Worksheet 13: Diffie-Hellman Key Exchange

Problem 1. Do this problem (and only this problem) by hand. Let $p = 11$ and $g = 2$, so that g is a primitive root of p.

(a) Calculate $g^8 \bmod p$ quickly using binary exponentiation.

(b) Find the smallest positive integer k such that $g^k \equiv 9 \bmod p$.

Note. For the rest of these problems, use SageMath (or another programming language of your choice). If you haven't installed SageMath on your computer, you can use `https://sagecell.sagemath.org/`.

Problem 2. Your friend Kwame would like to exchange a secret key with you using the Diffie-Hellman key exchange. You've publicly chosen the following values of `p` and `g`. Kwame secretly chooses a random integer `m` and then sends you `gm`, which is the `m`th power of `g` modulo `p`. You've chosen the random integer `n` below.

```
p = 712440987745420643362226282174114251
g = 7
gm = 580748625707819
n = 1423435384058
```

(a) What number do you send to Kwame?

(b) What is your shared secret key?

(c) How would Kwame compute the same shared secret key?

(d) Can you figure out what number `m` Kwame chose? *Note*. The numbers are small enough that it's *possible* for modern computers to figure this out. On my computer, it takes about 45 seconds — but SageMathCell times out before the calculation completes.

Solution. For (a), compute `Mod(g, p)^n`.

For (b), compute `Mod(gm, p)^n`.

For (c), compute `log(Mod(gm, p), Mod(g, p))`.

Problem 3. Arnold and Therein would like to share a secret key using the Diffie-Hellman key exchange. They publicly choose the following values of `p` and `g`. Arnold chooses a random integer `m` and sends Therein `gm`, which is the `m`th power `gm` of `g` modulo `p`. Therein chooses a random integer `n` and sends Arnold `gn`, which is the `n`th power of `g` modulo `p`.

```
p = 929779317878443
g = 3
gm = 38934892384
gn = 23948293048
```

Unfortunately for Arnold and Therein, you're a hacker who's listening in on their exchange — and they chose `p` to be far too small! What is their shared secret key?

Solution. Either of the following will work:

```
# Method 1
m = log(Mod(gm, p), Mod(g, p))
Mod(gn, p)^m

# Method 2
n = log(Mod(gn, p), Mod(g, p))
Mod(gm, p)^n
```

Problem 4. Varshā and Yǔ would like to share a secret key using the Diffie-Hellman key exchange. They publicly choose the following values of `p` and `g`. Unfortunately for Varshā and Yǔ, you're a hacker who's able to intercept their messages and pass on messages assuming a false identity; in other words, you're able to conduct a man-in-the-middle attack! You choose the random integer `t` below.

```
p = 1051018751114873289603934048438886470920726667
g = 3
t = 8791824433693936526410451922225
```

(a) Find the `t`th power of `g` modulo `p`.

(b) Varshā chooses a random integer `m` and tries to send Yǔ the number `gm` below, which is the `m`th power of `g` mod `p`. You intercept Varshā's message before it gets to Yǔ, and then send a modified message to Yǔ impersonating Varshā. What is the message you send to Yǔ?

```
gm = 52683272015416615800376683673390725049486384
```

(c) Yǔ chooses a random integer `n` and tries to send Varshā the number `gn` below, which is the `n`th power of `g` mod `p`. You again intercept Yǔ's message before it gets to Varshā, and then send a modified message to Varshā impersonating Yǔ. What is the message you send to Varshā?

```
gn = 22089373621730650431507258176281354479255011
```

(d) What does Varshā think her secret key with Yǔ is?

(e) What does Yǔ think her secret key with Varshā is?

Solution. The answer to (a), (b), and (c) is `Mod(g, p)^t`.

The answer to (d) is `Mod(gm, p)^t`.

The answer to (e) is `Mod(gn, p)^t`.