Gloire Rubambiza - MTH 312 - Assessment 2 Reflection

1. What went well

- Although it took me almost half the assessment period, I successfully enciphered and deciphered text using the Affine Shift cipher, especially the translation using modular arithmetic. It worth noting that, after deciphering text correctly, I am getting comfortable with the idea that deciphered text does not always have to make sense initially.
- Repeated squaring is much more intuitive to me. Realizing that every power can be written as a power of 2 solidified the concept.

2. Areas of improvement

- I got careless with the XOR operation because I was running out of time. I understand the concept, I just got carried away trying to move on to the next question.
    - Deeper connection: The XOR operation is popular because the operation easily undoes itself. In other words, a single XOR with the correct key is what is need to undo a message that was encrypted using an XOR operation.
- Similar to the XOR operation question, I rushed through the question on the ADFVGX cipher.
- To correct the carelessness, I plan to spend a bit more time on each question and reserve 5 minutes at the end of the assessment to review my work before submission.

Gloire Rubambiza
03/11/2018
MTH 312

In Class Assessment 2 - Revision - Question 9

q-b) XOR 1110 | 0111 | 1110 | 0011
1010 1000 1010 1000
cipher = 0100 1111 0100 1011

Gloire Kubamba
03/11/2018
MTH 312

In-Class Assessment 2- Revision- Question

5.a) Clear text: SPRING

Matching text: AGDGXAXDAAVG

B	R	E	A	K
A	G	D	G	X
A	X	D	A	A
V	G			

A	B	E	K	R
G	A	D	X	G
A	A	D	A	X
	V			G

Encrypted: GAAAVDDXAGXG

Gloire Rubambiza
03/11/2018
MTH 312

In-class Assessment 2 - Revisions

1. a) Determine whether 4 is a primitive root modulo 7 and explain your result

$4^6 \bmod 7 = 1$ *
$4^5 \bmod 7 = 2$
$4^4 \bmod 7 = 4$
$4^3 \bmod 7 = 1$ *
$4^2 \bmod 7 =$
$4^1 \bmod 7 =$

=> Despite $4^6 \bmod 7 = 1$, 4 is not a primitive root modulo 7 because $4^k \bmod 7 = 1$ for any k smaller than 6 i.e. 3.

b) Determine whether 5 is a primitive root modulo 7 and explain your result

$5^6 \bmod 7 = 1$
$5^5 \bmod 7 = 3$
$5^4 \bmod 7 = 2$
$5^3 \bmod 7 = 6$
$5^2 \bmod 7 = 4$
$5^1 \bmod 7 = 5$

=> 5 is a primitive root modulo 7 because $5^6 \bmod 7 = 1$ and $5^k \bmod 7 \neq 1$ for any k less than 6.