CSE 107 Discussion 2/28

Activity 1: Additive Diffie-Hellman (left over from last time)

In lecture we saw the Diffie-Hellman key exchange protocol: There is a public group $\mathbf{Z}_p^*$ for a prime p, and a public generator g of $\mathbf{Z}_p^*$. Alice and Bob proceed according to:

1. Alice chooses secret $x \xleftarrow{\$} \mathbf{Z}_{p-1}$ and Bob chooses secret $y \xleftarrow{\$} \mathbf{Z}_{p-1}$.
2. Alice computes public $X \leftarrow g^x \bmod p$ and Bob computes public $Y \leftarrow g^y \bmod p$.
3. X and Y are sent over a public channel, so that Alice and Bob know both.
4. Now Alice and Bob can both compute the shared secret $g^{xy} \bmod p$. Alice computes $Y^x \bmod p$ and Bob computes $X^y \bmod p$.

The *Computational Diffie-Hellman* (CDH) problem says that an eavesdropper only knowing X, Y cannot efficiently compute g^{xy}.

Let's consider a variant of the above protocol, which we call *Additive Diffie-Hellman*. Only Step (4) is changed: the shared secret will now be g^{x+y} instead of g^{xy}.

(a) Can Alice and Bob still agree on a shared secret in Step (4)? What does Alice compute, and what does Bob?

(b) Is additive DH secure against an eavesdropper who only knows X, Y? Why or why not?

Activity 2: Easy vs hard operations (left over from last time)

Stepping back to a more general question, which of the following operations can be done efficiently, and which are hard? Let p be a prime and g a generator of $\mathbf{Z}_p^*$.

(i) Given $a, b \in \mathbf{Z}_{p-1}$ compute $a + b \bmod (p-1)$

(ii) Given $A, B, C \in \mathbf{Z}_p^*$ compute $A \cdot B \cdot C \bmod p$

(iii) Given $D \in \mathbf{Z}_p^*$ compute $D^{-1} \bmod p$

(iv) Given g^a, g^b for $a, b \in \mathbf{Z}_{p-1}$, compute $g^{ab} \bmod p$

(v) Given b, g^a, g^b for $a, b \in \mathbf{Z}_{p-1}$, compute $g^{ab} \bmod p$

(vi) Given b, g^a, g^b for $a, b \in \mathbf{Z}_{p-1}$, compute $a \bmod (p-1)$

(vii) Given g^a, g^b for $a, b \in \mathbf{Z}_{p-1}$, compute $(a + b) \bmod (p-1)$

(viii) Given g^a, g^b for $a, b \in \mathbf{Z}_{p-1}$, compute $g^{a+b} \bmod p$

Activity 3: Easy vs hard operations, part 2!

Now let's work mod $N = pq$ for large primes p and q. Which of the following operations can be done efficiently, and which are hard? Unless stated otherwise, assume you don't know p and q but do know N.

1. take cube roots mod N, i.e., find $x \in \mathbf{Z}_N^*$ given $x^3 \bmod N$
2. take 65537th roots mod N, i.e., find $x \in \mathbf{Z}_N^*$ given $x^{65537} \bmod N$
3. take 65537th roots mod N when you know p and q
4. given x, find $x^{65537} \bmod N$
5. given x, find $x^{-1} \bmod N$
6. given $x^e \bmod N$ and $y^e \bmod N$, find $(xy)^e \bmod N$
7. given $x^e \bmod N$ and $y^e \bmod N$, find $(x+y)^e \bmod N$
8. given $x^e \bmod N$ and $x^f \bmod N$, find $x^{e+f} \bmod N$
9. break RSA if everyone uses the same e but their own d and N