CSE 5852: Problem Set 6

Due: November 7, 2016

This homework looks at some of the power of the discrete log and Diffie-Hellman. Please be clear what definitions are used in your proofs. Also since there are many definitions feel free to copy and paste from the problem set latex source. Recall we have three different assumptions related to the group $\mathbb{Z}_p^*$:

Assumption 1. *For any PPT $\mathcal{A}$, there exists a negligible ϵ such that for a random n-bit p and its generator and select a random $x \in \mathbb{Z}_p^*$,*

$$\Pr[\mathcal{A}(1^n, p, g, g^x \mod p) = x] \leq \epsilon(n).$$

Assumption 2 (Computational Diffie-Hellman Assumption)**.** *For any PPT $\mathcal{A}$, there exists a negligible ϵ such that for a random n-bit p and its generator and select a random $x, y \in \mathbb{Z}_p^*$,*

$$\Pr[\mathcal{A}(1^n, p, g, g^x \mod p, g^y \mod p) = g^{xy}] \leq \epsilon(n).$$

Assumption 3 (Decisional Diffie-Hellman Assumption)**.** *For any PPT $\mathcal{A}$, there exists a negligible ϵ such that for a random n-bit p and its generator and select a random $x, y, z \in \mathbb{Z}_p^*$,*

$$\Pr[\mathcal{A}(1^n, p, g, g^x, g^y, g^{xy}) = 1] - \Pr[\mathcal{A}(1^n, p, g, g^x, g^y, g^z) = 1] \leq \epsilon(n).$$

1 Diffie-Hellman Assumptions (30 pts)

Show the following theorems:

Theorem 1. ***10 pts*** *If there exists PPT $\mathcal{A}$ that breaks the discrete logarithm assumption with an inverse polynomial probability then there exists PPT $\mathcal{A}'$ that breaks the computational DH assumption with an inverse polynomial probability. (That is, computational DH implies discrete log.)*

Theorem 2. ***20 pts*** *If there exists PPT $\mathcal{A}$ that breaks the computational DH assumption with an inverse polynomial probability then there exists PPT $\mathcal{A}'$ that breaks the decisional DH assumption with an inverse polynomial probability. (That is, decisional DH implies computational DH.)*

Hint: The adversary that breaks the computational DH problem only takes p, g, g^x, g^y as input. How can you use their response to check the last value received by $\mathcal{A}'$?

2 Variants of Diffie-Hellman (35 pts)

In class we showed that Diffie-Hellman could be used once. In this problem we will show that it is okay to reuse a Diffie-Hellman element. Consider the following extension to the problem:

Assumption 4 (2-time Decisional Diffie-Hellman Assumption)**.** *For any PPT $\mathcal{A}$, there exists a negligible ϵ such that for a random n-bit p and its generator and select a random $x, y, z, r_1, r_2 \in \mathbb{Z}_p^*$,*

$$\Pr[\mathcal{A}(1^n, p, g, g^x, g^y, g^z, g^{xy}, g^{xz}) = 1] - \Pr[\mathcal{A}(1^n, p, g, g^x, g^y, g^z, g^{r_1}, g^{r_2}) = 1] \leq \epsilon(n).$$

Show the following theorems:

Theorem 3. ***10 pts*** *If there exists PPT $\mathcal{A}$ that breaks the breaks the DDH assumption with an inverse polynomial probability then there exists PPT $\mathcal{A}'$ that breaks the 2-time DDH assumption with an inverse polynomial probability. (That is, 2-time DDH implies DDH.)*

Theorem 4. ***25 pts*** *If there exists PPT $\mathcal{A}$ that breaks the breaks the 2-time DDH assumption with an inverse polynomial probability then there exists PPT $\mathcal{A}'$ that breaks the DDH assumption with an inverse polynomial probability. (That is, DDH implies 2-time DDH.)*

Hint: Call the setting where $\mathcal{A}$ is presented with $(g^x, g^y, g^z, g^{xy}, g^{yz})$, $\texttt{exp} - \texttt{0}$ and the setting where $\mathcal{A}$ is presented with $(g^x, g^y, g^z, g^{r_1}, g^{r_2}$, $\texttt{exp} - \texttt{2}$. Your argument should consider an intermediate experiment $\texttt{exp} - \texttt{1}$ (hybrid) where the adversary is presented with the values $(g^x, g^y, g^z, g^{xy}, g^{r_2})$. Your algorithm needs to function differently in the two cases of the hybrid argument.

3 El Gamal (35 pts)

Recall our definition of indistinguishable encryptions and El Gamal.

Definition 1. *The El-Gamal public-key encryption scheme is as follows:*

- $\mathsf{Gen}(p, g)$*:*

  Select x from $\mathbb{Z}_p^*$.

  Compute g^x.

  Output $pk = g^x, sk = x$.

- $\mathsf{Enc}(g^x, m \in \{0, 1\})$*:*

  Select $y \in \mathbb{Z}_p^*$ compute g^y

  If $m = 0$ send $c = (g^y, (g^x)^y)$ if $m = 1$ send $c = (g^y, g(g^x)^y = g^{xy+1})$.

- $\mathsf{Dec}(x, c)$*:*

  Parse c as $g^y = g^z$.

  Compute $(g^y)^x$ and then compute $h = (g^{xy})^{-1}$.

  If $hg^z = 1$ output 0, if $hg^z = g$ output 1.

Definition 2. *A public-key cryptosystem for* 1*-bit messages is polynomially-secure if for all polynomial time* $\mathcal{A}$ *there exists a negligible function* $\epsilon(n)$ *such that*

$$|\Pr_{pk,sk,\mathsf{Enc}}[\mathcal{A}(pk,\mathsf{Enc}(pk,0))=1]-\Pr_{pk,sk,\mathsf{Enc}}[\mathcal{A}(pk,\mathsf{Enc}(pk,1))=1]|<\epsilon(n).$$

Show that the ElGamal encryption scheme is polynomially-secure under the DDH assumption. That is, show that if there exists a PPT $\mathcal{A}$ that distinguishes between encryptions of 0 and encryptions of 1 then there is an algorithm that breaks the DDH problem.

Your proof should be by the hybrid argument. Denote by $\texttt{exp}-\texttt{0}$ the setting where $\mathcal{A}$ receive g^x, g^y, g^{xy} and $\texttt{exp}-\texttt{3}$ the setting where $\mathcal{A}$ receives $g^x, g^y, g\cdot g^{xy}$. Consider two hybrids $\texttt{exp}-\texttt{1}$ where $\mathcal{A}$ receives g^x, g^y, g^{r_1} and $\texttt{exp}-\texttt{2}$ where $\mathcal{A}$ receives $g^x, g^g, g\cdot g^{r_1}$.

- **15 pts** Show a $\mathcal{A}'$ that breaks DDH when $\mathcal{A}$ is able to distinguish between $\texttt{exp}-\texttt{0}$ and $\texttt{exp}-\texttt{1}$ with nonnegligible probability.
- **5 pts** What is the distance between $\texttt{exp}-\texttt{1}$ and $\texttt{exp}-\texttt{2}$? Why?
- **15 pts** Show a $\mathcal{A}'$ that breaks DDH when $\mathcal{A}$ is able to distinguish between $\texttt{exp}-\texttt{2}$ and $\texttt{exp}-\texttt{3}$ with nonnegligible probability.