Gloire Rubambiza - Self Assessment - Portfolio Review 4

- Based on my assessment of my provisional portfolio, I demonstrate proficiency in class outcomes at the B+ level.

- In addition to connecting the course to the outside world, I have shown the ability to develop and solve challenging problems independently. The evidence is as follows:
    - In Ada Lovelace: An Analysis of the Life of the Earliest Computer Programmer, I connect Ada Lovelace's childhood to my knowledge from my issues course on Health Psychology.
    - In question 6 of the first in-class assessment, I develop the problem by showing the scaffolding for converting a number from base 16 to binary.
    - In question 9 of the first assessment and questions 4 and 7 of the second assessment, I solve error-prone problems such as the Vigenere cipher, repeated squaring and Affine Shift translation, and the Router cipher with minimal support.
    - In all reading summaries, I show adequate connections between our class and the real world. For instance, the continued secrecy of cryptographic advancements by governments in the 19th century (Babbage in England) and 21st century (NSA in the USA).

- I demonstrate advanced reasoning, a high level of intellectual curiosity, and mathematical thinking - with evidence as follows:
    - In question 7 of the second assessment, in an attempt to save computation time, I check whether the greatest common factor of 67 and 7 is 1 before proceeding to the algebraic operations to find the multiplicative inverse.
    - In question 4 and the reflection for the second assessment, I find the relevant characteristics of repeated squaring by realizing that every exponent can be expressed as an addition of powers of 2 and mark the relevant powers that are needed for the final answer.
    - In Ada Lovelace: An Analysis of the Life of the Earliest Computer Programmer, I demonstrate high intellectual curiosity by providing a detailed, yet concise, paper on the life and contributions of Ada Lovelace to the computing field.

- Except for minor organization flaws , I have shown the ability to write clear, correct, and well-organized solutions to problems as demonstrated by the revisions for the first assessment, question 4 of the second assessment, and question 5 of the third assessment. Additionally, I have demonstrated the ability to write clear, well-reasoned papers in Ada Lovelace: An Analysis of the Life of the Earliest Computer Programmer as well as the project proposal.

- Lastly, the assessment reflections demonstrate errors in initial work as opportunities for improvement. The revisions provide cleaner answers to less than stellar initial work and contain minor oversights, if any.

Please add a table of contents.

Include your essay(s) (only one so far ...).

Gloire Rubambiza - MTH 312-01 - Introduction

- What are Singh's goals in writing this book?

=> Singh's goals in writing the book are to give a timeline to the evolution of codes and to prove the relevance of cryptography today.

- Why is (strong) encryption important today?

=> Strong encryption is important now more than ever because of our overwhelming reliance on interceptable forms of communication such as emails and the Internet economy.

- On page xv, Singh states that "... the public's growing demand for cryptography conflicts with the needs of law enforcement and national security." Do you think this is true? In what ways does it conflict? In particular, does strong encryption make law enforcement harder than it was before electronic communication (and thus wire taps) were possible?

=> To a certain extent, it is true. Case in point, the U.S government asking Apple for a backdoor into their software to unlock a dead terrorist's phone. The conflict mostly stems from people distrusting law enforcement i.e. suspicion that officers have backdoors into their private data. In my humble opinion, strong encryption does not make law enforcement harder. On the contrary, it makes it easier for law enforcement officers to have centralized and encrypted systems/databases to help them do their jobs more efficiently. Additionally, government agencies pour a lot of money into encryption research to (secretly) undermine the public's demand for privacy.

- What is the difference between a code and a cipher?

=> A code is a replacement of a word or phrase by another word, symbol or number whereas a cipher replaces letters in a word by other letters.

Gloire Rubambiza - MTH 312-01 - Chapter 1 (The Cipher of Mary Queen of Scots)

- What were some reasons Queen Elizabeth might not have wanted to execute Mary?

=> **Queen Elizabeth might not have wanted to execute Mary because she was her cousin. More importantly, Mary was the Queen of Scots, for killing Mary would set an undesirable precedent she was the head of another state.**

- What is steganography and how does it differ from cryptography?

=> Steganography involves discreet communication through hiding the existence of a message. It differs from cryptography because the latter hides the meaning of a message. Cryptography is, for the most part, immune to message interception whereas steganography is not.

- What is the difference between a transposition cipher and a substitution cipher?

=> The difference between a transposition and substitution cipher is that the former keeps the identity of the letters and shuffles their positions in a message whereas the latter obscures the identity of the letters while keeping their positions intact in a message.

- What is a scytale and how is it used?

=> A scytale is a wooden staff that was utilized by Spartans as the first military cryptographic device. By laying strips of leather on the scytale and writing a message on it, a sender can cipher a message that only a receiver with a scytale of a similar diameter may be able to decipher. Individually, the strips of letter contain meaningless letters.

- Singh discusses the *Kama-Sutra* and *mlecchita-vikalpā*. Why might this "art" have been more important for women than for men?

=> It might have been more important because there might have been repercussions for women with secret liaisons in case their patriarchal figure, be they husband or father, found out about said liaisons.

- What is the Caesar cipher?

=> The Caesar cipher substitutes letters from plain text with letters from a cipher alphabet that have been shifted one or more positions down the regular alphabet i.e. A for D, B for and E and so on.

- Discuss the role of a secret key in cryptography.

=> The role of a secret key in cryptography is to establish a specific way to use a general encryption algorithm. For instance, in the case of a substitution cipher, the secret key would determine the cipher alphabet to be used.

- Compare and contrast the *atbash* cipher and the Caesar cipher.

=> Both ciphers are ancient and based on substitution of letters. The *atbash* cipher replaces a letter based on its relative position to the end of the alphabet whereas the Caesar cipher replaces a letter based on a secret key that defines the cipher alphabet.

- What are nulls?

=> Nulls are symbols or letters in a deciphered message that are not substitutes for any letters, but rather meaningless noise to throw off anyone trying to decipher the message that is not the intended recipient.

- Discuss the relative merits of ciphers, codes (and codebooks), and nomenclators.

=> Nomenclators build off the separate complexities of ciphers and codewords by combining them into a single codebook whose encryption relies on ciphering the majority of the message and sprinkling codewords. Codes and ciphers are secure on their own merits. However, the summation of the two into nomenclators is no more secure than codes and ciphers individually. In other words, nomenclators are vulnerable to frequency analysis and context analysis, so to speak, just as ciphers and codewords are, respectively.

- Discuss the role of "social engineering" in the unmasking of the Babington plot. In particular, do you think Gifford or Phelippes played the more important role?

=> The naiveté of Babington and Mary in their communications made them vulnerable to social engineering. Walsingham knew Queen of Scots would not rest until she regained some, if not all, of her power. Therefore, he used the human resources at his disposal to unfold the assassination

plot. The Principal Secretary used Gifford because he knew Mary would trust a fellow Catholic. In other words, Gifford was used to gain Mary's trust and make her sign her death warrant. In my opinion, Gifford played the more important role because, without his Catholic background, cunning courier skills, and double agency, Mary would not have begun the communication with Babington that led to her death.

/ ✓ Finished @ 1:40PM ~ors > 2-7/18

Start 12:35 2/7 cm NAME: Gloire Rubambiza

Instructions

- Put your response to each question on a separate page and include your name and the problem number on each page.
- You do not need to attempt all of the questions. Work on the ones that you feel ready for and have time for.
- You may use scratch paper, a calculator, your texts, and your notes. Please do not use any network enabled device (smart phone, computer, tablet).
- You are welcome to discuss questions with your instructor for clarification.
- On the chart below, indicate which of the problems that you attempted should be assessed by circling the problem number.

NR

[✓ 1]	[✓ 2]	[✓ 3]	4	[✓ 5]	[✓ 6]	7	[✓ 8]	[✓ 9]

Table 1: Problems Attempted

1. **MC1** I can determine whether a small number is prime, and factor an integer into its prime factorization.

   MC2 I can find the greatest common divisor/greatest common factor of two positive integers and determine whether two integers are relatively prime.

   For each pair of integers, find their prime factorization and use it to find the greatest common factor of the pair.

   (a) 77 and 23. $7 \cdot 11 \cdot 1$ | $1 \cdot 23$ gcf = 1

   (b) 91 and 161. $91 \cdot 1$ | $161 \cdot 1$ gcf = 1

   (c) 126 and 135. $2 \cdot \boxed{3 \cdot 3} 7$ | $\boxed{3 \cdot 3} \cdot 3 \cdot 5$ gcf = ~~3~~ 9

Gloire Rubambiza

Gloire Rubambiza
02/07/2018

Assessment 1

2. a) 100 - 45 = 55

$45 - 0 \cdot 55 = 45$

$55 - 1 \cdot 45 = 10$

$45 - 4 \cdot 10 = 5$

$10 - 2 \cdot 5 = 0$

gcf(45, 100) = 5 ✓

b) $29 - 1 \cdot 19 = 10$

$19 - 1 \cdot 10 = 9$

$10 - 1 \cdot 9 = 1$

$9 - 1 \cdot 9 = 0$

gcf(19, 29) = 1 ✓

c) $64\ 2 \cdot 25 = 39$ $64 - 2 \cdot 25 = 14$

$25 - 0 \cdot 39 = 25$

$39 - 1 \cdot 25 = 14$

$25 - 1 \cdot 14 = 11$

$14 - 1 \cdot 11 = 3$

$11 - 3 \cdot 3 = 2$

$3 - 1 \cdot 2 = 1$

$2 - 2 \cdot 1 = 0$

gcf(64, 25) = 1 ✓

3. (a) (88 + 67) mod 7

= 155 mod 7

$155 = 7 \cdot 22 + 1$ ✓

$\Rightarrow$ (88 + 67) mod 7 = 1 ✓

3. (b) (13 − 67) mod 7

−54 mod 7

−54 = (−7 · 7) − 6 $\quad$ −7·7 − 6 = −55

⇒ (13 − 67) mod 7 = 6

(13−67) mod 7 = (−54) mod 7

= (−8·7 + 2) mod 7

$\boxed{= 2}$

(Or, −54 is 2 more than a multiple of 7)

(c) (575 + 919) mod 2

1494 mod 2

1494 = (2 · 747) + 0

⇒ (575 + 919) mod 2 = 0

(d) (14 · 7) mod 26

98 mod 26

98 = (3 · 26) + 20

⇒ (14 · 7) mod 26 = 20 ✓

4. a) The additive inverse of 12 modulo 77 = 65 ✓ because

65 mod 77 − 12 mod 77 = 0. (65 + 12) mod 77 = 0

b) The additive inverse of 45 modulo 8 = 5 because

45 mod 8 − 5 mod 8 = 0 $\quad$ ~~−5 mod 8~~ = 3

Also: (45 + 3) mod 8 = 0

5. a) The multiplicative inverse of 11 mod 26 exists if the greatest common factor of 26 and 11 is 1.

In other words 1 = (m · 11) mod 26

$$\begin{bmatrix}26\\1\\0\end{bmatrix} - 2 \cdot \begin{bmatrix}11\\0\\1\end{bmatrix} = \begin{bmatrix}15\\1\\-1\end{bmatrix} \begin{bmatrix}4\\1\\-2\end{bmatrix}$$

$$\begin{bmatrix}11\\0\\1\end{bmatrix} - 0 \cdot \begin{bmatrix}15\\1\\-1\end{bmatrix} = \begin{bmatrix}11\\0\\1\end{bmatrix} \qquad \begin{bmatrix}11\\0\\1\end{bmatrix} - 2 \cdot \begin{bmatrix}4\\1\\-2\end{bmatrix} = \ldots$$

45 mod 8 = 5

Gloire Rubambiza
02/07/2018

Assessment 1 (cont.)

5.(a) Continued

$$\begin{bmatrix}15\\1\\-1\end{bmatrix} - 1\begin{bmatrix}11\\0\\1\end{bmatrix} = \begin{bmatrix}4\\1\\-2\end{bmatrix} \checkmark$$

$$\begin{bmatrix}11\\0\\1\end{bmatrix} - 2\begin{bmatrix}4\\1\\-2\end{bmatrix} = \begin{bmatrix}3\\-2\\5\end{bmatrix} \checkmark$$

$$\begin{bmatrix}4\\1\\-2\end{bmatrix} - 1\begin{bmatrix}3\\-2\\5\end{bmatrix} = \begin{bmatrix}1\\3\\-7\end{bmatrix} \Rightarrow 1 = 3\cdot 26 + \boxed{(-7)\cdot 11}$$

$-7 \bmod 26 = \boxed{19}$

$$\begin{bmatrix}3\\-2\\5\end{bmatrix} - 3\begin{bmatrix}1\\3\\-7\end{bmatrix} = \begin{bmatrix}0\\-11\\26\end{bmatrix}$$

Because we found the additive inverse of the original matrix operation, the multiplicative inverse does exist. The multiplicative inverse of 11 mod 26 = -7.

What about the mult. inv. of 11 modulo 22 ?

6. c) $(37.25)_8$ to binary => each octal is three binary digits

0b 011 111 010 101 ✓

f) 0xA3C2 to decimal => each hex is 4 binary

$\Rightarrow \boxed{10\cdot 16^3 + 3\cdot 16^2 + 12\cdot 16^1 + 2\cdot 16^0}$

$\Rightarrow 10\cdot 4096 + 768 + 192 + 2$

$\Rightarrow 5058$

6. d) 3725 to decimal

$\Rightarrow 3 \cdot 8^3 + 7 \cdot 8^2 + 2 \cdot 8^1 + 5 \cdot 8^0$

$\Rightarrow$ 2005 ✓

g) 0xABC2 to binary => 1 hex digit = 4 binary digits

0b 1010 0011 1100 0010 ✓

9. a) R E S T R

S L E E P

=> J P W X G ✓

b) R E S T R E S T R E

I E D T O E L B F R

=> RELAXATION ✓

Write across rows, transpose, then read down columns.

8a.

J	U	N	G	L	E
K	P	L	N	I	R
E	C	M	D	P	O
E	A	A	C	E	N

E	G	J	L	N	U
R	N	K	I	L	P
O	D	E	P	M	C
N	C	E	E	A	A

Encoded message : RONNDCKEEIPELMAPCA

b)

E	G	J	L	N	U
C	A	S	I	O	M
D	E	E	G	E	
Y	S	A	U	O	
S	N	I	E	R	L
T	F	S	V	E	
R	O	N	R	A	
		N		L	

Gloire Rubambiza - MTH 312 - Assignment 1 Reflection

1. What went well

- I am good at encrypting/decrypting messages using the Vigenere Cipher
- Except for one careless mistake in calculations, I am confident in my ability to convert between bases
- I did not fall prey to the mistake of adding spaces and/or adding letters when none are needed in the columnar transposition. There are still areas of improvement (read on).

2. Areas of improvement

- I had a misconception about the greatest common factor (gcf) when it's not 1. Instead, I chose the smallest positive common factor.
- I need to read instructions more carefully and avoid carelessness in calculations (6(f))
- I am still struggling with modular arithmetic involving not only negative numbers, but also additive inverses.
    - I misunderstood and misinterpreted the results of modular arithmetic.
        - For instance, on question 3(b), I thought since I can find the nearest factor of 7 going in the negative direction from 0, whatever number was added/subtracted is the answer. Hence, my *wrong* answer of (13-67) mod 7 = 6.
        - This misconception is perpetuated to the Extended Euclidean Algorithm, too. In question 5(a), I thought finding the multiplicative inverse from the second to last step is the final answer not matter the sign of the answer, not realizing that a negative answer had to be operated on i.e -7 mod 26 to get 19.
        - **Deeper connection**: the misconception was reinforced in the *"send an encrypted message"* assignment where I got a negative number as the multiplicative inverse (-13), and plugged it into my Python program. Since the decrypted message using -13 was legible and sensible, I missed the connection that the multiplicative inverse is actually -13 mod 59 = 46. However, the light bulb went on in class as we went through the assignment and I thought back to the comment from my assignment partner to either get (-13) or (46) as the multiplier.
    - In regards to additive inverses, I keep falling for the trick of asking the wrong question. In other words, asking *"what do we need to subtract to get a factor of the modulus?"* instead of *"what do we need to add and perform a modulo operation to get 0?"*
- I need to be careful when doing columnar transposition by not writing across columns AND reading across columns

Gloire Rubambiza
MTH 312-01
02/11/2018

In-class Assessment 1 - Revisions

1-c)) 126 $\quad\quad$ 135

$1 \cdot 2 \cdot \boxed{3 \cdot 3}\, 7$ $\quad\quad$ $1 \cdot \boxed{3 \cdot 3} \cdot 5$

Greatest common factor of 126 and 135 = 9

2-c)

$$\begin{aligned} 64 - 2 \cdot 25 &= 14 \\ 25 - 1 \cdot 14 &= 11 \\ 14 - 1 \cdot 11 &= 3 \\ 11 - 3 \cdot 3 &= 2 \\ 3 - 1 \cdot 2 &= 1 \\ 2 - 2 \cdot 1 &= 0 \end{aligned}$$

$\Rightarrow$ gcf$(64, 25) = 1$

3-b)

$$\begin{aligned} &(13 - 67) \bmod 7 \\ &= (-54) \bmod 7 \\ &= (-8 \cdot 7 + 2) \bmod 7 \end{aligned}$$

$\Rightarrow (13 - 67) \bmod 7 = 2$

4-a) The additive inverse of 12 modulo 77 = 65 because
$(65 + 12) \bmod 77 = 0$

b) The additive inverse of 45 mod 8 = 3 because
$(45 + 3) \bmod 8 = 0$

Gloire Rubambiza
MTH 312-01
02/11/2018

In-Class Assessment 1 - Revisions

5. a) The multiplicative inverse of 11 mod 26 exists if the greatest common factor of 26 and 11 is 1.

$$\begin{bmatrix} 26 \\ 1 \\ 0 \end{bmatrix} - 2\begin{bmatrix} 11 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 4 \\ 1 \\ -2 \end{bmatrix}$$

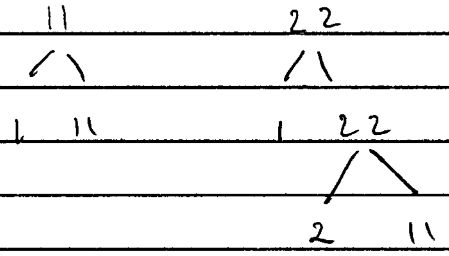
$$\begin{bmatrix} 11 \\ 0 \\ 1 \end{bmatrix} - 2\cdot\begin{bmatrix} 4 \\ 1 \\ -2 \end{bmatrix} = \begin{bmatrix} 3 \\ -2 \\ 5 \end{bmatrix}$$

$$\begin{bmatrix} 4 \\ 1 \\ -2 \end{bmatrix} - 1\cdot\begin{bmatrix} 3 \\ -2 \\ 5 \end{bmatrix} = \begin{bmatrix} 1 \\ 3 \\ -7 \end{bmatrix} \Rightarrow 1 = 3\cdot 26 + (-7)\, 11$$

$$\begin{bmatrix} 3 \\ -2 \\ 5 \end{bmatrix} - 3\begin{bmatrix} 1 \\ 3 \\ -7 \end{bmatrix} = \begin{bmatrix} 0 \\ -11 \\ 26 \end{bmatrix}$$

$\Rightarrow$ The multiplicative inverse of 11 mod 26 = -7 mod 26 = $\boxed{19}$

5. b)



$\Rightarrow$ 11 mod 22 does not have a multiplicative inverse because their greatest common factor is 11 i.e. not 1.

Gloire Rubambiza
MTH 312 -01
02/11/2018.

In-Class Assessment 1 - Revisions

6.a) Convert the decimal number $(985)_{10}$ to octal

$985 = 123 \cdot 8 + 1$

$123 = 15 \cdot 8 + 3$

$15 = 1 \cdot 8 + 7$

$1 = 0 \cdot 8 + 1$

$\Rightarrow (985)_{10} = (1731)_8$

6.b) Convert the decimal number $(985)_{10}$ to binary

ref 6a) $985_{10} = 1731_8$

$\Rightarrow 1731_8 = 001\ 111\ 011\ 001_2$

6.e) Convert the decimal number $(3725)_{10}$ to hexadecimal (base 16)

$3725 = 232 \cdot 16 + 13$

$232 = 14 \cdot 16 + 8$

$14 = 0 \cdot 16 + 14$

$\Rightarrow (3725)_{10} = E8D$

6.f) Convert the hexadecimal number 0xA3C2 to decimal

$A3C2 = 10 \cdot 16^3 + 3 \cdot 16^2 + 12 \cdot 16^1 + 2 \cdot 16^0$

$= 10 \cdot 4096 + 768 + 192 + 2$

$= 41,922$

Gloire Rubambiza
MTH 312 -01
02/11/2018

In-class Assessment 1 - Revisions

8. a)

J	U	N	G	L	E
K	E	E	P	C	A
L	M	A	N	D	C
I	P	E	R	O	N

E	G	J	L	N	U
A	P	K	C	E	E
C	N	L	D	A	M
N	R	I	O	E	P

Encoded message: ACNPNRKLICDOEAEEMP

JUNGLE	E	G	J	L	N	U
6	C	R	F	S	U	O
6	D	A	O	N	E	R
6	Y	E	S	N	V	E
6	S	S	E	I	R	A
6	T	N	A	G	O	L
3			I		E	M

J	U	N	G	L	E
F	O	U	R	S	C
O	R	E	A	N	D
S	E	V	E	N	Y
E	A	R	S	I	S
A	L	O	N	G	T
I	M	E			

Decrypted message: four score and seven years is a long time.

Gloire Rubambiza - MTH 312 - Ch.2 Le Chiffre Indechiffrable

1. Important information

Fact: The effort required to implement the Vigenere cipher discouraged many people from employing it whereas monoalphabetic was quick and easy to use and impregnable by people not schooled in cryptanalysis

Fact: The main two advantages of the Vigenere cipher is that it's impregnable to frequency analysis and it has a great number of keys. Yet, it was neglected for almost two centuries. The sheer volume of letters to be processed made the Vigenere cipher almost useless.

Fact: The homophonic cipher is a type of monoalphabetic cipher because each symbol can only a substitute for one letter.

Fact: Bazeries was the cryptanalyst that broke the Great Cipher and revealed, after two centuries of mystery, the secrets of King Louis XVI.

Fact: Although they sound fictional, the evidence in support of the authenticity of the Beale papers is compelling.

Reflection: I think the advantages of the Vigenere cipher and the trade-offs developed is the overlying theme of the chapter because all the alternatives mentioned later in the chapter attempt to reduce complexity in exchange for less security.

2. Questioning

Answered question: How does the numbering of different letters relate to its sound? We can think of all the substitutes for the letter as representing the sound of the letter in the ciphertext.

Unanswered question: How was the postal office not able to realize that the Black Chambers were somewhat compromising their business?

Unanswered question: What does Babbage mean by "I wish to God these calculations had been executed by steam!"?

3. Connection

- Based on our discussion of the introduction and reading this chapter, it seems the public need for privacy dates to the days of Morse code when people were asking for a good cipher to ensure privacy in their communications handled by Morse operators.
- The author mentioned in the introduction that the NSA might already know secrets on how to break all current ciphers. It is likely the practice was common in the times of Babbage as well, because the author suggests Babbage did not publish his technique to help Britain gain an advantage in wars for decades.

=> The above connections clarified the text because they relate the chapter to previous readings and one of our objectives for the class: discussing the ever-increasing role of cryptography and privacy in our daily lives.

Gloire Rubambiza - MTH 312 - Ch.3 The Mechanization of Secrecy

1. Important information

Fact: Guglielmo Marconi, an Italian physicist, invented radio and sent the first transatlantic radio transmission in December of 1901.

Fact: The ADFGVX cipher was developed by the Germans and cracked by the French because the sheer volume of radio traffic required strong cryptanalysis to stay ahead of the enemy during the Great War.

Fact: The one time pad cipher was invented in response to the insecurity of the modified Vigenere cipher that uses a key that is as long as a message itself.

Fact: The cipher disk is a mechanized version of the Vigenere cipher.

Reflection: The Great War was a challenging time for code makers because any new ciphers were eventually broken. The advent of radio made matters worse because radio communications could be intercepted by enemies easily. I think the eventual success of the Enigma machine was spurred on by the Allies arrogance and underestimation of Germany because the Allies' cryptanalysis bureaus had broken the Zimmerman note and changed the course of history. The interception and cracking of the Zimmerman telegram is a prime example of social engineering to make Mexico look like the incapable party when Germany could not deduce that their ciphers had been broken by the Allies.

2. Questioning

Answered question: Why was the one time pad not adopted widely? There would have to be plenty of random keys generated for each message and the army alone sent hundreds, if not thousands, of messages each day.

Unanswered question: What cipher was used to encrypt the Zimmerman note?

Unanswered question: What did the Kaiser title mean in Germany during the Great War?

3. Connection

- In high school history classes, we were told of the impact of the Zimmerman note on the Great War. However, there was no mention of cryptography and cipher bureaus playing critical roles as well. The book finally answers my question of "couldn't Germany have encrypted the telegram before sending it?"
- The technique used by the French to learn a Morse operator's *"fist"* sounds like the modern equivalent of using data mining to learn a competitor's secrets or user's behavior patterns. Nowadays, this is critical info that drives business decisions.

=> The connections made are helpful in putting a cryptographic view point on the Zimmerman note based on what I already knew from history classes.

Gloire Rubambiza
02/28/2018
MTH 312

Assessment 2 – Question 4

4.a) $35^{10} \bmod 127$

$35^{1} \bmod 127 = 35$

$35^{2} \bmod 127 = (35 \bmod 127 \cdot 35 \bmod 127) \bmod 127$

$= 35^{2} \bmod 127$

$= 82$ *

$35^{4} \bmod 127 = (35^{2} \bmod 127 \cdot 35^{2} \bmod 127) \bmod 127$

$= 82^{2} \bmod 127$

$= 120$

$35^{8} \bmod 127 = (35^{4} \bmod 127 \cdot 35^{4} \bmod 127) \bmod 127$

$= 120^{2} \bmod 127$

$= 49$ *

$35^{10} \bmod 127 = (35^{8} \bmod 127 \cdot 35^{2} \bmod 127) \bmod 127$

$= (49 \cdot 82) \bmod 127$

$= \boxed{81}$ ✓

4.b) $23^{12} \bmod 50$

$23^{2} \bmod 50 = (23 \bmod 50 \cdot 23 \bmod 50) \bmod 50$

$= 23^{2} \bmod 50$

$= 29$

$23^{4} \bmod 50 = (23^{2} \bmod 50 \cdot 23^{2} \bmod 50) \bmod 50$

$= 29^{2} \bmod 50$

$= 41$ *

$23^{8} \bmod 50 = (23^{4} \bmod 50 \cdot 23^{4} \bmod 50) \bmod 50$

$= 41^{2} \bmod 50$

$= 31$ *

$23^{12} \bmod 50 = (23^{8} \bmod 50 \cdot 23^{4} \bmod 50) \bmod 50$

$= 41 \cdot 31 \bmod 50$

$= \boxed{21}$ ✓

Gloire Rubambiza
MTH 312
02/28/2018

Assessment 2 - Question 5

5.a) Clear text : SPRING

Matching text = AGDGXAXDAAGG

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

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

Encryption : GAAAGDGXAGXG
GAAAVDDXAGXG

5. b)

A	C	D	R
G	D	A	D
A	G	D	F
D	X	A	A
G	V		

C	A	R	D
D	G	D	A
G	A	F	D
X	D	A	A
V	G		

Decrypted : PLAYING ✓

Gloire Rubambiza
02/28/2018
MTH 312

Assessment 2 - Question 7

7.a) C o l d ␣ A i r

28 14 11 3 62 26 8 17

$x \rightarrow (15x + 13) \bmod 67$

$C \rightarrow 28 \longrightarrow (15 \cdot 28 + 13) \bmod 67 = 31 = F$

$o \rightarrow 14 \longrightarrow (15 \cdot 14 + 13) \bmod 67 = 22 = w$

$l \rightarrow 11 \longrightarrow (15 \cdot 11 + 13) \bmod 67 = 44 = S$

$d \rightarrow 3 \longrightarrow (15 \cdot 3 + 13) \bmod 67 = 58 = 6$

$␣ \rightarrow 62 \rightarrow (15 \cdot 62 + 13) \bmod 67 = 5 = f$

$A \rightarrow 26 \longrightarrow (15 \cdot 26 + 13) \bmod 67 = 1 = b$

$i \longrightarrow 8 \longrightarrow (15 \cdot 8 + 13) \bmod 67 = 66 = ?$

$r \rightarrow 17 \longrightarrow (15 \cdot 17 + 13) \bmod 67 = 0 = a$

Cipher text = FwS6fb?a ✓

b) g z C .

6 25 28 63

$f(x) = (7x + 4) \bmod 67$

gcf (7, 67) = 1 → multiplicative inverse exists

$1 = m \cdot 7 + k \cdot 67$

$67 = 9 \cdot 7 + 4$

$$\begin{bmatrix} 67 \\ 1 \\ 0 \end{bmatrix} - 9 \cdot \begin{bmatrix} 7 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 4 \\ 1 \\ -9 \end{bmatrix}$$

$$\begin{bmatrix} 7 \\ 0 \\ 1 \end{bmatrix} - 1 \begin{bmatrix} 4 \\ 1 \\ -9 \end{bmatrix} = \begin{bmatrix} 3 \\ -1 \\ 10 \end{bmatrix}$$

$$\begin{bmatrix} 4 \\ 1 \\ -9 \end{bmatrix} - 1 \begin{bmatrix} 3 \\ -1 \\ 10 \end{bmatrix} = \begin{bmatrix} 1 \\ 2 \\ -19 \end{bmatrix}$$

$$\begin{bmatrix} 3 \\ -1 \\ 10 \end{bmatrix} - 3 \begin{bmatrix} 1 \\ 2 \\ -19 \end{bmatrix} = \begin{bmatrix} 0 \\ -7 \\ 67 \end{bmatrix}$$

$\Rightarrow 1 = 2 \cdot 67 + -19 \cdot 7$

Gloire Kubambiza
02/22/2018
MTH 312

Assessment 2 - Question 7 (Continued)

7.b continued

Translation

$g \to 6 = (7x+4) \bmod 67$

"subtract 4" $2 \bmod 67 = 7x \bmod 67$

"unmultiply" by 7 $-19 \cdot 2 \bmod 67 = -19 \cdot 7x \bmod 67$

$-38 \bmod 67 = x$

$x = 29 = D$

$Z \to 25 = 21 \bmod 67 = 7x \bmod 67$

$-19 \cdot 21 \bmod 67 = -19 \cdot 7x \bmod 67$

$-399 \bmod 67 = x$

$x = 3 = d$

$E \to 28 = 24 \bmod 67 = 7x \bmod 67$

$-19 \cdot 24 \bmod 67 = -19 \cdot 7x \bmod 67$

$-456 \bmod 67 = x$

$x = 13 = n$

$o \to 63 = 59 \bmod 67 = 7x \bmod 67$

$-19 \cdot 59 \bmod 67 = -19 \cdot 7x \bmod 67$

$-1121 \bmod 67 = x$

$x = 18 = s$

Decrypted text = Ddns ✓

Gloire Rubambiza
02/28/2018
MTH 312

Assessment - Question 9

9.a) 0101 | 1000 | 0101 | 1001
K 1010 1000 1010 1000
cipher = 1111 | 0000 | 1111 | 0001 ✓

b) 1110 | 0111 | 1110 | 0011
1010 1000 1010 1000
Cipher = 0110 1111 0101 1011
0100 1111 0100 1011

1 if the digits are different

0 if the digits are the same

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

9.b) XOR 1110 | 0111 | 1110 | 0011

1010 1000 1010 1000

cipher = 0100 1111 0100 1011

Gloire Kubambian

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: G A A A V D D X A G X G

Gloire Rubambiza - MTH 312 - Unbreakable Typex?

Summary

The Code Book mentions briefly that Great Britain used an apparently unbreakable cipher, Typex, during World War II. However, no further details are provided explaining why it could not broken. In my exploration on the topic I found two interesting articles on the topic.

- The Codes and Ciphers article mentions that Typex was based off of the Enigma machines, with major improvements.
- The Guardian notes in its article that Germans declared Typex "unbreakable" after only 6 weeks of attempting to break the cipher system. Additionally, the article notes that the development of Typex infringed several German patents.

=> With more drive, I believe the Germans could have used, through espionage, some of the theoretical mathematics developed by Marian Rejewski to analyze and break Typex. Alas, the advancements made by the Poles were to be kept secret.

Resources

1. https://www.codesandciphers.org.uk/heritage/ModSec.htm
2. https://www.theguardian.com/lifeandstyle/2012/jul/18/british-enigma-machine-typex

MTH 312 - Semester Project Proposal

Team Members: Wesley Guthrie, Tom Novakoski, Gloire Rubambiza, Colin Smith

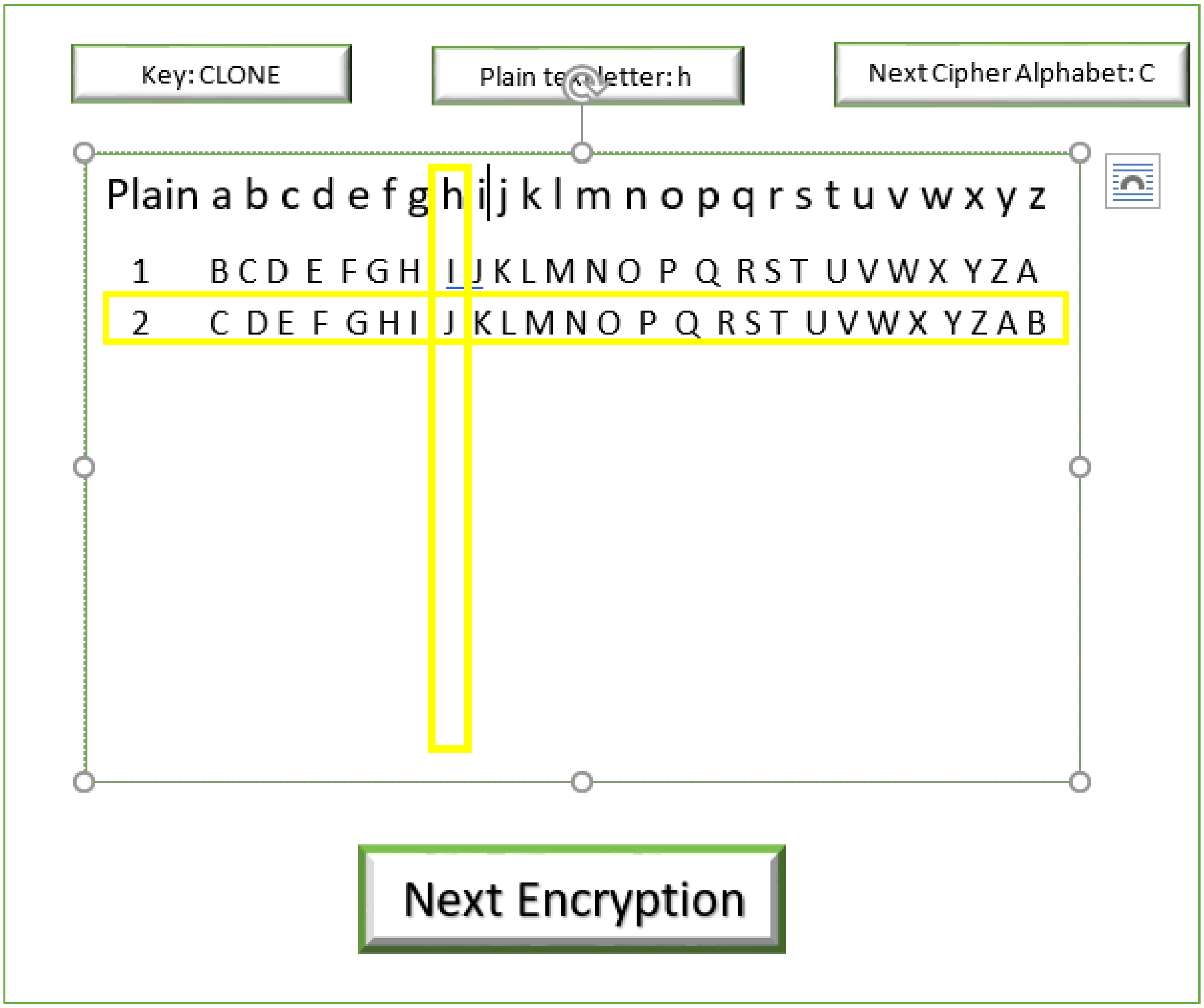
1. Introduction

The Vigenère cipher, developed by Blaise de Vigenère in the 1523, is a polyalphabetic cryptographic system that relies on a secret key shared by a sender a receiver. The secret key determines the cipher alphabets to be used when encrypting and decrypting messages. Despite its promise of security against people not schooled in cryptanalysis, the system was not widely adopted in its infancy in the 16th century mostly due to its complexity. In our project, we will reach out to the public and provide them with a basic understanding of the Vigenère cipher.

2. Public Service Project

Because the general public uses applications on their smartphones and desktops on a daily basis, we will explore that space to achieve our goal of introducing them to the Vigenère cipher. Specifically, we will build a Java program that a user can launch and easily step through to learn about the encryption and decryption process of the Vigenère cipher.

The program will feature a simple graphical user interface, as shown in fig. 1, that illustrates the steps involved in selecting a cipher alphabet using the key and enciphering a single letter.



Plain	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B

3. Division of Labor

The preliminary division of labor is as follows:

- Model/Controller class(es): Wesley, Colin
- GUI: Gloire, Wesley
- Documentation: Gloire, Tom

4. Deliverables

- Java program runnable on any system featuring Linux and Java Runtime Environment
- Project design documentation
- Demo with a few classmates/prof
- Final report/reflection

Target label	Target	
☒	**MC1**	I can do basic arithmetic involved with divisibility and primality: find the quotient and remainder obtained when dividing two integers, determine whether a small number is prime, and factor an integer into its prime factorization.
☒	**MC2**	I can find the greatest common divisor/greatest common factor of two positive integers and determine whether two integers are relatively prime.
□	**MC3**	I can determine whether an integer is a primitive root *modulo* p where p is a prime number.
☒	**MC4**	I can use the Euclidean Algorithm to find the greatest common factor of two positive integers.
☒	**MC5**	I can find the value of a mod n for any integer a and positive integer n.
☒	**MC6**	I can calculate sums and products using modular arithmetic.
☒	**MC7**	I can find the additive inverse of an integer *modulo* n
☒	**MC8**	I can determine whether an integer has a multiplicative inverse *modulo* n, and calculate it if it does.
☒	**MC9**	I can use the Extended Euclidean Algorithm to determine whether an integer has a multiplicative inverse *modulo* n, and calculate it if it does.
□	**MC10**	I can find the XOR of two bit strings of the same length.
☒	**MC11**	I can convert integers between decimal, binary, octal, and hexadecimal representations.
□	**MC12**	I can calculate $\varphi(n)$ where n is a positive integer and φ is Euler's totient function.
☒	**MC13**	I can raise an integer to a positive integer power *modulo* n using the repeated squaring algorithm, Fermat's Little Theorem, and Euler's Theorem.
□	**MC14**	I can use the Chinese remainder theorem to solve systems of modular equations.
□	**MC15**	I can factor an integer using Fermat's algorithm.

Table 1: MATHEMATICAL CONTENT Learning Targets

Target label	Target	
☒	**CS1**	I can encrypt and decrypt messages using a variety of substitution ciphers (cryptogram, Playfair, ADFGX).
□	**CS2**	I can encrypt and decrypt messages using a shift cipher.
□	**CS3**	I can encrypt and decrypt messages using a decimation or affine cipher.

Table 2: CRYPTOGRAPHY SKILLS Learning Targets

Target label	Target	
☒	**CS4**	I can encrypt and decrypt messages using a variety of transposition ciphers (rail fence, route cipher, columnar transposition).
☒	**CS5**	I can encrypt and decrypt messages using the Vigenere cipher.
□	**CS6**	I can encrypt and decrypt English character messages using a one-time pad.
☒	**CS7**	I can encrypt and decrypt a bit string using the Simple XOR cipher.
□	**CS8**	I can encrypt a short message using S-DES.
□	**CS9**	I can encrypt and decrypt a short message using RSA.
□	**CS10**	I can encrypt and decrypt a short message using El Gamal.
□	**CS11**	I can determine a mutually agreed-upon key using the Diffie-Hellman protocol.
□	**CS12**	I can create a digital signature for a short message using RSA.
□	**CS13**	I can encrypt and decrypt messages using a Hill (Block) cipher.
□	**CS14**	I can encrypt and decrypt short messages using a Pohlig-Hellman Cipher.
□	**CS15**	I can describe the process of sending a message using the three-pass protocol.

Table 2: CRYPTOGRAPHY SKILLS Learning Targets

Target label	Target	
□	**CC1**	I understand and can explain the differences (including advantages and disadvantages) among different types of ciphers.
□	**CC2**	I understand and can explain the differences among secret key cryptography, secure key exchange, public key cryptography, and hash functions.
□	**CC3**	I understand and can explain the different encryption features needed for secret key cryptography, secure key exchange, public key cryptography, and hash functions.
□	**CC4**	I understand and can articulate issues concerning "big data," privacy, security, and transparency and the role of encryption in these issues.

Table 3: CRYPTOGRAPHY CONCEPTS Learning Targets

Gloire Rubambiza
03/23/2018
MTH 312-01

In-class Assessment 3

4. a)

P R M T E A I S S N T W Y H P E R O L G C L D A
U E A H M T C I I I S A T E O T Y F O I A I E S

Encrypted: PRMTEAISSNTWYHPEROLGCLDA UEAH MTCIIITSATEOTYFO IAIES ✓

b) G D W D E E O G I T A Y H N A D O W L F N M T E A I S
O O N E P N V H N O N T I G N Y U I L I D A H M T C

Decrypted: GO DOWN DEEP ENOUGH INTO ANYTHING AND YOU WILL FIND MATHEMATICS. ✓

Gloire Rubambiza
03/23/2018
MTH 312-01

In-Class Assessment 3

5. a)

G	O	D	M	A
D	E	T	H	E
I	N	T	E	G
E	R	S	A	L
L	E	L	S	E
I	S	T	H	E
W	O	R	K	O
F	M	A	N	

Encrypted: GDIELIWFMANKROSTHSLERSAETNETHMDOAEGLEEO ✓

b)

W	H	E	N	B
O	Z	O	T	H
E	C	L	O	W
N	D	I	E	D
H	E	L	E	F
T	S	O	M	E
B	I	G	S	H
O	E	S	T	O
F	I	L	L	

Decrypted: WHEN BOZO THE CLOWN DIED HE LEFT SOME
BIG SHOES TO FILL ✓

Gloire Rubambiza - MTH 312 - Assessment 3 Reflection

1. What went well

- Despite walking into the assessment unprepared, I performed tremendously well with the Rail and Route ciphers. To be honest, it was a first time encrypting and decrypting with both ciphers and I was surprised by my performance.

2. Areas of improvement

- Compared to previous assessments, I was very unprepared for the third assessment. Having missed Monday and Wednesday class while on my graduate school visit at Cornell University, I thought the assessment would be held the following Friday. As a result, I did not get to assess myself on as many learning targets as I would have wanted had I been prepared.
- In hindsight, I could have done well on the Chinese remainder theorem because it made sense immediately during the revision in class.
- On the fourth in class assessment, I will do extensive preparation to tackle the missed learning targets from the third assessment as well as those in the upcoming assessment.

Ada Lovelace: An Analysis of The Life of the Earliest Computer Programmer

1. Childhood and Education

1.1. Family lineage and education

Ada Byron Lovelace, born Augusta Ada Byron in 1815, was the only child of George Gordon Byron, a celebrated British poet and Anne Isabella ("Annabella") Milbanke [1]. Born in a troubled marriage, Ada barely knew her father. Like Ada, George had a volatile childhood despite being born of parents of high rank in England. George left England shortly after Ada's birth without any warning to his destination. Therefore, Ada was raised by a single mother.

Intermittently, Anabella would suspect George of a mental illness despite his penmanship genius. As such, Ada once wrote to her mother that she would like to redeem her father's "misused genius" by bringing out great truths and principles [2]. Such a statement from a girl was rare in Victorian England because the education of girls with Ada's rank included the social graces, music, painting and foreign languages. However, through a passion passed on from her mother, Ada pursued her interest in Mathematics and Italian. Through her contributions to the Difference and Analytical Engines developed by Charles Babbage, she has been dubbed as the first computer programmer.

1.2. Psychological analysis

Psychological theory provides an explanation for children raised in families with constant stress yet lead successful lives as adults – an external and influential mentor. Interestingly, it is unclear whether such a mentor for Ada was embodied in Charles Babbage or a motivational adoration of her deceased father. Although she met Babbage aged seventeen, Ada is also quoted writing to her mother, regarding her father, that: "If he has transmitted to me any portion of that genius, I would use it to bring out great truths and principles. I think he has bequeathed this task to me. I have this feeling strongly; and there is a pleasure attending it" [2].

2. Charles Babbage and the Difference Engines.

2.1. Life as Lady Lovelace

Ada began collaborating with Charles Babbage on a translation project when she was in her mid-twenties and married to William King, Lord Lovelace [1]. It is surprising that, in Victorian England, William was not intimated by an intellectually superior wife and had no issue with Ada working with Charles Babbage. In fact, the Babbages and Lovelaces eventually became close family friends.

2.2. Generalized Contributions

The pioneering collaboration between Ada and Charles began as a translation of a paper describing the function and theory of Charles' Analytical engine written by L. F. Menebrea, an Italian Mathematician and ambassador to France. Ada translated the paper from French to English.

Through her translation work on the Menebrea paper, Ada annotated the original paper so much that the annotations superseded the original paper. Charles suggested that Ada publishes her annotations as an original paper, but Ada preferred to honor her commitment to the publisher, which was to translate Menebrea's text [1]. Ultimately, Ada chose to sign her completed work under the alias of "A.A.L." – an acronym only a few close friends and family members knew was Lady Lovelace.

2.3. Computing Contributions

In annotating the Menebrea text, Ada observed that human-facilitated calculations are error prone because of the *shifting* meaning of many of the symbols used in mathematical notation and operations [3]. Ada stresses the importance of separating the annotation of *numerical operations* from *numerical data* and *operations.* Furthermore, Ada distinguished the Analytical Engine from the Difference Engine as the former *embodying the science of operations* while the latter embodies *one particular and very limited set of operations* [3]. Given succinct abstraction of numerical data and operations, then it is possible to represent entities – which are synonymous to the Object-Oriented paradigm in computer programming [4].

In addition to data abstraction, Lady Lovelace predicted one of the most important shortcomings of computer programming – at least before the advent of artificial intelligence; that is the need for human instruction and intervention in any successful computations.

She warns that "the Analytical engine has no pretensions whatever to originate anything. It can do whatever we know how to order it to perform. It can follow analysis, but it has no power anticipating any analytical revelations or truths. Its province is to assist us in making available what we are already acquainted with. Any thinking which the machines do indeed do must be put in. They must be programmed to think and cannot do so for themselves" [1].

3. The Lovelace Legacy

In addition to the Menebrea translation project, Ada and Charles collaborated on testing mathematical theories of probability. They devised what they expected to be an infallible system to beat the odds when betting on horses [1]. At first, the gambling involved Ada's husband too, William. Eventually, Charles and William quit gambling after noticing the shortcomings of the system. However, Ada kept gambling and her health began declining. The mathematical genius passed away at age thirty-six from an illness that was later diagnosed as cancer.

While working on the Analytical engine, Ada developed instructions for doing computations on Babbage's Analytical engine [1]. Her work represents the forerunner of computer programming. For those that chose to honor Ada Lovelace's contributions to the field of computing, the programming language *Ada* has been named after the de facto first computer programmer.

References

[1] N. C. o. T. o. Mathematics, "Ada Byron Lovelace," in *Celebrating Women in Mathematics and Science*, Reston, The National Council of Teachers of Mathematics, Inc., 1996, pp. 57-65.

[2] V. R. Huskey and H. H. D, "Lady Lovelace and Charles Babbage," *Annals of the History of Computing,* vol. 2, no. 4, pp. 299-329, 1980.

[3] M. Philip and M. Emily, "Sketch of the Analytical Engine Invented by Charles Babbage by L. F. Menebrea. With Notes upon the Memoir by the Tranlsator, Ada Augusta, Countess of Lovelace," in *Charles Babbage and His Calculating Engines*, New York, Dover Publications, Inc., 1961, pp. 225-297.

[4] D. Swade, *The Babbage Engine,* Mountain View: Computer History Museum, 2018.