{4} - \frac{1}{2}$$

$$= \boxed{\frac{1}{4}}$$

Problem 2

Given

$141 = n$

$\langle g \rangle$ = generator

$h_1 \in q \qquad h_1 = g^a \bmod n$

$h_2 \in q \qquad h_2 = g^b \bmod n$

$DL(h_1) = a$

$DL(h_2) = b$

- $DL(h_1 h_2) = [DL(h_1) + DL] \bmod (n-1)$

$= (a+b) \bmod (n-1)$

- $DL(h_1/h_2) = DL(h_1 h_2^{-1}) = [DL(h_1) - DL(h_2)] \bmod (n-1)$

$= (a-b) \bmod (n-1)$

(3) 60 points

(a) f_0 runs in time t

HCG

$|H| = \frac{|G|}{100} = \frac{n}{100}$

$$f_0(h) \begin{cases} \log_g h & \text{if } h \in H \\ \text{fail} & \text{else} \end{cases}$$

Design an Algorithm f_1 that runs time $t + \text{poly}(\lambda)$.

f_1 Algorithm

for some $h \in G$, take arbitary $m \in G$

Randomize (h, g):

$k = h \times m \quad \forall m \in G$

Apply f_0 to k.

$$dL(k) = d(hm) = [d(h) + d(m)] \bmod (n-1)$$

$$= [d(h) + d(m)] \bmod (n-1)$$

return $dL(k)$

This Algorithm spits every output to have atleast 1% of being in H subset.

36

We know that the outputs of f_1 all have 1% chance of being from Set H.

⇒ Hence if we call f_1 once we have 499 t running time left. As running time of f_1 ($t + poly(\lambda)$) and we had $500t + poly(\lambda)$.

Randomly take 499 outputs of f_1. They all will have 1% chance of being from set H. Run f_0 on all 499 element of f_1 output.

Hence $499 \times 1\%$ of being in $\in H$
$= 499 \times 0.01 = 4.99$ of the answers will have dL.

So return 5 elements where 4.99 will have

$$= \frac{4.99}{5} \times 100$$

$$= 99\%$$

So if we send 5 outputs from f_2 where 4.99 of the answers have dL then the f_2 will output atleast 99% for every $h \in G$.

f_2

run f_1 once and get (elements) = outputs with 1% probability $\in H$. → $t + poly(\lambda)$

Use 499 outputs from f_1 and check/run f_0 on all 499 outputs. → $499t$

output elements from these 499 elements which belong $\in H$. ⇒ $499 \times 0.01 = 4.99$ elements $\in H$

output 5 elements where 4.99 elements will belong $\in H$.

Hence 99%

$500t + poly(\lambda)$