14.3: Decisional Diffie-Hellman Problem

The Diffie-Hellman protocol is parameterized by the choice of cyclic group \( G \) (and generator \( g \)). Transcripts in the protocol consist of \((g^a, g^b)\), where \( a \) and \( b \) are chosen uniformly. The key corresponding to such a transcript is \( g^{ab} \). The set of possible keys is the cyclic group \( G \).

Let us substitute the details of the Diffie-Hellman protocol into the KA security libraries. After simplifying, we see that the security of the Diffie-Hellman protocol is equivalent to the following statement:

We have renamed the libraries to \( \mathcal{L}_{dh\text{-}real} \) and \( \mathcal{L}_{dh\text{-}rand} \). In \( \mathcal{L}_{dh\text{-}real} \) the response to QUERY corresponds to a DHKA transcript \((g^a, g^b)\) along with the corresponding “correct” key \( g^{ab} \). The response in \( \mathcal{L}_{dh\text{-}real} \) corresponds to a DHKA transcript along with a completely independent random key \( g^c \).

Definition \((\PageIndex{1})\)

The **decisional Diffie-Hellman (DDH) assumption** in a cyclic group \( G \) is that \( \mathcal{L}_{dh\text{-}real} \cong \mathcal{L}_{dh\text{-}rand} \) (libraries defined above).

Since we have defined the DDH assumption by simply renaming the security definition for DHKA, we immediately have:

**Claim 14.6:**
The DHKA protocol is a secure KA protocol if and only if the DDH assumption is true for the choice of $\mathcal{G}$ used in the protocol.

**For Which Groups does the DDH Assumption Hold?**

So far our only example of a cyclic group is $\mathbb{Z}_p^*$, where $p$ is a prime. Although many textbooks describe DHKA in terms of this cyclic group, it is not a good choice because the DDH assumption is demonstrably false in $\mathbb{Z}_p^*$. To see why, we introduce a new concept:

**Claim 14.7: Euler Criterion**

If $p$ is a prime and $X = g^x \in \mathbb{Z}_p^*$, then $X^{p-1} \equiv_p (-1)^x$.

Note that $(-1)^x$ is 1 if $x$ is even and $-1$ if $x$ is odd. So, while in general it is hard to determine $x$ given $g^x$, Euler’s criterion says that it is possible to determine the parity of $x$ (i.e., whether $x$ is even or odd) given $g^x$.

To see how these observations lead to an attack against the Diffie Hellman protocol, consider the following attack:

<table>
<thead>
<tr>
<th>$A$:</th>
</tr>
</thead>
<tbody>
<tr>
<td>$(A, B, C) \leftarrow \text{QUERY}()$</td>
</tr>
<tr>
<td>return $1 \equiv_p C^{p-1}$</td>
</tr>
</tbody>
</table>

Roughly speaking, the adversary returns true whenever $C$ can be written as $g$ raised to an even exponent. When linked to $\mathcal{D}_{\text{dh-real}}$, $C = g^{ab}$ where $a$ and $b$ are chosen uniformly. Hence $ab$ will be even with probability $3/4$. When linked to $\mathcal{D}_{\text{dh-rand}}$, $C = g^c$ for an independent random $c$. So $c$ is even only with probability $1/2$. Hence the adversary distinguishes the libraries with advantage $1/4$.

Concretely, with this choice of group, the key $g^{ab}$ will never be uniformly distributed. See the exercises for a slightly better attack which correlates the key to the transcript.

**Quadratic Residues.**

Several better choices of cyclic groups have been proposed in the literature. Arguably the simplest one is based on the following definition:

**Definition** \(\mathcal{G}^{\ast}_n\)

A number $X \in \mathbb{Z}_n^*$ is a **quadratic residue modulo** $n$ if there exists some integer $Y$ such that $Y^2 \equiv_n X$. That is, if $X$ can be obtained by squaring a number mod $n$. Let $\mathcal{Q}_n^\ast \subseteq \mathbb{Z}_n^*$ denote the set of quadratic residues mod $n$.

For our purposes it is enough to know that, when $p$ is prime, $\mathcal{Q}_p^\ast$ is a cyclic group with $(p - 1)/2$ elements (see the exercises). When both $p$ and $(p - 1)/2$ are prime, we call $p$ a **safe prime** (and call $(p - 1)/2$ a **Sophie Germain prime**). To the best of our knowledge the DDH assumption is true in $\mathcal{Q}_p^\ast$ when $p$ is a safe prime.