Semigroup actions and the discrete log problem

Jim Renshaw

June 12, 2019

UNIVERSITY OF Southampton
School of Mathematics

Outline

1. Background
2. Groups acting on semigroups

Discrete Log

- Choose a large prime p and a residue n coprime to $p - 1$.
- Encode data using integers in $\mathbb{Z}_p$.
- Encrypt data using the function $x \mapsto x^n \mod p$.
- Decrypt using the function $x \mapsto x^m \mod p$ where $nm \equiv 1 \mod (p - 1)$.

Discrete Log

- More algebraically, let $G = U_{p-1}$ be the group of units of the ring $\mathbb{Z}_{p-1}$ and $S = U_p$ the group of units of $\mathbb{Z}_p$.
- For $n \in G, x \in S$ define an action of G on S by $n \cdot x = x^n$.
- The value of x is the *plaintext*, n is the *(encryption) key* and $n \cdot x$ is the *ciphertext*.
- We call n the *discrete log* of x^n.
- The usefulness of this system lies in the fact that we know of no efficient, non-quantum algorithms, to solve this particular *discrete log problem* - given x, x^n and p, calculate n.

Discrete Log

Can we 'improve' on this action of a group on a group by replacing one or both of the groups by a semigroup?

Completely Regular semigroups

Let S be a semigroup and define an action of U_r, the group of units mod r, on S by

$$n \cdot x = x^n.$$

In order for this action to be invertible, there needs to exist m such that

$$(x^n)^m = x.$$

Hence S must be completely regular.

Completely Regular semigroups

Two classic examples:

1. Discrete Log Cipher
   For U_{p-1} acting on $\mathbb{Z}_p$, we have

$$\mathbb{Z}_p = U_p \cup \{0\}.$$

Completely Regular semigroups

Two classic examples:

1. Discrete Log Cipher
   For U_{p-1} acting on $\mathbb{Z}_p$, we have
   $$\mathbb{Z}_p = U_p \cup \{0\}.$$
2. RSA cipher
   For distinct primes p and q, $U_{\phi(pq)}$ acts on $\mathbb{Z}_{pq}$ and
   $$\mathbb{Z}_{pq} \cong U_{pq} \dot{\cup} U_p \dot{\cup} U_q \dot{\cup} \{0\}.$$

Completely simple semigroups

Suppose now that S is a completely simple semigroup, considered as a Rees matrix semigroup $\mathcal{M}[G; I, \Lambda; P] = I \times G \times \Lambda$ and suppose also that G is finite, of order r so that $g^r = 1$ for all $g \in G$.

$$(i, g, \lambda)(j, h, \mu) = (i, gp_{\lambda j}h, \mu).$$

Define an action of U_r, the group of units in $\mathbb{Z}_r$, on S by $n \cdot x = x^n$, so that if $x = (i, g, \lambda)$ then

$$n \cdot x = x^n = (i, (gp_{\lambda i})^{n-1}g, \lambda).$$

Completely simple semigroups

Suppose now that n is coprime to r and that $mn \equiv 1 \mod r$. Then

$$x^{mn} = (i, (gp_{\lambda i})^{mn-1} g, \lambda) = (i, (gp_{\lambda i})^{mn} p_{\lambda i}^{-1}, \lambda) = (i, (gp_{\lambda i}) p_{\lambda i}^{-1}, \lambda) = (i, g, \lambda) = x.$$

Consequently if we know n, x^n and P, then we can compute x^{mn} and so recover x.

Moreover

$$(gp_{\lambda i})^{mn-1} g = \left(\left((gp_{\lambda i})^{n-1} g\right) p_{\lambda i}\right)^m p_{\lambda i}^{-1}.$$

We will in fact assume that $|\Lambda| = 1$.

Completely simple semigroups

Theorem (Banin & Tsaban, 2016)

The discrete log problem over a semigroup, can be reduced, in polynomial time, to the classic discrete log problem in a subgroup of S.

However this assumes that we can compute with the semigroup S and in order to do that with a Rees Matrix Semigroup, we would require knowledge of the sandwich matrix P.

Chosen plaintext attack

- $|I| = m$;
- $g_1, \ldots, g_{m+1}$ distinct elements of G;
- Encrypt the values (i, g_i) as $(i, g_i^n p_i^{n-1})$.
- Pigeon hole principle : $i \neq j$ such that $p_i = p_j$ and hence

$$(g_i^n p_i^{n-1})(g_j^n p_j^{n-1})^{-1} = (g_i g_j^{-1})^n.$$

- $\binom{m+1}{2} = O(m^2)$ possible pairs.

Chosen plaintext attack

- Encrypt (i, g) and (i, g^{-1});
- obtain $(i, (gp_i)^{n-1}g)$ and $(i, (g^{-1}p_i)^{n-1}g^{-1})$;
- If G is abelian, then we can calculate $(p_i^{n-1})^2$ and hence $(g^2)^n$.

Completely Simple Cipher

Alice wants to sent Bob a secret message. Let G be a finite (abelian) group and let $I = G$. Let $n \in U_{|G|}$ and $s \in I$ be two secret keys known only to Alice and Bob.

We encrypt $g \in G$ as follows: choose a random value $i \in I$ and let $p_i = H(i, s)$, where H is some cryptographically secure hash function.

Alice computes $(i, (gp_i)^{n-1}g)$ as her encrypted value of g to send to Bob.

Bob calculates $p_i = H(i, s)$ and $m \in U_{|G|}$ such that $mn \equiv 1 \mod |G|$ and then computes

$$g = \left(\left((gp_i)^{n-1}g\right) p_i\right)^m p_i^{-1}.$$

Brute force attack

Group case.
Given g and g^n, calculate $g, g^2, \ldots, g^n$.
Worst case $\phi(|G|) \sim O(|G|)$ multiplications.

Brute force attack

Group case.
Given g and g^n, calculate $g, g^2, \ldots, g^n$.
Worst case $\phi(|G|) \sim O(|G|)$ multiplications.

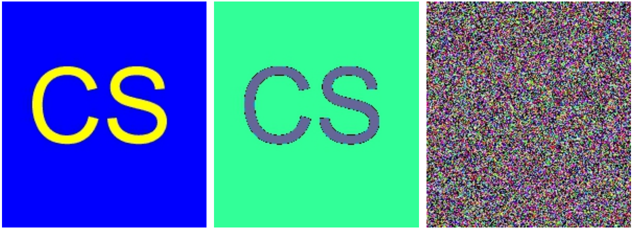
Semigroup case.
Given g and $(i, (gp_i)^{n-1}g)$

Computing n using trial multiplication attack would consists of computing $(gq)^{m-1}g$ for $1 \leq m \leq n$ and $q \in G$ in order to find the relevant pair (n, p_i). Worst case $|G|\phi(|G|) \sim O(|G|^2)$.

Completely Simple Cipher

1. If $|G| = n$ is odd there are at least
$$S(n) = n \prod_{p|n} \left(1 - \frac{2}{p}\right)$$
solutions.
2. If $|G| = n$ is even there are at least $T(n)$ solutions where
$$T(n) = O(\frac{n}{4r} S(r))$$
where r is the largest odd factor of n.

Completely Simple Cipher



(a) original (b) group (c) semigroup

Figure : discrete log encryption on similar blocks