18.733

Vishnuta Rudrush

HomeWork 3

Due March 10, 2017

1) Cyclic Groups Warmup [3 points]

In the forward direction;

Given g is a generator of $\mathbb{Z}_p^*$

$$\mathbb{Z}_p^* = \{g^0, g^1, \ldots g^{2q-1}\} = \langle g \rangle \; ; \; g^{2q} = 1$$

$$\sqrt{g^{2q}} = g^q \equiv \sqrt{1} \equiv \pm 1 \bmod p.$$

If $g^q = 1 \bmod p \Rightarrow$ generator wraps around early and does not generate $\{g^0, g^1 \ldots g^{2q-1}\}$

Hence, $g^q \equiv -1 \bmod p$

In the reverse direction;

Suppose $g^q \equiv -1 \bmod p$, which means $\langle g \rangle = \{g^0, g^1 \ldots\}$ would be a subset of $\mathbb{Z}_p^*$.

To prove; the subset so generated is actually the complete $\mathbb{Z}_p^*$

$$|\mathbb{Z}_p^*| = 2q + 1 - 1 = 2q.$$

Using Lagrange's theorem, a subgroup of $\mathbb{Z}_p^*$ must divide $|\mathbb{Z}_p^*| = 2q$.

Therefore, if $|\langle g \rangle| \in \{1, 2, q, 2q\}$ cannot be one and can't be q as ~~g^q~~ $g^q \neq 1$. Similarly, it can be shown that $|\langle g \rangle| \neq$ and hence, $|\langle g \rangle| = 2q$, Therefore, g is a generator of $\mathbb{Z}_p^*$.

2) Security of Provable Compression Function [3 points]

Contraposition:

H is not CR which implies that it is easier to find a discrete log.

$H(x, y) = g^x h^y$; compression function

Therefore, H is collision resistant, then

$g^{x_1} h^{y_1} = g^{x_2} h^{y_2}$

$g^{x_1 - x_2} = h^{y_2 - y_1}$

Let $h = g^k$ where k = discrete log

$g^{x_1 - x_2} = g^{k(y_2 - y_1)}$

$\therefore x_1 - x_2 = k(y_2 - y_1)$

$\therefore k = \left(\frac{x_1 - x_2}{y_2 - y_1}\right) = (x_1 - x_2)(y_2 - y_1)^{-1}$

Known: x_1, x_2, y_1, y_2 and ~~x_1, x_2~~, they belong to $\mathbb{Z}_p^*$, ~~which~~ a cyclic group.

Therefore $(y_2 - y_1)^{-1}$ can be computed in polynomial time as it is present in $\mathbb{Z}_p^*$.

Hence, k can be found.

3) Taking Roots Modulo Composite Numbers is Hard [4 parts]

From Fermat's factorization, we can see that, for any odd integer N;

$N = a^2 - b^2$ for some $a, b \in Z_N$ and N can be found.

$\therefore (a+b)(a-b) = kpq$ for some integer k, showing that prime factorization of both sides must be equal. Therefore, at least p or q must be a greatest common factor.

Also known, for a square in Z_N, there are 4 square roots. From the Chinese remainder theorem, the 4 square root would be $\pm x, \pm z$ for some $x, z \in Z_N$.

Hence, say $x \in Z_N$; $y = x^2 \bmod N$

say $x' = A(y) = \sqrt{x}$; we need find $x \neq x'$; such that one of $\gcd(x - x', N)$, $\gcd(x + x', N)$ is a non-trivial factor of N.

Therefore, we can see that the square root of a number modulo a composite is at least as hard as factoring an RSA modulus $N = pq$ where p and q are prime numbers.

4) PRG from the Discrete Log Problem [4 points]

We can use the legendre symbol to find the lsb of x.
If x is even, g^x is a square;
i.e $\sqrt{g^x} = \pm g^{x/2}$; otherwise x is odd and g^x is not a square.

So, an algorithm can proceed by checking if g^x is a square, if it is not, we can decrement x by 1, which is equivalent to multiplying g^x by g^{-1}. On obtaining the 2 square roots, we can proceed to find which of the 2 square roots is to be used. For this, we can use the half function $half_{p-1}(g^x, g, p)$ and whichever value corresponds to the half function being zero, i.e $half_{p-1}(g^x, g, p) = 0$ should be used.

We can repeat or iterate this over the number of bits in the p and at the end we have value of x.

Algorithm: Compute x for input $(g, p, y = g^x)$

1) Let n = number of bits in p, $y_n = y$
2) Let L = legendre symbol of y_n
3) If $L = 1$, set n^{th} bit to zero else to 1 and set $y_n = y_n g^{-1} \bmod p$.
4) Find $\sqrt{y_n} \bmod p = (s, -s)$; $y_{n-1} = s$
5) Find $A = A(y_{n-1}, g, p) = half_{p-1}(y_{k-1}, g, p)$
6) If $n = 1$, then $y_{n-1} = -s$
7) $n = n-1$; if $n! = 0$, repeat (go to step 2) else output in x.

5) (Programming) Oracle Padding Attack [6 points]

b) Yes, an attack would still be possible.
If Eve is geographically very far away from the network, Eve would have to make a large number of queries to obtain the same result. She would have to also consider taking an average latency of the requests. So, therefore further away Eve is from the oracle, larger the number of requests.

c) The oracle can be setup to handle only a set number of requests from a client. If a client makes more than the expected number of requests as per the oracle, subsequent requests from the client can be dropped.
We could also consider encrypting and then MACing the requests, preventing malicious adversaries such as Eve from making requests.