# Diffie-Hellman Key Exchange

CP341 / MA340 – Cryptography

Block 8, Spring 2019

1. Write a short program that implements fast exponentiation *without* storing powers. (Hint: Use the binary expansion of the exponent from left to right.)

2. Write a short program that implements the Diffie-Hellman key exchange protocol by completing the following steps.

   a. Write a function that chooses a prime $p$ of a given bit size. Use the `primitive_root` function in Sage or write a function in Python that finds a generator $g$ for the prime $p$. Return both $p$ and $g$.

   b. Write a function that choose a random number $a$ between 2 and $p-2$. Use the fast exponentiation algorithm from the previous problem to calculate $A \equiv g^a \pmod{p}$. Return both $a$ and $A$.

   c. Write a function that simulates Alice and Bob's calculations to find the Diffie-Hellman key $K$. Verify that Alice and Bob's keys match, and if so, return the common key $K$.

3. Write a short program that computes the discrete logarithm by brute force. Use the `next_prime` function in Sage to find the next prime $p$ greater than $2^{10}$, $2^{20}$, and $2^{30}$. Use the `primitive_root` function in Sage to find a base number $g$ which generates $(\mathbb{Z}/p\mathbb{Z})^\times$. Finally, run and time your Sage code to compute the discrete logarithm $a$ for each of the three primes and three primitive roots:

$$g^a \equiv 101 \pmod{p}$$

4. Use the `log` command to use Sage's discrete logartihm to time computing the discrete logarithm problem for the next "safe primes" (that is, $p$ is prime and $\frac{p-1}{2}$ is prime) greater than $2^{20}$, $2^{40}$, $2^{60}$, $2^{80}$, and $2^{100}$.

$$g^a \equiv 101 \pmod{p}$$

   Extrapolate how long it would take to compute the discrete logarithm for a prime of size $2^{1000}$.

5. By choosing an "unsafe prime", use the discrete logarithm function in Sage to show that the time to compute a discrete logarithm dramatically decreases. For example, let $p = 2^{100} + 1095$ and time the following discrete logarithm problem.

$$g^a \equiv 101 \pmod{p}$$

   What makes this particular choice of $p$ insecure?