Modern Cryptography

600.442

Lecture #13

Dr. Christopher Pappacena

Fall 2013

Last Time

- The limitations of private-key cryptography
- Diffie-Hellman key exchange, informally
- The discrete log problem
- Number theory

Group Exponentiation

If G is a group with operation $\circ$, we define g^m to be the result of applying the group operation to g a total of m times:

$$g^m = g \circ \cdots \circ g \ (m \text{ times}).$$

If the group operation in G is addition we write mg in place of g^m.

All the usual rules of exponentiation hold: $g^0 = e$, $g^m \circ g^n = g^{m+n}$, and $g^{-m} = (g^{-1})^m$.

Proposition: g^m can be computed in $O(\|m\|)$ group operations.

This is known as "double and add" or "square and multiply".

Lagrange's Theorem

The following result from group theory is very important to cryptography:

Theorem: Let G be a finite group, say $|G| = n$. Then $g^n = e$ for every $g \in G$.

Proof: (G abelian) Multiplication by g is permutation of the elements of G. If we write $G = \{g_1, \ldots, g_n\}$ then

$$g_1 \circ \cdots \circ g_n = (g \circ g_1) \circ \cdots \circ (g \circ g_n) = g^n \circ g_1 \circ \cdots \circ g_n$$

Canceling $g_1 \circ \cdots \circ g_n$ gives $g^n = e$.

Cyclic Groups

A group G is called *cyclic* if there exists an element g, called a *generator* for G, such that every element of G is a power of g. We write $G = \langle g \rangle$.

Example: The additive group $\mathbb{Z}_N$ is cyclic with generator 1.

Example: The additive group $\mathbb{Z}_{10}$ is cyclic with generator 3 (board).

If G is a group and $g \in G$, then the set of powers of g forms a subgroup of G called the *cyclic subgroup generated by* g. The *order* of g is the smallest positive m with $g^m = e$.

Example: The element 2 has order 5 in $\mathbb{Z}_{10}$ since $\langle 2 \rangle = \{0, 2, 4, 6, 8\}$.

Important Facts About Cyclic Groups

- If g has order m then $g^x = g^y$ if and only if $x = y \pmod{m}$.
- If G has order n and $g \in G$ has order m, then m divides n.
- If G has prime order p then G is cyclic.
- If p is a prime integer then $\mathbb{Z}_p^*$ is cyclic of order $p - 1$.

Example: $\mathbb{Z}_7^*$ is generated by 3 (board).

The Discrete Logarithm Problem

If $G = \langle g \rangle$ is a cyclic group of order n, then every $h \in G$ is a power of g: $h = g^x$ for some $x \in \{0, \ldots, n-1\}$.

The *discrete logarithm problem* is to find x, given h.

The difficulty of the discrete logarithm problem does not depend on G as an *abstract* group; rather, it depends on how G is represented.

Example: The group $\mathbb{Z}_p^*$ is a cyclic group with generator 3 for $p =$ 2147483647. The group $\mathbb{Z}_{p-1}$ under addition is also a cyclic group of order $p-1$, with generator 1.

The discrete logarithm of 2041619674 in the first group is 62 and in the second group it is 2041619674.

The Discrete Logarithm Experiment

Let $\mathcal{G}$ be an algorithm which, on input n, returns a cyclic group G of order q (with $\|q\| = n$) and a generator g. Consider the following experiment:

- Run $\mathcal{G}(n)$ to obtain (G, q, g).
- Choose $h \leftarrow G$ uniformly at random. This can be done by choosing $y \leftarrow \{0, \ldots, q-1\}$ uniformly at random and setting $h = g^y$.
- $\mathcal{A}$ is given (G, q, g, h) and outputs $x \in \{0, \ldots, q-1\}$.
- We say $\mathcal{A}$ *succeeds* if $h = g^x$, otherwise $\mathcal{A}$ *fails*.

We write $\mathsf{DLog}_{\mathcal{A},\mathcal{G}}(n) = 1$ if $\mathcal{A}$ succeeds, and 0 if $\mathcal{A}$ fails.

Definition: The *discrete logarithm problem is hard relative to* $\mathcal{G}$ if, for all PPT adversaries $\mathcal{A}$, we have

$$\Pr[\mathsf{DLog}_{\mathcal{A},\mathcal{G}}(n) = 1] \leq \mathtt{negl}(n)$$

for some negligible function $\mathtt{negl}$ of n.

Example: On input n, $\mathcal{G}$ selects a prime p with $\|p\| = n$ such that $(p-1)/2$ prime, finds a generator g for $\mathbb{Z}_p^*$, and returns $(\mathbb{Z}_p^*, p-1, g)$.

The discrete logarithm problem is widely believed to be hard relative to $\mathcal{G}$.

The Diffie-Hellman Problem

In the original Diffie-Hellman protocol, the shared secret is g^{xy} and the eavesdropper observes g^x and g^y. The difficulty of recovering the former from the latter is known as the *Diffie-Hellman problem*.

Formally, there are two variants:

- Computational Diffie-Hellman (CDH): Given g^x and g^y, compute g^{xy}.

- Decisional Diffie-Hellman (DDH): Given a triple (g^x, g^y, h), decide whether or not $h = g^{xy}$.

If we can solve the discrete log problem in G then we can solve CDH and DDH, and if we can solve CDH then we can solve DDH.

(These are both problems on HW 7.)

So DDH is the strongest of the three problems.

The DDH Problem, Formally

Definition: We say that the *DDH problem is hard realative to* $\mathcal{G}$ if for all PPT algorithms $\mathcal{A}$, there exists a negligible function $\texttt{negl}(n)$ such that

$$|\,\mathsf{Pr}[\mathcal{A}(\mathcal{G}, g, g^x, g^y, g^{xy}) = 1] - \mathsf{Pr}[\mathcal{A}(\mathcal{G}, g, g^x, g^y, h)]| \leq \texttt{negl}(n)$$

where $x, y \leftarrow \{0, \ldots, q-1\}$ and $h \leftarrow \mathcal{G}$.

Key Exchange, Formally

Consider the following *key exchange experiment* $\mathsf{KE}^{\mathsf{eav}}_{\mathcal{A},\Pi}(n)$:

- Two parties execute a key-exchange protocol Π with input n. The protocol produces a transcript of all messages sent between the two parties as well as a secret key k.
- A random bit $b \leftarrow \{0,1\}$ is chosen. If $b = 0$ set $\tilde{k} \leftarrow \{0,1\}^n$, otherwise set $\tilde{k} = k$.
- $\mathcal{A}$ is given $\tilde{k}$ and the transcript and outputs a bit b'.
- We set $\mathsf{KE}^{\mathsf{eav}}_{\mathcal{A},\Pi}(n) = 1$ if $b = b'$ and say that $\mathcal{A}$ *succeeds*; otherwise $\mathcal{A}$ *fails*.

Diffie-Hellman, Formally

- Given n, Alice runs $\mathcal{G}(n)$ to obtain (G, q, g).
- Alice chooses $x \leftarrow \{0, \ldots q-1\}$, sets $A = g^x$, and sends (G, q, g, A) to Bob.
- Bob chooses $y \leftarrow \{0, \ldots, q-1\}$, sets $B = g^y$, and sends B to Alice.
- The shared key is $k = B^x = A^y$ and the transcript is (G, q, g, A, B).

A Technical Detail

The definition of a key exchange protocol produces a shared secret key which is a bit string. The Diffie-Hellman protocol produces a shared secret element of the group G.

We need a way to extract bit strings from group elements.

In practice this is not too hard, since the group elements are represented by bit strings on a computer. Sometimes we have to be a bit careful because some of the individual bits which represent group elements may be biased.

Theorem: If the decisional Diffie-Hellman problem is hard relative to $\mathcal{G}$, then the Diffie-Hellman Key Exchange protocol is secure in the presence of an eavesdropper.

Proof: Board.

DDH being hard relative to $\mathcal{G}$ is exactly what is needed to make the proof work out.

Note that this is a strictly stronger assumption than the discrete logarithm problem or the computational Diffie-Hellman problem, originally identified by Diffie and Hellman.

Surprisingly, the DDH problem is actually *easy* relative to $\mathcal{G} = \mathbb{Z}_p^*$, the group we introduced earlier for which the discrete log problem is believed to be hard!

This suggests that the DDH problem is *strictly* stronger than the discrete log problem.

Quadratic Residues

Let p be a prime and a an element of $\{1, \ldots, p-1\}$. We say that a is a *quadratic residue* if there exists x such that $x^2 = a \pmod{p}$. Otherwise a is a *quadratic nonresidue*.

Example: For $p = 11$ the quadratic residues are $\{1, 3, 4, 5, 9\}$ and the quadratic nonresidues are $\{2, 6, 7, 8, 10\}$.

Theorem: There are exactly $(p-1)/2$ quadratic residues and exactly $(p-1)/2$ quadratic nonresidues modulo p.

Define the *Legendre Symbol* $\left(\frac{a}{p}\right)$ by $\left(\frac{a}{p}\right) = 1$ if a is a quadratic residue modulo p and $\left(\frac{a}{p}\right) = -1$ if a is a quadratic nonresidue.

Quadratic Residues and DDH

Basic facts about Legendre Symbols:

- $\left(\frac{a}{p}\right)$ can be computed in polynomial time in $\|p\|$.
- $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

If g is a generator for $\mathbb{Z}_p^*$ then $\left(\frac{g^x}{p}\right) = 1$ if and only if x is even. Using this fact we can determine $\left(\frac{g^{xy}}{p}\right)$ from g^x and g^y.

This means we can use Legendre Symbols to solve the DDH problem in $\mathbb{Z}_p^*$ with probability 3/4 – details on board.

There is a simple fix for this - the set of all quadratic residues forms a cyclic subgroup of $\mathbb{Z}_p^*$ of order $(p-1)/2$, so we modify $\mathcal{G}$ to return a generator for this group:

On input n, $\mathcal{G}$ selects a prime p with $\|p\| = n$ such that $(p-1)/2$ is prime. It selects a generator h for $\mathbb{Z}_p^*$, sets $g = h^2$, sets G equal to the group of quadratic residues modulo p, and returns $(G, (p-1)/2, g)$.

The DDH problem, CDH problem, and discrete log problem are all believed to be hard relative to this $\mathcal{G}$.