CS 681: Computational Number Theory and Algebra **Lecture 25: Discrete Log Problem**
Lecturer: Manindra Agrawal **Notes by: Arun Iyer**

October 18, 2005.

1 Discrete Log Problem

Definition 1.1 *Given a finite group G, and g,e $\in$ G, find m (if it exists) such that $g^m = e$. This problem is known as the Discrete Log Problem.*

Examples :

1. Given $G = \mathbb{Z}_n$ *under* $+$, find an m such that $mg = e(mod\, n)$.
2. Given $G = \mathbb{Z}_n^*$ *under* $*$, find an m such that $g^m = e(mod\, n)$.
3. Given $G = P_n$ *under composition* and g and e be two permutations, find an m such that that $g^m = e$.
4. Given $G = F_{p^r}$ *under* $+$, find an m such that $mg(x) = e(x)$.
5. Given $G = F_{p^r}$ *under* $+$, find an m such that $g^m(x) = e(x)(mod\, p, h(x))$.

2 Application : El Gamal Public Key Encryption

Given a group G and $g \in G$ of large order, randomly choose an $m \in \mathbb{Z}$ and let $e = g^m$. Then,
Public Key : (g,e)
Private Key : m

2.1 Encryption Method

Input : message s ($s \in G$)

1. Randomly choose $k \in \mathbb{Z}$
2. Compute $r = g^k$
3. Output se^k, r

2.2 Decryption Method

Input : se^k, r

1. Compute r^m
2. Compute inverse of r^m i.e $(r^m)^{-1}$
3. Output $se^k(r^m)^{-1}$

3 Slight Improvement in Special Case

Normally for encryption purposes we use the group $G = F_p^*$ under *. However, this encryption can fall weak if $p-1$ turns out to be smooth. To avoid this circumstance, a large prime p is chosen such that $p-1 = 2q$ where q is a large prime as well.

4 Solving Discrete Log using Index Calculus

Basic Idea : Find r and s such that $g^r e^s = 1$ and $(s, order(g)) = 1$. (Note that : If m is the message, then $g^r e^s = g^r g^{ms} = g^{r+ms}$. This implies $m = -rs^{-1}(mod\ order(g)))$

1. Randomly choose r and s and compute $g^r e^s = u$
2. Check if u is $k - smooth$
3. If yes, collect the triple (r,s,u)
4. Repeat until k tuples are collected, let (r_i,s_i,u_i), $1 \leq i \leq k$ be these triples
5. Let $u_i = \prod_{j=1}^{k} p_j^{\alpha_{i,j}}$, [$p_j$'s are primes]
6. Find vector $\overrightarrow{\beta}$ such that

$$\sum_{j=1}^{k} \beta_i \alpha_{i,j} = 0(mod\ p-1)\forall i$$

7. Compute $r = \sum_{i=1}^{k} \beta_i r_i$ and $s = \sum_{i=1}^{k} \beta_i s_i$
8. Compute $m = -rs^{-1}(mod\ p-1)$