7.2.4. RSA assumption

- The factoring problem has no known efficient solution.
- While it has been studied for hundreds of years a solution may exist.

- However, the current assumption is that it will never be solved in polynomial time
- But it is not very practical for cryptography purposes.
- A related problem is the Rivest, Shamir, and Adleman Problem.
- AKA RSA problem. This problem is based on the following Assymmetry.

$$|\mathbb{Z}_N^*| = \phi(N) = (p-1)(q-1) \quad \text{where} \quad N = pq$$

(1.) If factorization of N is known then computing $\phi(N)$ is trivial, which implies g^e computations mod N are easy. ✓

(2) If factorization of N is unknown, then it is difficult to compute $\phi(N)$ (factor it!) and so g^e computation mod N are not possible.

Informally: We know the following

$\forall y \in \mathbb{Z}_N^*$, $\exists$ $y^{1/n} \bmod N$ s.t. $(y^{1/n})^n \bmod n$

B/c of group structure

$= y \bmod N.$

$$\boxed{\begin{array}{l} \text{(since if } (N,c)=1 \text{ then } y_c \text{ is a permutation)} \\ \text{and } \exists\, g \text{ s.t. } \quad y_c(g) = g^c = y \qquad g^c = y^{1/n} \end{array}}$$

The RSA problem states

$\boxed{\text{Given } N, c, y \text{ find an } x \text{ such that } x^c = y \bmod N.}$ is hard!

The RSA assumption is that there exists an GenRSA relative to which RSA problem is hard.

Let's define the RSA problem. Formally

Let GenRSA be a PT algorithm that on input 1^n, outputs a modulus N that is the product of two n-bit primes, an integer $e > 0$ with $(e, \phi(N)) = 1$ and an int d s.t $ed = 1 \bmod \phi(N)$. The algorithm may fail with negl probability.

RSA experiment: $\text{RSA-inv}_{A, \text{GenRSA}}(n)$

1. Run $\text{GenRSA}(1^n)$ to obtain (N, e, d)
2. Choose $y \leftarrow \mathbb{Z}_N^*$
3. A is given N, e, y and outputs $x \in \mathbb{Z}_N^*$
4. Output is 1 if $x^e = y \bmod N$ and 0 otherwise

find x s.t $x^e = y \bmod N$

Note. If factorization of N is known then RSA experiment is easy to solve. compute $\phi(N)$ (then compute $y^d \bmod N$

compute $d = [e^{-1} \bmod \phi(N)]$

$(y^d)^e = y$

Def. We say RSA problem is hard relative to GenRSA if $\forall$ PPT A, $\exists$ a negligible function negl s.t

$$\Pr[\text{RSA-inv}_{A, \text{GenRSA}}(n) = 1] \leq \text{negl}(n)$$

RSA Assumption

There exists a GenRSA relative to which the RSA problem is hard

A GenRSA can allways be constructed from Any GenModulus algorithm as follows.

GenRSA

Input: Security parameter 1^n

Output: (N, e, d) where

$(N, p, q) \leftarrow \text{GenModulus}(1^n)$

$\phi(N) = (p-1)(q-1)$

find e s.t. $(e, \phi(N)) = 1$

Compute $d := [e^{-1} \bmod \phi(N)]$

return N, e, d

13.1

Def. Let $g \in G$ s.t. $|G| < \infty$. Then the order of g is the smallest integer i with $g^i = 1$.

Def. Let $g \in G$ s.t. $|G| < \infty$. Then $\langle g \rangle$ is the subgroup generated by g and is defined to be $\{g^0, g^1, \dots, g^{|g|-1}\}$

Proposition. Let G be a finite group and $g \in G$ an element of order i. Then $g^x = g^y$ iff $x = y \bmod i$.

$\Leftarrow$

If $x = y \bmod i$ then $g^x \overset{FLT}{=} g^{[x \bmod i]} = g^{[y \bmod i]} = g^y$.

$\Rightarrow$

Let $x' = [x \bmod i]$
$y' = [y \bmod i]$
then by $\Leftarrow$ $g^{x'} = g^{y'} \Rightarrow g^{x'} g^{-y'} = 1$

If $x' \neq y'$, WLOG $x' > y'$. Then $x', y' < i$ and $x' - y' < i$.

Then $g^{x'} g^{-y'} = g^{x'-y'} = 1$

$\Rightarrow |g| < i$ #

Def. G is a cyclic group if there exists $g \in G$ s.t. $|g| = |G|$.

Note.
This definition implies that for any $h \in G$ $h = g^x$ for some x.

Example.

$$\mathbb{Z}_8^* = \{1, 3, 5, 7\}$$

$\langle 3 \rangle = \{3, 1\}$ - Subgroup generated by 3

Example

$$\mathbb{Z}_6^+ = \{1, 2, 3, 4, 5, \cancel{6}\}$$

$\mathbb{Z}_5^+$ is cyclic and generated by $\langle 1 \rangle$

$\mathbb{Z}_5^+$ is also generated by $\langle 5 \rangle$.

$$\{5, 4, 3, 2, 1\}$$

Conclusion: Cyclic groups do not have a "canonical" generator

However we can place a restriction on the possible orders of a cyclic group.

So a group of prime order is cyclic. However this is not applicable for $\mathbb{Z}_p^*$. But we can show such groups are cyclic

Thm. If p is prime, then $\mathbb{Z}_p^*$ is cyclic.

Proof. Need field Theory. Out of scope.

Example. $\mathbb{Z}_7^*$ is cyclic.

$\langle 2 \rangle = \langle 2, 4, 8 \rangle = \langle 2, 4, 1 \rangle$

2 is not a generator

$\langle 3 \rangle = \{3, 9, 27, 81, 243, 729\} = \{3, 2, 6, 4, 5, 1\}$

3 is a generator

Something you have heard before is that all cyclic groups of the same order are equivalent up to isomorphism.

Example.

Let G be cyclic of order n, and g be a generator.

Then $f: \mathbb{Z}_n \to G$ defined by $f(a) = g^a$ is a isomorphism.

$f(a + a') = g^{a+a'} = g^a \cdot g^{a'} = f(a) \cdot f(a')$

Injection: $\ker f \neq \emptyset$

$\exists\, a \in \mathbb{Z}_n$ s.t. $f(a) = 1$ and $a \neq 1$

$f(a) = g^a = 1$ then $g^1 = g^a = 1$.

but $g^1 = g \mapsto g \neq 1$.

Surjection

injections on finite groups are surjections

Interesting Note

While groups may be isomorphic. The computational complexity of operations in the two groups are very different.

Proposition 7.51. Let G be a finite group of order m, and say $g \in G$ has order i. Then $i \mid m$.

Proof

$g^m = 1$ by FLT

$g^m = g^{[m \bmod i]}$ by corrollary of FLT

Suppose i does not divide m. Then $i' = [m \bmod i]$ is a pos int s.t $i' < i$ and $g^{i'} = 1$. But $g^i = 1$ $\#$

This proves a surprisingly powerful Thm.

Corollary. If G is a group of prime order p, then G is cyclic. Furthermore, all non-identity elements are generators of G.

Proof. If $g \in G$ the $|g| = 1$ or p. Only the identity has order 1. Then all other elements have order p and generate G.