Section 2.3: Diffie-Hellman Key Exchange (p65)

(2.3A) Problem: Alice and Bob want to share a secret key for use in a symmetric cipher, but their only means of communication is insecure (ie, Eve can see all information that is exchanged).

- The difficulty of the DLP provides a solution to this problem and is the basis of the Diffie-Hellman Key Exchange.

(2.3B) Diffie-Hellman Key Exchange Protocol

1. **Public Parameter Creation**
   - Alice & Bob: choose large prime \( p \) & a primitive root \( g \) of \( \mathbb{F}_p \) (where \( 2 \leq g \leq p-2 \))

2. **Private Computations**
   - Alice: chooses a secret integer \( a \), then computes \( A \equiv g^a \) (mod \( p \))
   - Bob: chooses a secret integer \( b \), then computes \( B \equiv g^b \) (mod \( p \))

3. **Public Exchange of Values (over the insecure communication channel)**
   - Alice: sends \( A \) to Bob
   - Bob: sends \( B \) to Alice

4. **Further Private Computations**
   - Alice: computes \( A' \equiv B^a \) (mod \( p \))
   - Bob: computes \( B' \equiv A^b \) (mod \( p \))

(2.3C) The two values Alice & Bob compute at the end, \( A' \) and \( B' \), are actually the same value:

\[
A' = B^a = (g^b)^a = g^{ab} = (g^a)^b = A^b = B' \pmod{p}
\]

- This value, \( k = A' = B' \), will serve as the secret key for their symmetric cipher.

(2.3D) Ex: Alice and Bob agree to use \( p = 1193 \) and a primitive root \( g = 3 \). Alice chooses the secret key \( a = 69 \) and Bob chooses the secret key \( b = 96 \). Using the DHK exchange, find the shared secret key \( k \).
(2.3E) Why would $g = p - 1$ be a bad choice when performing a D-H Key Exchange?

(2.3F) Even though Eve has access to $p$, $g$, $A$, & $B$, she would still need to be able to solve either (from the previous example) $3^a \equiv 919 \pmod{1193}$ for $a$ or $3^b \equiv 30 \pmod{1193}$ for $b$ in order to figure out the shared secret key $k$.

(2.3G) Solving the DLP is one way Eve could obtain $k$, but the DLP isn’t the precise problem Eve encounters in this scenario. The security of $k$ rests on the difficulty of the following, potentially easier, problem:

- The **Diffie-Hellman Problem (DHP)** is the problem of computing the value of $g^{ab} \pmod{p}$ from the known values of $g^a \pmod{p}$ and $g^b \pmod{p}$, where $p$ is a prime and $g$ is an integer.

(2.3H) The DHP is definitely not harder than the DLP (solving the DLP would also solve the DHP), but it is unknown if the converse is true.

Exercises: 2.6