CS 346 Class Notes

Mark Lindberg

Apr 4, 2016

This Time:

Upcoming exam:

Study problem sets 3 and 4.

Authenticated encryption, up to and including Chinese Remainder Theorem.

The factoring assumption:

First attempt:

Pick a random n-bit number N. Adversary $\mathcal{A}$ gets N, outputs x. $\mathcal{A}$ wins if x is a nontrivial factor of N. We'd like to say that $\mathcal{A}$ has $\leq \texttt{negl}$ probability of success. This fails because, for example, 2 is a factor of 50% of numbers, and this gives way better than negligible success.

Actual factoring experiment:

Three parameters: n, $\mathsf{GenModulus}$.

$\mathsf{GenModulus}$ on input 1^n, generates distinct n-bit primes p, q and their product N, where N is the modulus. (Note: $\mathsf{GenModulus}$ is allowed to fail with $\texttt{negl}(n)$ probability.)

$\mathsf{Invert}_{\mathcal{A},\mathsf{GenModulus}}(n)$: Run $\mathsf{GenModulus}(1^n)$ to get N, p, q. Gives N, n to $\mathcal{A}$. $\mathcal{A}$ outputs x. $\mathcal{A}$ wins if $x = p$ or $x = q$.

The factoring assumption:

$\exists$ PPT $\mathsf{GenModulus}$ such that $\forall$ PPT $\mathcal{A}$, $\Pr[\mathsf{Invert}_{\mathcal{A},\mathsf{GenModulus}}(n) = 1] \leq \texttt{negl}(n)$. It is believed that the above holds for "basic" $\mathsf{GenModulus}$.

RSA assumption: $\mathsf{GenRSA}(1^n)$ produces N, e, d. Run $\mathsf{GenModulus}(1^n)$, to get N, p, q. Determine an e relatively prime to $\phi(N) = (p-1)(q-1)$. Determine d as $e^{-1} \pmod{\phi(N)}$.

The experiment: $\mathsf{Invert}_{\mathcal{A},\mathsf{GenRSA}}(n)$: Run GenRSA to get N, e, d. Select a uniform random $y \in \mathbb{Z}_n^*$.

Give $\mathcal{A}$ n, N, e, y, $\mathcal{A}$ outputs x.

$\mathcal{A}$ succeeds if $x^e = y \pmod{N}$.

$f_e(x) = x^e$, f_e corresponds to a permutation on $\mathbb{Z}_n^*$.

RSA Assumption:

$\exists \mathsf{GenRSA}$ such that $\forall$ PPT $\mathcal{A}$, $\Pr[\mathsf{Invert}_{\mathcal{A},\mathsf{GenRSA}}(n) = 1] \leq \texttt{negl}(n)$.

We do have, 8.2.5, that if factoring is polynomial time solvable, then the RSA problem is polynomial time solvable.

He then goes over "textbook" RSA. Sorry, but I completely zoned out because I've taught this subject before.

Cryptographic assumption in cyclic groups.

G is a finite group. Let $g \in G$. $\langle g \rangle = \{g^0, g^1, \ldots, g^{i-1}\}$, where i is the least positive integer such that $g^i = 1$. Note that $\forall g$, $g^{|G|} = 1$.

$\langle g \rangle$ is the subgroup of G generated by g, and it is a group of order i.

We say that g has order i in the group G.

Proposition 8.52: $g^x = g^{x \pmod{i}}$. Easy because $g^i = 1$.

Proposition 8.53: $g^x = g^y \Rightarrow x \equiv y \pmod{i}$. Easy.

Proposition 8.54: $i \mid |G|$.

Proof is in theorem 8.14.

Corollary 8.55: If $|G|$ is a prime p, every element $g \in G$ except the identity element is a generator.

A generator is an element such that $\langle g \rangle = G$.

Caution: $\mathbb{Z}_N^*$ does not have prime order.

Theorem 8.56: For any prime p, $\mathbb{Z}_p^*$ is a cyclic group of order $p-1$.

Residues and subgroups. Again, I had an entire class on algebraic structures, so I'm having a hard time concentrating today.