Introduction to Cryptology

Lecture 20

Announcements

- HW 8 due 4/24
- EC’s
- Homeworks 5, 6 and Class Ex’s returned at end of class.

Agenda

- Last time:
  - Number theory background (8.2)
- This time:
  - Number theory background
  - Hard problems

Modular Exponentiation

Is the following algorithm efficient (i.e. poly-time)?

ModExp(a, m, N) //computes $a^m \; mod \; N$

Set $temp := 1$

For $i = 1$ to m

Set $temp := (temp \cdot a) mod \; N$

return $temp$;

No—the run time is $O(m)$. m can be on the order of N. This means that the runtime is on the order of $O(N)$, while to be efficient it must be on the order of $O(\log N)$.

Modular Exponentiation

We can obtain an efficient algorithm via "repeated squaring."

ModExp(a, m, N) //computes $a^m \ mod \ N$, where $m = m_{n-1}m_{n-2} \cdots m_1 m_0$ are the bits of m.

Set $s \coloneqq a$

Set $temp \coloneqq 1$

For $i = 0$ to $n - 1$

If $m_i = 1$

Set $temp \coloneqq (temp \cdot s) mod \ N$

Set $s \coloneqq s^2 \ mod \ N$

return $temp$;

This is clearly efficient since the loop runs for n iterations, where $n = \log_2 m$.

Modular Exponentiation

Why does it work?

$$m = \sum_{i=0}^{n-1} m_i \cdot 2^i$$

Consider $a^m = a^{\sum_{i=0}^{n-1} m_i \cdot 2^i} = \prod_{i=0}^{n-1} a^{m_i \cdot 2^i}$.

In the efficient algorithm:

s values are precomputations of a^{2^i}, for $i = 0\ to\ n-1$ (this is the "repeated squaring" part since $a^{2^i} = (a^{2^{i-1}})^2$).

If $m_i = 1$, we multiply in the corresponding s-value.

If $m_i = 0$, then $a^{m_i \cdot 2^i} = a^0 = 1$ and so we skip the multiplication step.

Toolbox for Cryptographic Multiplicative Groups

Can be done efficiently	No efficient algorithm believed to exist
Modular multiplication	Factoring
Finding multiplicative inverses (extended Euclidean algorithm)	RSA problem
Modular exponentiation (via repeated squaring)	Discrete logarithm problem
	Diffie Hellman problems

We have seen the efficient algorithms in the left column.
We will now start talking about the “hard problems” in the right column.

The Factoring Assumption

The factoring experiment $Factor_{A,Gen}(n)$:

1. Run $Gen(1^n)$ to obtain (N, p, q), where p, q are random primes of length n bits and $N = p \cdot q$.
2. A is given N, and outputs $p', q' > 1$.
3. The output of the experiment is defined to be 1 if $p' \cdot q' = N$, and 0 otherwise.

Definition: Factoring is hard relative to Gen if for all ppt algorithms A there exists a negligible function neg such that

$$\Pr\left[Factor_{A,Gen}(n) = 1\right] \leq neg(n).$$

How does Gen work?

1. Pick random n-bit numbers p, q
2. Check if they are prime
3. If yes, return (N, p, q). If not, go back to step 1.

Why does this work?

- Prime number theorem: Primes are dense!
  - A random n-bit number is a prime with non-negligible probability.
  - Bertrand's postulate: For any $n > 1$, the fraction of n-bit integers that are prime is at least $1/3n$.
- Can efficiently test whether a number is prime or composite:
  - If p is prime, then the Miller-Rabin test always outputs "prime." If p is composite, the algorithm outputs "composite" except with negligible probability.

Miller-Rabin Primality Test

ALGORITHM 8.44
The Miller-Rabin primality test

Input: Integer $N > 2$ and parameter 1^t
Output: A decision as to whether N is prime or composite

if N is even, **return** "composite"
if N is a perfect power, **return** "composite"
compute $r \geq 1$ and u odd such that $N - 1 = 2^r u$
for $j = 1$ to t:
  $a \leftarrow \{1, \ldots, N-1\}$
  if $a^u \neq \pm 1 \bmod N$ and $a^{2^i u} \neq -1 \bmod N$ for $i \in \{1, \ldots, r-1\}$
    return "composite"
return "prime"

Why does it work?

First, note that $a^{2^i u} = \sqrt{a^{2^{i+1} u}}$, and that if p is prime then $\sqrt{1}\ mod\ p \equiv \pm 1$.

- If N is prime: By Fermat's Little Theorem, $a^{N-1} \equiv a^{2^r u} \equiv 1\ mod\ N$.
  - Case 1: One of $a^{2^i u} \equiv -1\ mod\ N$.
  - Case 2: None of $a^{2^i u} \equiv -1\ mod\ N$. Then by the facts above, all of $a^{2^i u} \equiv 1\ mod\ N$. In particular, $a^{2u} \equiv 1\ mod\ N$. So by facts, $a^u \equiv \sqrt{a^{2u}} \equiv \pm 1\ mod\ N$.
- If N is composite: At least half of $a \in Z_N^*$ will satisfy $a^u \neq \pm 1\ mod\ N$ and $a^{2^i u} \neq -1\ mod\ N$ for $i \in \{1, \ldots, r-1\}$.

The RSA Assumption

The RSA experiment $RSA - inv_{A,Gen}(n)$:

1. Run $Gen(1^n)$ to obtain (N, e, d), where $\gcd\big(e, \phi(N)\big) = 1$ and $e \cdot d \equiv 1\ mod\ \phi(N)$.
2. Choose a uniform $y \in {Z^*}_N$.
3. A is given (N, e, y), and outputs $x \in {Z^*}_N$.
4. The output of the experiment is defined to be 1 if $x^e = y\ mod\ N$, and 0 otherwise.

Definition: The RSA problem is hard relative to Gen if for all ppt algorithms A there exists a negligible function neg such that

$$\Pr\big[RSA - inv_{A,Gen}(n) = 1\big] \leq neg(n).$$

Relationship between RSA and Factoring

Known:

- If an attacker can break factoring, then an attacker can break RSA.
  - Given p, q such that $p \cdot q = N$, can find $\phi(N)$ and d, the multiplicative inverse of $e \; mod \; \phi(N)$.
- If an attacker can find $\phi(N)$, can break factoring.
- If an attacker can find d such that $e \cdot d \equiv 1 \; mod \; \phi(N)$, can break factoring.

Not Known:

- Can every efficient attacker who breaks RSA also break factoring?

Due to the above, we have that the RSA assumption is a stronger assumption than the factoring assumption.

Cyclic Groups

For a finite group G of order m and $g \in G$, consider:

$$\langle g \rangle = \{g^0, g^1, \dots, g^{m-1}\}$$

$\langle g \rangle$ always forms a cyclic subgroup of G.

However, it is possible that there are repeats in the above list.

Thus $\langle g \rangle$ may be a subgroup of order smaller than m.

If $\langle g \rangle = G$, then we say that G is a cyclic group and that g is a generator of G.

Examples

Consider $Z^*{}_{13}$:

2 is a generator of $Z^*{}_{13}$:

2^0	1
2^1	2
2^2	4
2^3	8
2^4	$16 \rightarrow 3$
2^5	6
2^6	12
2^7	$24 \rightarrow 11$
2^8	$22 \rightarrow 9$
2^9	$18 \rightarrow 5$
2^{10}	10
2^{11}	$20 \rightarrow 7$
2^{12}	$14 \rightarrow 1$

3 is not a generator of $Z^*{}_{13}$:

3^0	1
3^1	3
3^2	9
3^3	$27 \rightarrow 1$
3^4	3
3^5	9
3^6	$27 \rightarrow 1$
3^7	3
3^8	9
3^9	$27 \rightarrow 1$
3^{10}	3
3^{11}	9
3^{12}	$27 \rightarrow 1$

Definitions and Theorems

Definition: Let G be a finite group and $g \in G$. The order of g is the smallest positive integer i such that $g^i = 1$.

Ex: Consider Z_{13}^*. The order of 2 is 12. The order of 3 is 3.

Proposition 1: Let G be a finite group and $g \in G$ an element of order i. Then for any integer x, we have $g^x = g^{x \bmod i}$.

Proposition 2: Let G be a finite group and $g \in G$ an element of order i. Then $g^x = g^y$ iff $x \equiv y \bmod i$.

More Theorems

Proposition 3: Let G be a finite group of order m and $g \in G$ an element of order i. Then $i \mid m$.

Proof:

- We know by the generalized theorem of last class that $g^m = 1 = g^0$.
- By Proposition 1, we have that $g^m = g^{m \bmod i} = g^0$.
- By the $\leftarrow$ direction of Proposition 2, we have that $0 \equiv m \bmod i$.
- By definition of modulus, this means that $i \mid m$.

Corollary: if G is a group of prime order p, then G is cyclic and all elements of G except the identity are generators of G.

Why does this follow from Proposition 3?

Theorem: If p is prime then ${Z^*}_p$ is a cyclic group of order $p - 1$.

Prime-Order Cyclic Groups

Consider ${Z^*}_p$, where p is a strong prime.

- Strong prime: $p = 2q + 1$, where q is also prime.
- Recall that ${Z^*}_p$ is a cyclic group of order $p - 1 = 2q$.

The subgroup of quadratic residues in ${Z^*}_p$ is a cyclic group of prime order q.