Gloire Rubambiza - MTH 312 - Assessment 4 Reflection

1. What went well

- Overall, the assessment overall went very well.
- The pre-assessment preparation was instrumental in letting me focus on learning targets that can be hit inside and outside the classroom. In other words, I hit longer targets such as the `Chinese Remainder Theorem` and `RSA` in the preparation phase and tackled smaller targets such as `Diffie-Hellman` and `Elgamal` during the in-class assessment.
- I did incredibly well for being in a noisy environment as the rest of the class was focusing on their group projects.
- Because of the pre-assessment preparation, I now have a better understanding and appreciation for repeated squaring based on my solution to the `RSA` problem.

2. Areas of improvement

- I made a calculation error on question 5.a mostly because I had written the notes for Elgamal encryption without the modular part i.e. `n = m * B^r` instead of `m * B^r mod p`. I will improve upon this in my revisions for the assessment.
- In hindsight, I spent a ton of time on repeated squaring for the RSA when I could have used the programs we built in class for repeated squaring. While the calculations were error prone, it was good practice with modular exponentiation.
- I still do not have a strong grasp on the features of Pohlig-Hellman that make it viable for the three pass protocol.

Gloire Rubambiza
04/21/2018
MTH 312 - 01

Assessment 4 - Revisions

5. a) $m = 14297$, $p = 33083$, $g = 186$, $B = 21866$

Nonce $(r) = 3$

$R = g^r = 186^3 = \boxed{6,434,856}$

$n = m \cdot B^r \bmod p = 14297 \cdot 21866^3 \bmod 33083$

$= 14297 \cdot 15792 \bmod 33083$

$n = \boxed{19832}$

Send n, R

Gloire Rubambiza
04/21/2018
MTH 312 - 01

Assessment 4 - Revisions

7) The Pohlig-Hellman Cipher can be used to implement the three pass protocol by sharing a large prime p.. What is secret to each party are two numbers e and d such that $\gcd(e, p-1) = 1$ and $(d \cdot e) \bmod p-1 = 1$.

The features that make P.H a viable choice are:

- The composition of decimation ciphers yields a decimation cipher: the encryption processes of Alice and Bob do not interfere with each other.
- Decimation ciphers are commutative: the encryption and decryption orders of both parties can be rearranged and undone.
- P.H does not require shared secret keys.