

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

$$\begin{array}{r} \text{q-b) XOR } 1110 \mid 0111 \mid 1110 \mid 1001 \\ \underline{1010 \mid 1000 \mid 1010 \mid 1000} \\ \text{cipher} = 0100 \mid 1111 \mid 0100 \mid 1011 \end{array}$$

In-Class Assessment 2 - Revision - Question

5.a) Clear text: SPRING

Matching text: AGDGXAXDAAVG

B	R	E	A	X
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: GA AAVDDXAGXG