Codesmasher: Learning About A Cryptographer in a Game about Cryptography

by

Nicholas M. Parker

And

Xinxin Qian

A Thesis Project

Submitted to the Faculty

of the

WORCESTER POLYTECHNIC INSTITUTE

in partial fulfillment of the requirements for the

Degree Master of Science

In

Interactive Media and Game Development

APPROVED:

Dean O'Donnell, Thesis Advisor ____

Edward Gutierrez, Committee ____

Abstract

Codesmasher is an educational code breaking game that seeks to tell the story of Elizebeth Smith Friedman, “America’s First Female Cryptanalyst". Through a combination of stories presented from Elizebeth’s point of view, to solving encoded messages using various cipher techniques that Elizebeth herself used, the player learns about her career and her impact on the art of cryptography in the United States and gain a better appreciation for military code breakers. This paper discusses the process of how we researched Elizebeth’s story, created the game, playtested it and gathered data, analyzed the playtest data, and finally published the game on itch.io.

Acknowledgements

Xinxin Qian: Thank you to everyone who has helped us on this paper: Dean and the other readers, my cat, computer and CSDN. Without your help, I may not have been able to graduate successfully during COVID and enjoy a hard but exciting time making a game.

Nick Parker: I would like to give my sincere thanks to my family, specifically my parents and my sister, for being constant sources of support and always being available to offer any guidance that they could. I also want to give thanks to our advisor Dean O'Donnell for his help and insights throughout the entirety of this process.

Table of Contents

Introduction

Codesmasher's main experience goal is to provide an interesting and engaging way for players to learn about Elizebeth Smith Friedman by following in her footsteps. Instead of just reading about the cyphers she decrypted, players are asked to decode messages using the very methods she pioneered. We hope to show players a small piece of the amount of work and effort that is put into codebreaking, and show the impact the Elizebeth made during her career.

Codesmasher is a menu based puzzle game made using Unity. It has been published on itch.io for the PC and the target audience will range from 18 and up. *Codesmasher* will be marketed towards individuals with an interest in history, cryptology, and cryptanalysis.

Also as a disclaimer, it should be noted that the spelling of Elizebeth's name is not a typo. It is in fact spelt with an E.

Research and Inspiration

Elizebeth Smith Friedman

Elizebeth Smith Friedman's cryptology career started in 1916. Then named Elizebeth Smith, she was an avid fan of William Shakespeare. During this time, she had decided to travel to Chicago's Newberry Library to see a copy of Shakespeare's First Folio that was held there.[1] During her stay, she had a conversation with a librarian about her interest and love for Shakespeare. The librarian told Elizebeth about a wealthy textile merchant named Colonel

[1] Fagone, J. (2018). *The woman who smashed codes: A true story of love, spies, and the unlikely heroine who outwitted America's enemies* (pp. 11-12). New York City, New York: Dey St., an imprint of William Morrow.

George Fabyan who owned a private think-tank called Riverbank Laboratories, and was also interested in Shakespeare. The librarian then called Fabyan who soon arrived in his limousine and invited Elizebeth to stay the night at Riverbank.[2] She agreed, and during her stay, he offered her a job to assist American educator Elizabeth Wells Gallup and her sister in investigating the Baconian theory of Shakespeare's authorship. This theory perpetuates that the famous philosopher Sir Francis Bacon was the real author of Shakespeare's play. The theory is based on the belief of correspondences between philosophical ideas of Bacon and the works of Shakespeare.[3] More important to Elizebeths story, it was also believed that Bacon had left cryptographic ciphers and codes in the plays and poems that proved this theory. As such, Elizabeth's work would involve decrypting these messages.[4] She agreed, and her cryptology career began.[5]

Not long after, Riverbank began working on military cryptography as well. Until the Army Cipher Bureau was established following World War I, Riverbank was the only facility in the U.S. capable of solving enciphered messages. After World War 1 began, a number of U.S. Government departments asked Riverbank Labs for help and sent personnel there for training.[6] In addition, among the staff of fifteen at Riverbank was the man that would become her husband in 1917, William F. Friedman,[7] who would later go on to run the research division of the SIS in the 1930s and 50s, and assist in the breaking of Japan's PURPLE cipher before America's

[2] Ibid, (15-16)
[3] Ibid, (17-18)
[4] Ibid, (33-34)
[5] Ibid, (35)
[6] Ibid, (66-69, 82-85)
[7] Ibid, (49, 57-60)

entrance into World War II.[8] Elizebeth and William worked together at Riverbank until 1921, where they both left Chicago to move to Washington D.C. where they began working for the War Department.[9]

While Elizebeth and William worked closely together, many of her contributions to cryptology were unique. During her time with the War Department, she and her team worked extensively on breaking ciphers used by anti-prohibitionists, smugglers and bootleggers.[10] While ciphers used by these individuals were very basic at first, they began to increase in complexity as the operations began to grow and become for financial success.[11] However, this increase in sophistication did not seem to pose a problem to Elizebeth, who mounted a number of successful attacks against substitution and transposition ciphers, both basic and complex.

During this time, Elizebeth worked at a number of government departments including the War Department, and the U.S. Treasury Department. In 1923, she was hired as a cryptanalyst for the U.S. Navy, which later led to a position with the U.S. Treasury Department's Bureau of Prohibition and of Customs. In 1927, the department established a joint effort with the Coast Guard's Intelligence Division to monitor international smuggling, drug-running, and criminal activity both in and out of the U.S. With the recent developments made in radio technology, these smugglers used encrypted radio messages to communicate, presuming they'd be able to communicate securely. However, Elizebeth and her unit were able to decrypt the messages. From 1927 to 1939, Elizebeth's unit was of great importance during a very acting period of smuggling

[8] Ibid, (149-150)
[9] Ibid, (114-115)
[10] Ibid, (133-136
[11] Ibid, (136-138)

within the United States. Her unit was eventually folded into the Coast Guard itself, where Elizebeth solved the bulk of the intercepted ciphers collected in San Francisco and Florida herself.[12] During this time she taught a number of departments on cryptology. Over the course of three years of working for the Coast Guard, the Bureau of Narcotics, the Bureau and Internal Revenue, the Bureau of Prohibition and Customs, and the Departments of Justice, she solved over 12,000 rum-runner messages and at least 24 different coding systems used by the smugglers.[13] Her work during this time led to the conviction of the narcotics smuggling Ezra Brothers and the indictment of Al Capone.[14]

In 1931 she was among the group of people that convinced Congress to create a headquartered cryptanalytic section to meet the need for a more dedicated effort against ciphered communications. Through this she began teaching other analysts cryptanalytic fundamentals and deciphering techniques. During this time, she also testified in a number of cases against accused smugglers. In 1933, her efforts had led to the convictions of 35 bootlegging ringleaders.[15] She also worked on the case of Velvalee Dickinson, known as the “Doll Woman”, a convicted Japanese spy who’s correspondence with Japan included naval vessel movements in Pearl Harbor. These materials were analyzed and solved by Elizebeth herself, which resulted in a guilty verdict against Dickinson[16]

[12] Ibid, (139-141)

[13] Kahn, David (1967). *The Codebreakers: The Story of Secret Writing*. New York, NY: Macmillan Co. Inc. p. 806.

[14] Haynes, Suyin (January 11, 2021). "How America's 'First Female Cryptanalyst' Cracked the Code of Nazi Spies in World War II—and Never Lived to See the Credit". Time.

[15] Fagone, J. (2018). *The woman who smashed codes: A true story of love, spies, and the unlikely heroine who outwitted America's enemies* (pp. 143-145). New York City, New York: Dey St., an imprint of William Morrow.

[16] Pollak, Michael (April 26, 2013). "Answers to Questions About New York". The New York Times.

During World War II, Elizebeth's Coast Guard unit was transferred to the Navy where they were the principal source of intelligence on Operation Bolivar, the German spy network in South America. Before the Pearl Harbor attacks that brought the U.S. into the war, there was concern that Nazi Germany would use Latin America to attack the U.S.[17] While the FBI were originally given the responsibility of countering this threat, the only agency with staff experienced in detecting, monitoring, and decrypting spy transmissions was Elizebeth's Coast Guard unit. Her team remained the primary U.S code breakers assigned to the South American threat where they solved numerous cipher systems used by the Germans and other Nazi sympathizers, including three seperate Enigma machines.[18] Two of these turned out to be used by Johannes Siegfried Becker, the SS agent who headed the operation in South America. By breaking this spy ring, it led to Argentina, Bolivia and Chile to break from the Axis powers and join the Allies.[19] Over the course of World War II, Friedman's team decoded 4,000 messages sent on 48 different radio circuits. Her unit also supported the recently established FBI.[20] Unfortunately, her unit was not always credited and, after the war, director J. Edgar Hoover began a public media campaign that claimed that the FBI had led the code breaking effort against the spy network in South America.[21]

[17] Fagone, J. (2018). *The woman who smashed codes: A true story of love, spies, and the unlikely heroine who outwitted America's enemies* (pp. 180-185). New York City, New York: Dey St., an imprint of William Morrow.
[18] Ibid, (185-189, 194-202)
[19] Haynes, Suyin (January 11, 2021). "How America's 'First Female Cryptanalyst' Cracked the Code of Nazi Spies in World War II—and Never Lived to See the Credit". Time.
[20] Fagone, J. (2018). *The woman who smashed codes: A true story of love, spies, and the unlikely heroine who outwitted America's enemies* (pp. 298-299). New York City, New York: Dey St., an imprint of William Morrow.
[21] Ibid, (299-300)

After Elizebeth and William had retired from government service, the two of them being Shakespeare enthusiasts, wrote a manuscript titled “The Cryptologist Looks at Shakespeare”, which was eventually published as *The Shakespearean Ciphers Examined.* In this manuscript, they addressed a number of theories regarding Shakespeare’s authorship from a scientific and cryptographic point of view, and ultimately dismissed and debunked the theory that Francis Bacon had written Shakespeare’s plays.[22] The book won a number of awards and was critically acclaimed, more so than any other book discussing the topic. The Friedman's book is regarded as the final word on the subject of the Baconian authorship theory.

Following William’s death in 1969, Elizebeth spent much of her retirement compiling a library and bibliography of her husband's work. This collection is lodged in the George C. Marshall Research Library in Lexington, Virginia, and is regarded as the most extensive private collection of cryptographic material in the world. [23]

Elizabeth Smith Friedman’s received a great deal of recognition for her contributions, but unfortunately most of these were posthumous. In 1999, she was inducted to the NSA Hall of Honor, and in 2002 the NSA’s OPS1 building in Fort Meade, Maryland was dedicated as the William and Elizebeth Friedman Building during the NSA’s 50th Anniversary Commemoration. [24] In April of 2019, the U.S. Senate passed a resolution for the purpose of “Honoring the life and

[22] Friedman, William F.; Friedman, Elizebeth S. (1957). *The Shakespearean Ciphers Examined: An Analysis of Cryptographic Systems Used As Evidence That Some Author Other Than William Shakespeare Wrote the Plays Commonly Attributed to Him*. Cambridge: Cambridge University Press.

[23] Joyce, Maureen (November 2, 1980). "Elizebeth Friedman Dies, Cryptanalyst, Pioneer in the Science of Code-Breaking". The Washington Post.

[24] "Elizebeth S. Friedman — 1999 Hall of Honor Inductee"

legacy of Elizebeth Smith Friedman, Cryptanalyst".[25] Finally, in July 2020, the U.S. Coast Guard announced that it had named the 11th Legend-Class National Security Cutter in honor of Elizebeth Smith Friedman.[26]

Cypher PC Game

Once he had a good handle of Elizebeth's story, we needed to figure out the best way to show that story in a PC game format. We also needed to establish a strong sense of how we wanted the game to look and feel. In order to do that, we looked for other games revolving cryptography that we could use as inspiration. The first game we found was a game called *Cypher*.

Fig 1: Opening shot of *Cryptogram*

[25] "Senate Passes Wyden-Fischer Resolution Recognizing WWII Codebreaker Elizebeth Friedman". wyden.senate.gov. April 2, 2019.

[26] "Eleventh National Security Cutter Named for Elizebeth Smith Friedman". U.S. Coast Guard.

Cypher is a first person puzzle game developed for the PC. The game presents the player with a stark white building designed to resemble a library or museum with several different wings. Each wing represents a different type of cryptography, with descriptions and puzzles presented as if they were museum exhibits. The wings of the museum consist of sections covering steganography, transposition, monoalphabetic and polyalphabetic substitution, mechanised and digital cryptography, and an additional wing for extra challenge puzzles.

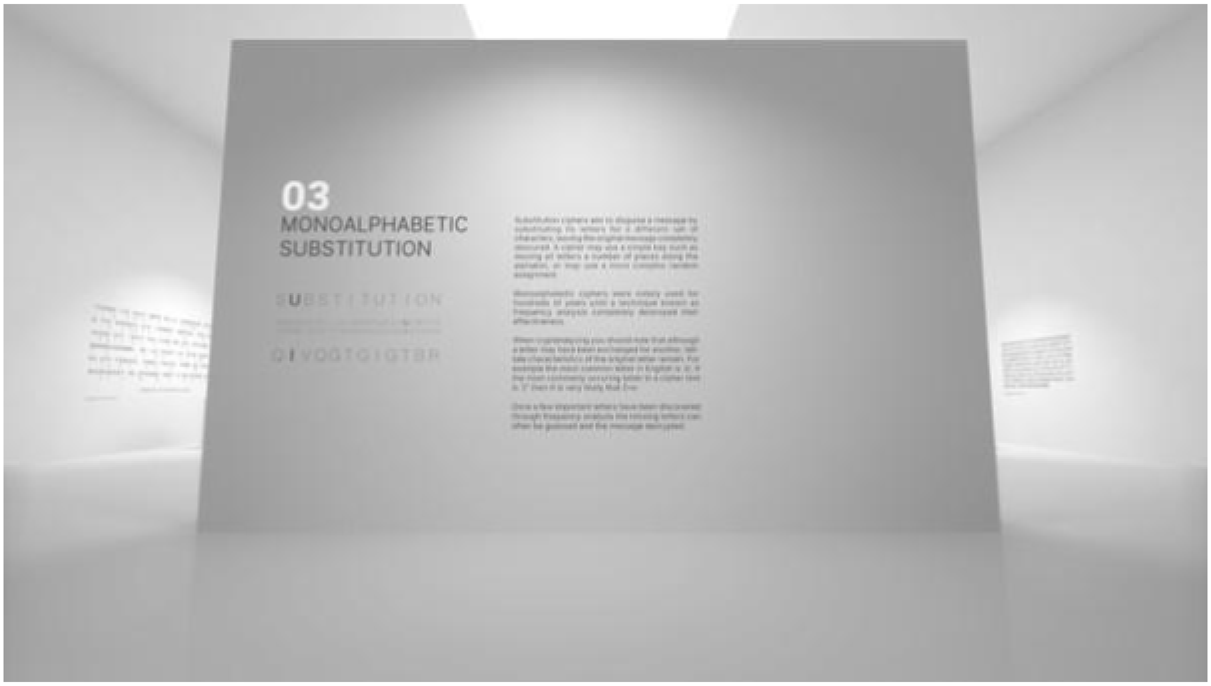


Fig 2: 3rd level/wing of *Cryptogram* "museum"

Each wing presents the player with a description of the type of cryptography and a total of five puzzles to solve, with the puzzles increasing in difficulty as the player progresses. When the player approaches one of the "exhibits", the puzzle will display on the wall behind a small computer-like terminal (see Fig 3).

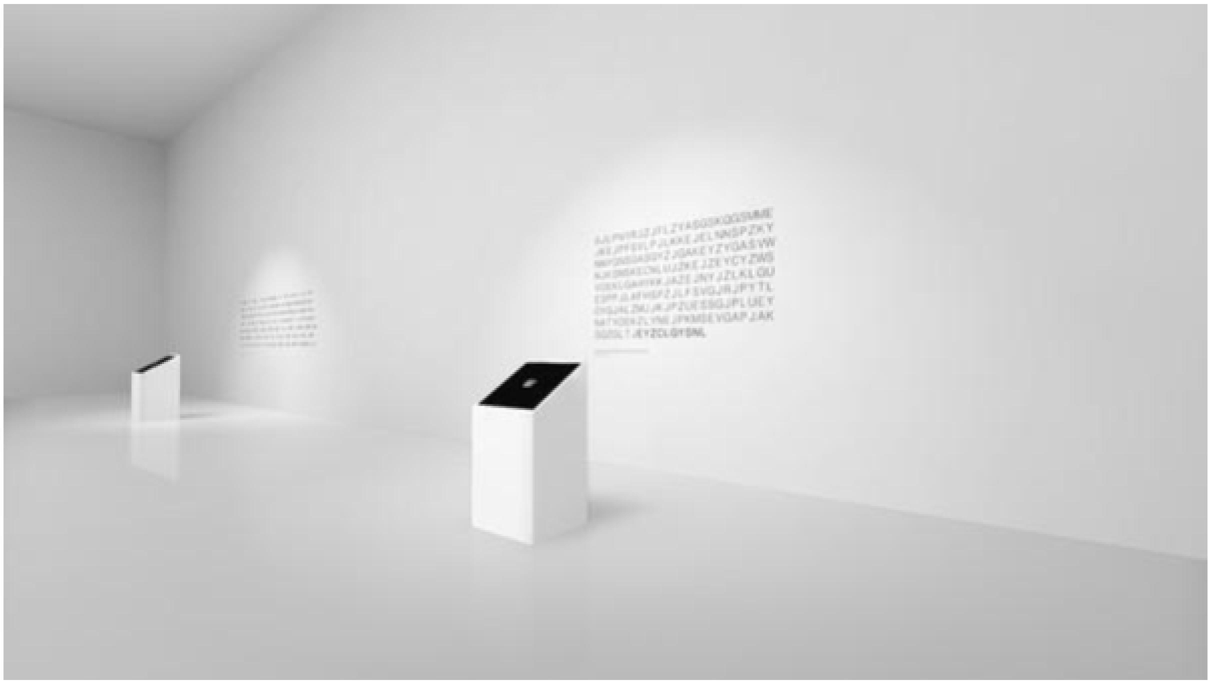
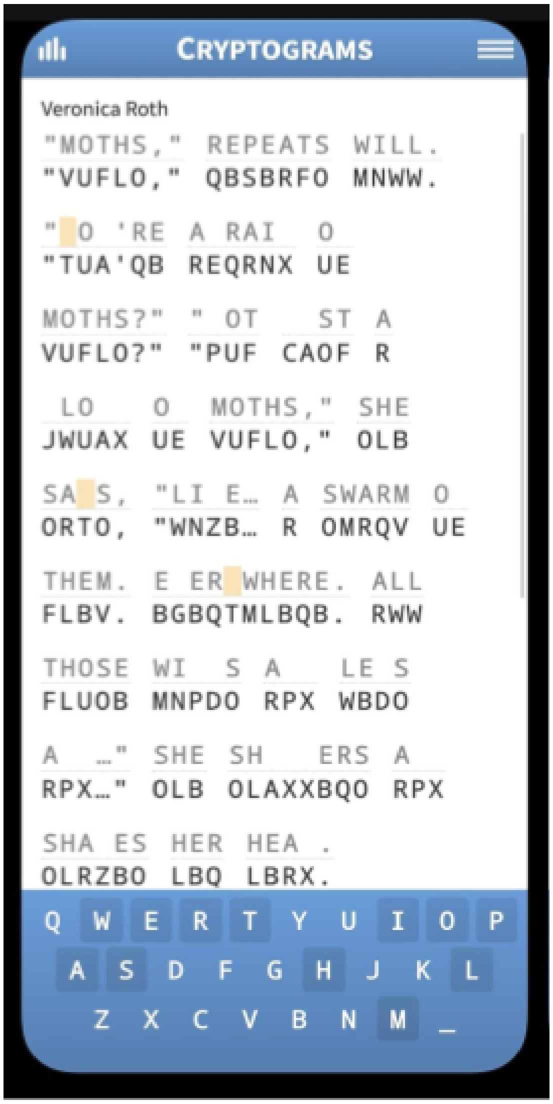


Fig 3: Example of the input interface for a puzzle

Once the player has solved the puzzle on their own, likely outside of the game with pencil and paper, they can interact with the terminal to input their answer. Once the player fully completes each wing of the museum, the final door opens which leads to optional challenge puzzles as well as the ending of the game.

While we had planned from the beginning to make our game menu based instead of an interactive environment, *Cypher* gave us a strong idea of how to present our puzzles and descriptions of said puzzles in a clear and concise way. It also gave us an example of the proper way to increase difficulty using puzzles that are inherently meant to be difficult to solve.

Cryptogram Mobile Game



Veronica Roth

"MOTHS," REPEATS WILL.
"VUFLO," QBSBRFO MNWW.

" O 'RE A RAI O
"TUA'QB REQRNX UE

MOTHS?" " OT ST A
VUFLO?" "PUF CAOF R

LO O MOTHS," SHE
JWUAX UE VUFLO," OLB

SA S, "LI E… A SWARM O
ORTO, "WNZB… R OMRQV UE

THEM. E ER WHERE. ALL
FLBV. BGBQTMLBQB. RWW

THOSE WI S A LE S
FLUOB MNPDO RPX WBDO

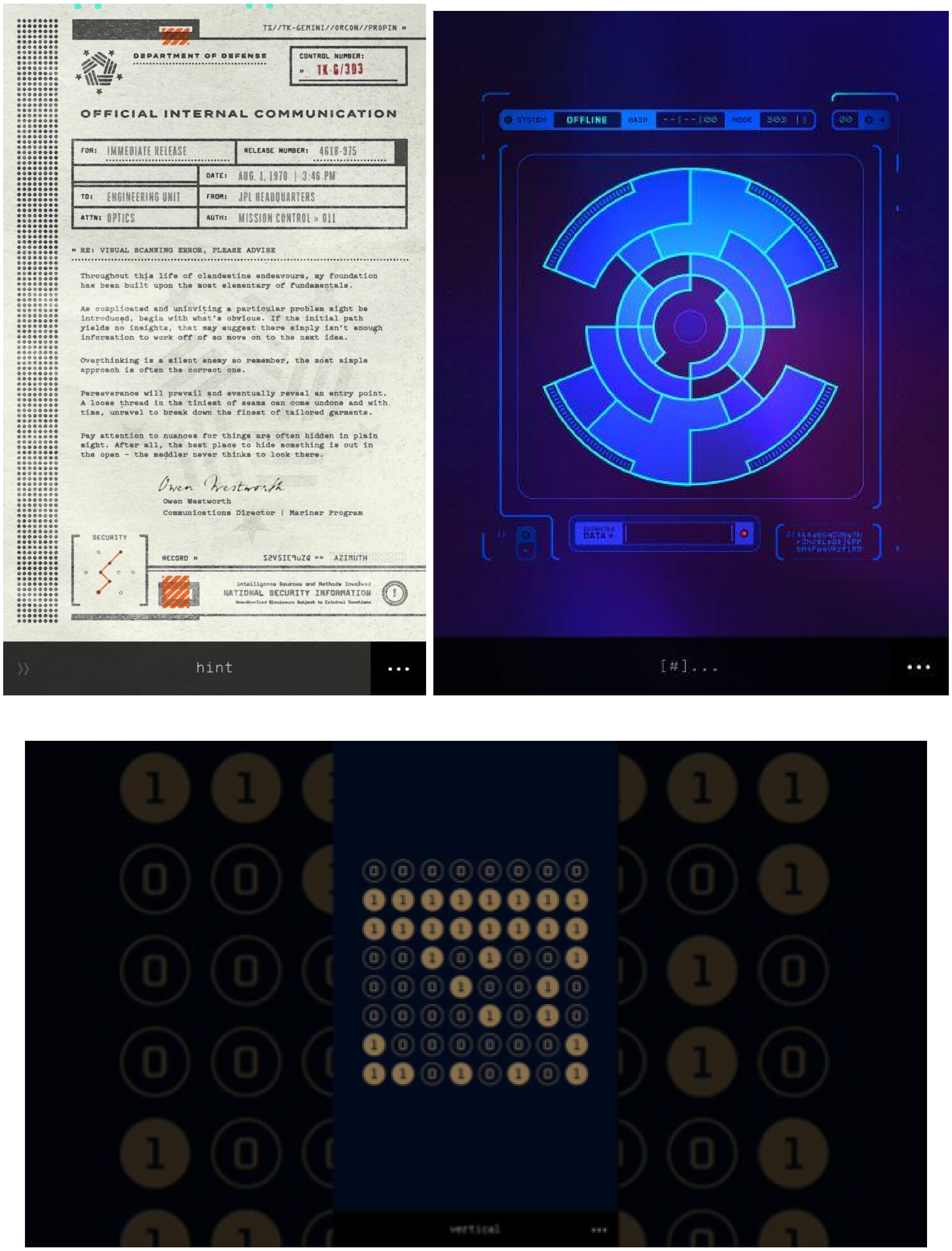
A …" SHE SH ERS A
RPX…" OLB OLAXXBQO RPX

SHA ES HER HEA .
OLRZBO LBQ LBRX.

Fig 4: Screenshot of a quote from a Veronica Roth book in *Cryptogram*

Cryptogram is a rather simple mobile game that presents a number of famous quotes from ten popular categories like ancient wisdom, celebrities, comedy, philosophy, politicians and sports. Each quote is presented as a cryptogram using a substitution cipher simple enough to be solved by hand, similar to games like *Wheel of Fortune*. While simple, the layout and presentation of this game was the basis of how we would build our UI for the substitution cipher, with each letter of the ciphertext below a series of squares that players would click on and input the letter related to that substitution. It also gave us the idea of having other instances of the same letter autofill when the player entered the letter in a single space.

The Guides/The Guides Axiom Mobile Game



TS//TK-GEMINI//ORCON//PROPIN «

DEPARTMENT OF DEFENSE

CONTROL NUMBER:
» TK-6/303

OFFICIAL INTERNAL COMMUNICATION

FOR: IMMEDIATE RELEASE
RELEASE NUMBER: 4618-975
DATE: AUG. 1, 1970 | 3:46 PM
TO: ENGINEERING UNIT
FROM: JPL HEADQUARTERS
ATTN: OPTICS
AUTH: MISSION CONTROL » 011

» RE: VISUAL SCANNING ERROR, PLEASE ADVISE

Throughout this life of clandestine endeavours, my foundation has been built upon the most elementary of fundamentals.

As complicated and uninviting a particular problem might be introduced, begin with what's obvious. If the initial path yields no insights, that may suggest there simply isn't enough information to work off of so move on to the next idea.

Overthinking is a silent enemy so remember, the most simple approach is often the correct one.

Perseverance will prevail and eventually reveal an entry point. A loose thread in the tiniest of seams can come undone and with time, unravel to break down the finest of tailored garments.

Pay attention to nuances for things are often hidden in plain sight. After all, the best place to hide something is out in the open – the meddler never thinks to look there.

Owen Westworth

Owen Westworth
Communications Director | Mariner Program

SECURITY

RECORD »
S2VSIE9uZQ == AZIMUTH

Intelligence Sources and Methods Involved
NATIONAL SECURITY INFORMATION
Unauthorized Disclosure Subject to Criminal Sanctions

0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1
0	0	1	0	1	0	0	1
0	0	0	1	0	0	1	0
0	0	0	0	1	0	1	0
1	0	0	0	0	0	0	1
1	1	0	1	0	1	0	1

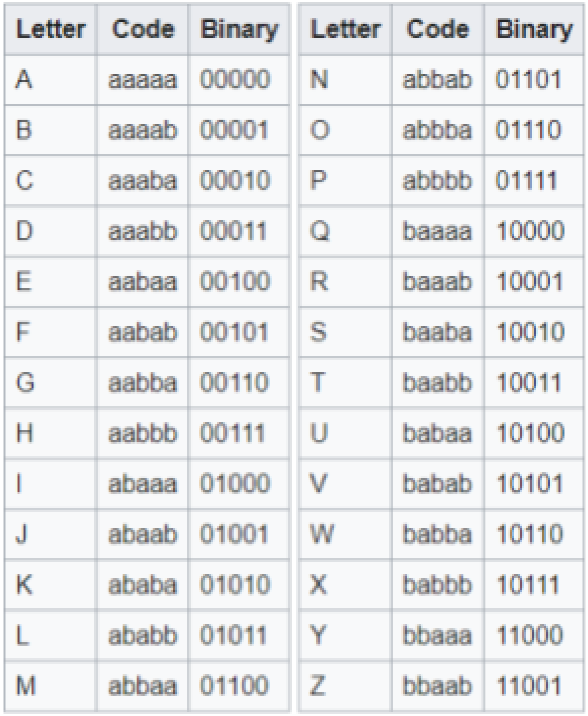
Fig 5-7: Screenshots from both games in the *The Guides* series

The Guides series of games are mobile games that challenge players with a number of codes, puzzles and interactive ciphers that are presented in strange and unique ways. Both games require the player to think outside the box to solve puzzles, using things like their phones rotation and taking screenshots to solve different puzzles. The game is presented with a mysterious, almost hacker like point of view. While the game was a bit too complex and out of the box for what we would end up creating, it was still an interesting way to view what sorts of fantastic and impressive mechanics could be implemented with the simple backbone of solving puzzles and ciphers.

Types of Ciphers

Once we had completed our research on Elizebeth, we then needed to figure out which cipher's we wanted to utilize in our game. In our initial pitch, we realized that we could separate the major parts of Elizebeth's career into three timelines, each one being represented by a specific type of cipher. These timelines are as follows: The Bacon cipher to represent Elizebeth's time at Riverside, the substitution cipher to represent her time working against smugglers, and finally the Enigma cipher during her time working on Project Bolivar. Once that was decided, we then of course needed to do research on the ciphers themselves.

First, we looked at the Bacon cipher. While the Bacon cipher being a way that Sir Francis Bacon hid his authorship of Shakespeare's works was debunked, the Bacon cipher by itself is an actual cipher that was created by Bacon in 1605 in a book titled *The Proficience and Advancement of Learning Divine and Humane.* The Bacon cipher is a method of message encoding that conceals a message in the presentation of text rather than the content of the text. To encode a message, each letter of the plaintext (the unencrypted message) is replaced by a group of five of the letters ‘A’ or ‘B’ (see Fig 8).



Letter	Code	Binary	Letter	Code	Binary
A	aaaaa	00000	N	abbab	01101
B	aaaab	00001	O	abbba	01110
C	aaaba	00010	P	abbbb	01111
D	aaabb	00011	Q	baaaa	10000
E	aabaa	00100	R	baaab	10001
F	aabab	00101	S	baaba	10010
G	aabba	00110	T	baabb	10011
H	aabbb	00111	U	babaa	10100
I	abaaa	01000	V	babab	10101
J	abaab	01001	W	babba	10110
K	ababa	01010	X	babbb	10111
L	ababb	01011	Y	bbaaa	11000
M	abbaa	01100	Z	bbaab	11001

Fig 8: Bacon alphabet table of letters to AB strings and binary

The writer then makes use of two different typefaces for the cipher. After creating a false message with the same number of letters as all of the As and Bs, each letter of the false message is presented in the appropriate typeface, with one representing As and the other Bs. To decode the message, this method is applied in reverse with each “typeface 1” replaced with an A and each “typeface 2” replaced with a B. The Baconian alphabet is then used to recover the original message. The different typefaces can be anything the encoder wishes.[27]

[27] Helen Fouché Gaines, *Cryptanalysis: a Study of Ciphers and Their Solutions* (1989), page 6

For our purposes, we simply used bolded and non-bolded letters. For example, a message using our format would look something like this:

“Whic**h** now that s**u**bj**ect**s m**er**i**t**s doth rehearse”

The message is then rewritten with As and Bs and made into groups of five, removing the extra letters at the end:

aaaab aaaaa aaaba abbba abbab

And using the Baconian alphabet, the answer is: BACON

There were of course struggles when attempting to decode what were believed to be ciphers from Shakespeare’s writings, as Elizebeth and William would discover. Due to these documents being written and printed in the 16th century, there were many instances of what looked to be different typefaces in the text, when in actuality they were errors and artifacts due to the archaic nature of the 16th century printing press. The Friedman’s would discuss in their memoire that while the Bacon cipher is a real way of encoding messages, the methods being used by people that believed that Bacon wrote Shakespeare were persuasive, and that these people were creating rules to find secret messages that were either flawed as methods, or imperfect in their findings.[28]

This problem extended to our game as well, which was not intended at first but turned out to be an excellent layer of realism. The font we chose for our game was designed to look like

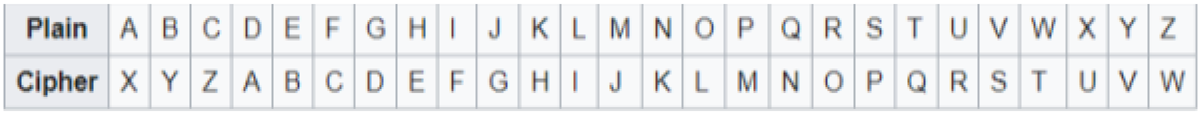
[28] Friedman, William F.; Friedman, Elizebeth S. (1957). *The Shakespearean Ciphers Examined: An Analysis of Cryptographic Systems Used As Evidence That Some Author Other Than William Shakespeare Wrote the Plays Commonly Attributed to Him*. Cambridge: Cambridge University Press.

typewriter writing, and some letters look more bold than others, regardless of if they are actually bolded as part of the cipher. This led to a bit of frustration on behalf of our players, but also helped them to understand the same challenge and frustration Elizebeth felt during her early years at Riverside.

Our second cipher is the substitution cipher. This cipher, as Elizebeth learned, can start simple but become very complex, as there are many different variations of substitution that can be used. These variations can include simple substitutions, a cipher that operates on single letters, polygraphic substitution, which operates on larger groups of letters, monoalphabetic ciphers, which use a fixed substitution over an entire message, and polyalphabetic ciphers, which use a number of different substitutions throughout the entire text. For our purposes, we stuck with the simplest form as it was the easiest to implement and explain to players. The simple substitution, also known as the Caesar cipher, is a form of substitution cipher in which each letter in the plaintext is replaced by a letter with some fixed number of positions down the alphabet.[29] For example, if the alphabet is shifted to the left by three letters, the letter D would be replaced with A, E would become B, etc.

As a visual example, a Caesar cipher alphabet could look like this:

[29] Singh, Simon (2000). *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography*



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
Cipher	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W

Fig 9: Example of Ceaser cipher alphabet, right shift by three

When encrypting, a person would look at the letter of the message in the plain line, and write down the corresponding letter in the cipher line. A message using this format would look like this:

Plaintext: THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG

Cipher Text: QEB NRFZH YOLTK CLU GRJMP LSBO QEB IXWV ALD

Deciphering is done in reverse, by shifting the letters to the right by three.[30]

Finally, we took a look at the Enigma machine, one of the most well known and difficult ciphers to be used, at least until it was broken. The Enigma machine was developed in the early to mid 20th century and was employed extensively by Nazi Germany during World War II, where Elizebeth first encountered its use.[31]

[30] Wobst, Reinhard (2001). Cryptology Unlocked. Wiley. p. 19

[31] "EnigmaHistory". cryptomuseum.com.

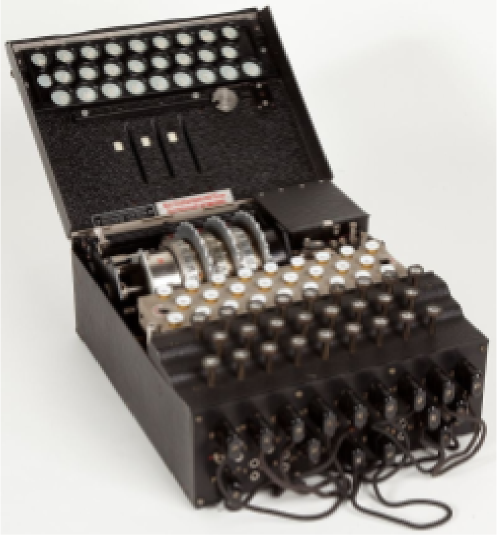


Fig 10: A three rotor variation of an Engima Machine

The Enigma machine has an electromechanical rotor mechanism that scrambles the 26 letters of the alphabet. The machine functions similarly to a typewriter in visuals and design. To encode a message using it, one person enters text on the Enigma's keyboard while another person writes down which of the 26 lights above the keyboard is illuminated at each key press. If plain text is entered, the lit up letters are the encoded ciphertext. Entering ciphertext transforms it back into readable plaintext. While this may seem simple at first, the machine had added security measures. The rotors and lampboard could be given different settings which changed the output of codes. These settings were generally changed daily during the war, with some settings even being changed for each message. This made breaking the code near impossible if one did not have the machine settings at the time that the message was created. This of course changed in

1932 when Polish mathematician and cryptanalyst Marian Rejewski finally broke the code using a theory of permutations and flaws in the German ciphering process.[32]

It should be noted, that while our original vision was to add the Enigma machine to our game, it was not implemented. The reasons for this are explained in the Post Mortem section of this paper

Experience Design

Target Audience

1. 18+ but there’s no reason younger, interested people wouldn’t be able to play.
2. Fans of puzzle games
3. People interested in cryptography and cryptanalysis
4. People wishing to learn about important female figures of US history.

Codesmasher has two parts: the story and the ciphers. So our target audience are those who are interested in one of those genres. These can be players of puzzle and text adventure games, or lovers of history. Thus, we are trying to meet both of these expectations with interesting ciphers and engaging stories. However, a player may only be interested in one aspect. For example, a player more interested in the story may not be interested in spending the time decoding ciphers. To avoid them getting disappointed or frustrated from failing to decode, we decided to build a detailed tutorial and hint system. The tutorial is presented through a series of messages given from Elizebeth’s point of view that walk the player through the first cipher on

[32] Simkim, John. "Enigma Machine". *Spartacus Educational.* Spartacus Educational.

their own, and then let them complete the next two encryptions on their own. In addition, our hint system can be used to clear parts of the message to give players a head start. If the player is still stuck and frustrated, asking for enough hints will give the player the answer so they can continue on. This way, if a player is more interested with Elizebeth's story than decoding messages, they can move ahead.

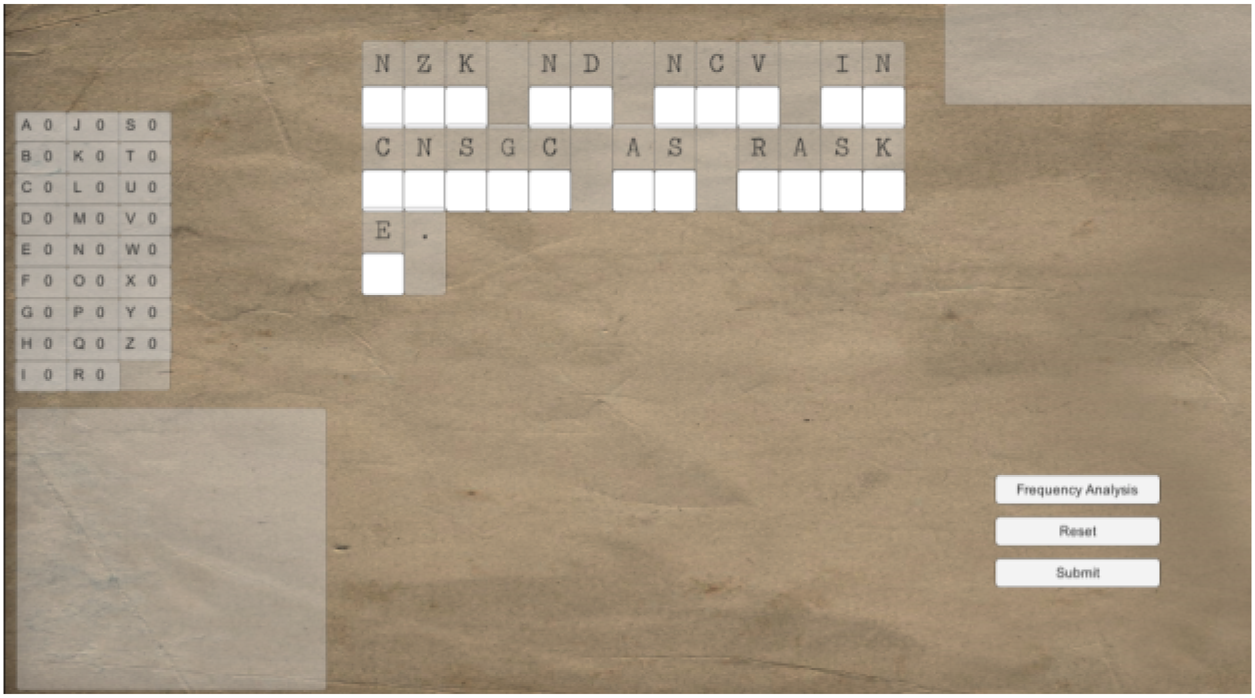
Experience Goals

The main experience goal of *Codesmasher* is to allow players to discover Elizebeth Smith Friedman's story and the history of decoding through decrypting and solving ciphered messages. Players will become Elizebeth's apprentice of sorts, with her being a helpful voice teaching you how to solve codes. By experiencing how Elizebeth Smith Friedman decoded the ciphers that existed during her life, players may not only learn about those ciphers and gain accomplishment from decoding them, but also get a better understanding of her story.

Art Design

Art Direction

In terms of art direction and a general theme, we had a solid view from the beginning. We wanted the theme of our visuals to represent the time period that Elizebeth worked during. As such, we designed our game to simulate a typewriter writing on old paper in a typewriter style font. Below is an early pass at what our puzzle interface would look like:

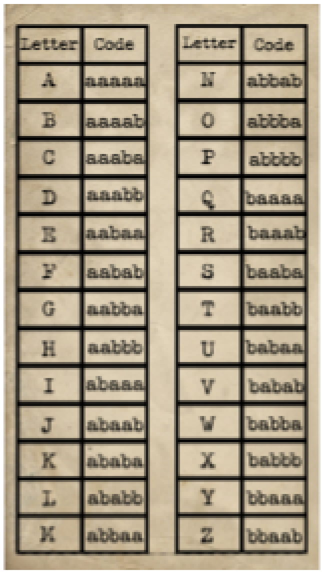


NZK ND NCV IN
CNSGC AS RASK
E.

A 0	J 0	S 0
B 0	K 0	T 0
C 0	L 0	U 0
D 0	M 0	V 0
E 0	N 0	W 0
F 0	O 0	X 0
G 0	P 0	Y 0
H 0	Q 0	Z 0
I 0	R 0	

Fig 11: Early iteration of our substitution cipher interface

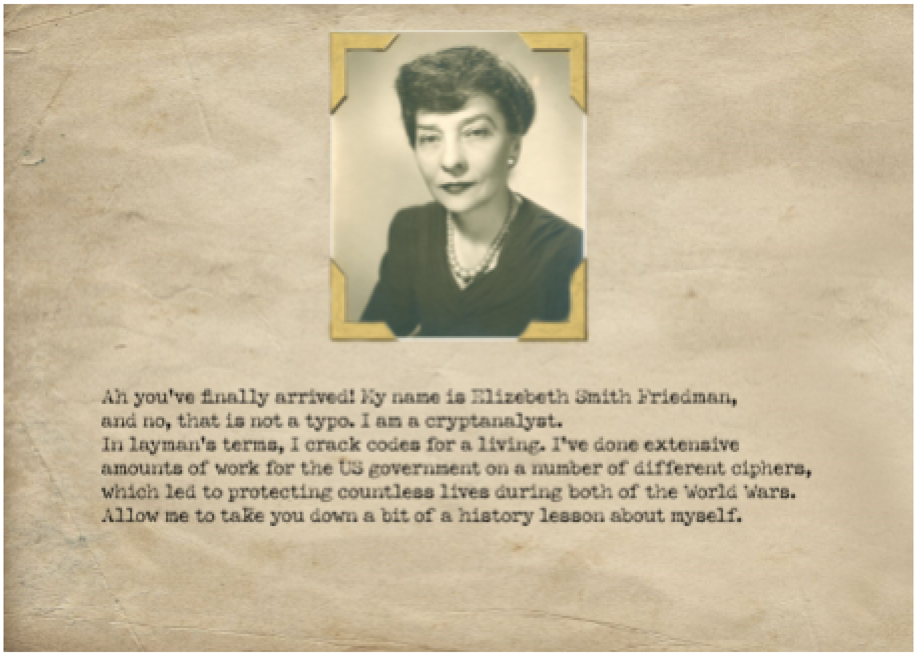
In addition, we needed to create a Baconian alphabet for the player to use, so we designed this in a similar way to look like an old piece of parchment:



Letter	Code	Letter	Code
A	aaaaa	N	abbab
B	aaaab	O	abbba
C	aaaba	P	abbbb
D	aaabb	Q	baaaa
E	aabaa	R	baaab
F	aabab	S	baaba
G	aabba	T	baabb
H	aabbb	U	babaa
I	abaaa	V	babab
J	abaab	W	babba
K	ababa	X	babbb
L	ababb	Y	bbaaa
M	abbaa	Z	bbaab

Fig 12: Modified Bacon cipher alphabet. Binary equivalents were removed as they were unnecessary and it made the decoding process too complicated

Next, we wanted to include cutscenes of a sort from Elizebeth's point of view that described her life. These would play in between different ciphers and would be presented from her point of view. For these, we decided on designing them based off of a scrapbook like visual, keeping with the same font and old parchment feel. Images would be shown corresponding to the story that was being told, and they would look as if they were in scrapbook frames. An example would be something like this:



Ah you've finally arrived! My name is Elizebeth Smith Friedman,
and no, that is not a typo. I am a cryptanalyst.
In layman's terms, I crack codes for a living. I've done extensive
amounts of work for the US government on a number of different ciphers,
which led to protecting countless lives during both of the World Wars.
Allow me to take you down a bit of a history lesson about myself.

Fig 13: Cutscene example with an image of Elizebeth

We then needed buttons that could be used for the interface and the main menu. Staying with the typewriter aesthetic, we found images of blank typewriter buttons and added the necessary font to them. This made the main menu look something like this:

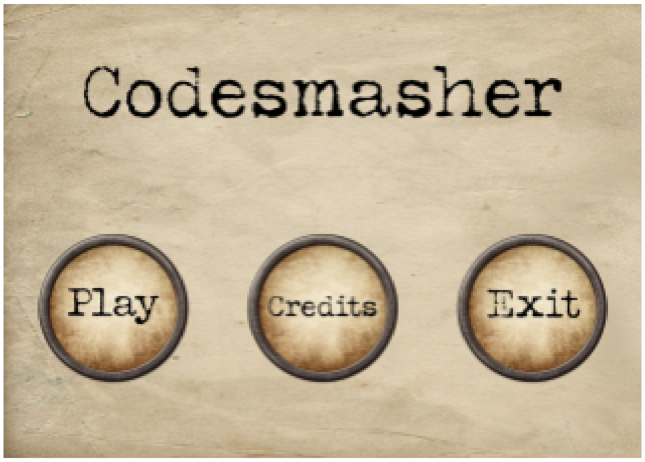


Fig 14: Main Menu

With these combined elements, we felt like we had captured a good visual aesthetic that would fit with the subject material and still be visually pleasing.

Fonts

As mentioned above, we wanted the font to have an almost antique look, reminiscent of typewriters or old printing presses. We decided to go with a font titled *Typeka* which gave an excellent similarity to typewriter font, but was still clear and easy to read.

This font choice did come with a few drawbacks however. When creating the Bacon cipher, the two typefaces we used were simply non bolded and bolded letters. Unfortunately, the *Typeka* font shows very little change when bolded. This led to some confusion among testers when decoding these ciphers as it was hard to tell which letters were bolded and which were not. While this was certainly frustrating for some, we decided to keep this font anyway. Our reasoning was for a connection to the subject material. The Baconian Shakespeare theory, as surmised by the Friedmans, was believed to simply be errors in the antique printing techniques that caused markings in Shakespeare's text that resembled a possible code. As such, keeping this "error" in our font actually made the game more historically accurate to the sort of work Elizebeth needed to do in order to solve Bacon ciphers. In addition, players would be able to compare one letter with another instance of the same letter in order to try and differentiate the two. This will be explained further in the Technical Design section below.

User Interface

For the user interface design, we first made a paper prototype. Below, you can see an example of the title screen in the prototype. However we decided to split this into a title scene and a menu scene in later versions.

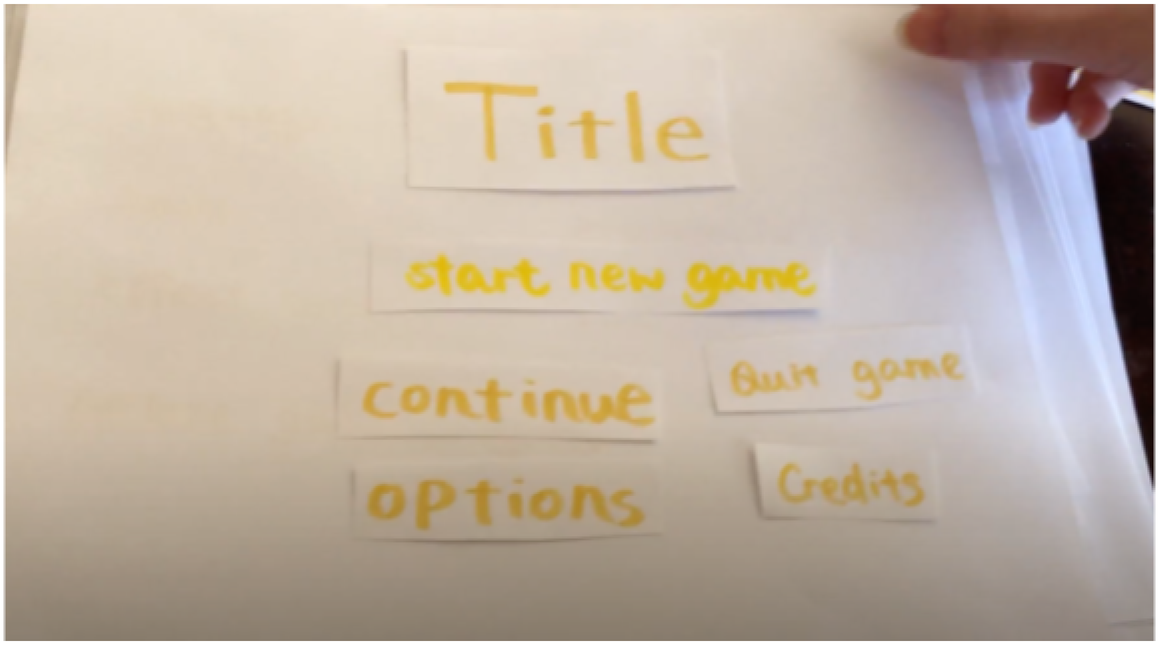
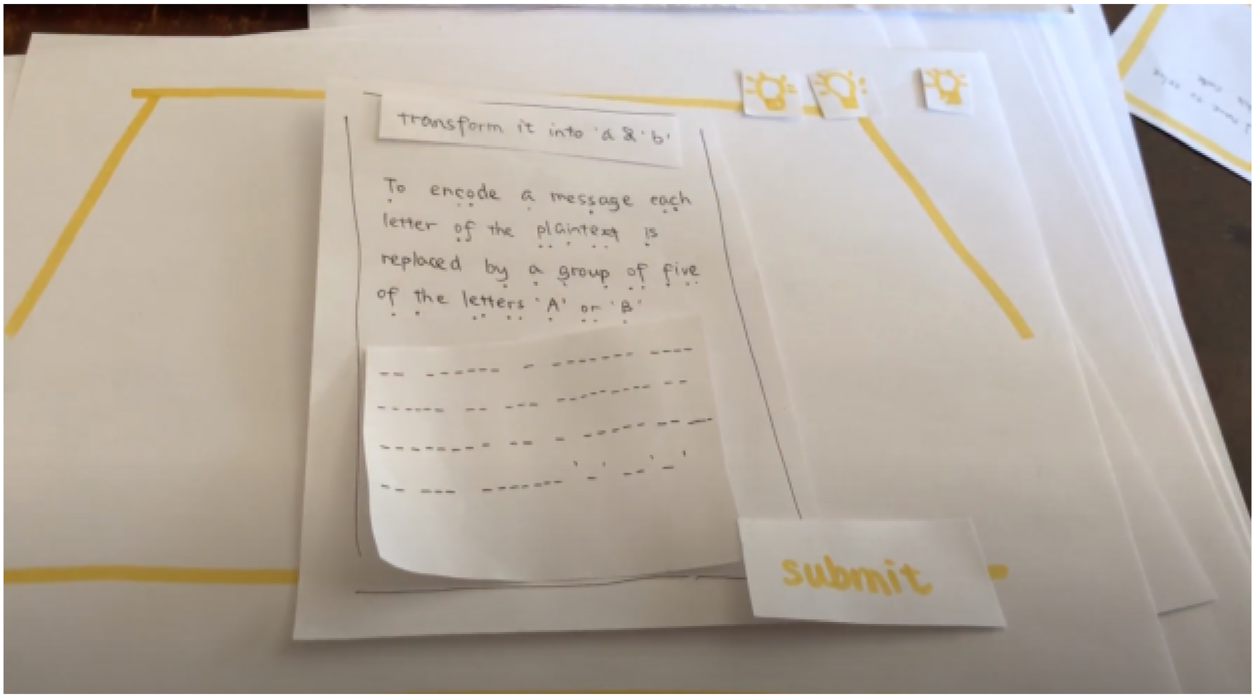


Fig 15: Title Scene of Paper Prototype

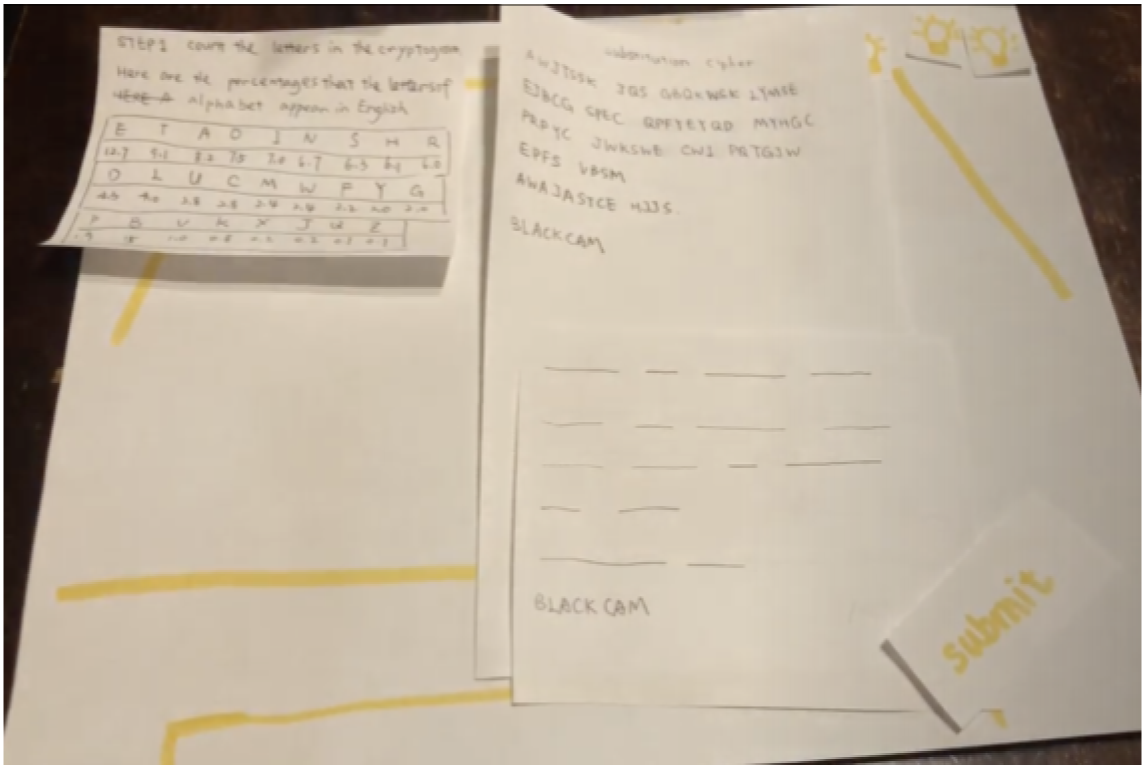
The prototype interface we designed for the bacon cipher only had the hints, code panel, input panel and the submit button. Later, after our first playtesting on the code system, we found it rather hard for the players to understand what they should do next with only a sentence on the top of the code panel as a tutorial. In addition, only having a submit button makes the game harder than we expected, as if a player makes a mistake, they won't know where that mistake was made without a way to check their answer.



To encode a message each letter of the plaintext is replaced by a group of five of the letters 'A' or 'B'

Fig 16: Bacon Cipher Interface of Paper Prototype

For the substitution cipher, we made the paper prototype version look almost the same as the bacon cipher, only we moved the tutorials into the left part of the screen. We made the ciphered text and answer panel separate and players have to input the characters one by one to fill in the answer.



STEP1 count the letters in the cryptogram

Here are the percentages that the letters of ~~HERE A~~ alphabet appear in English

E	T	A	O	I	N	S	H	R
12.7	9.1	8.2	7.5	7.0	6.7	6.3	6.1	6.0
D	L	U	C	M	W	F	Y	G
4.3	4.0	2.8	2.8	2.4	2.4	2.2	2.0	2.0
P	B	V	K	X	J	Q	Z	
1.9	1.5	1.0	0.8	0.2	0.2	0.1	0.1	

substitution cipher

AWJTSSK JQS QAQKWEK LYWSE
EJBCG CPEC QPFYEYQD MYHGC
PRDYC JWKSWE CWI PRTGJW
EPFS VBSM
AWAJASTCE HJJS.

BLACKCAM

BLACK CAM

Fig 17: Substitution Cipher Interface of Paper Prototype

For the mockup version of the bacon cipher interface, added some new functions to enrich the experience of decoding. We added a picture of Elizebeth to make the whole process more like a conversation with her. The check button and last input panel were added for checking the input and telling what was wrong to the players.

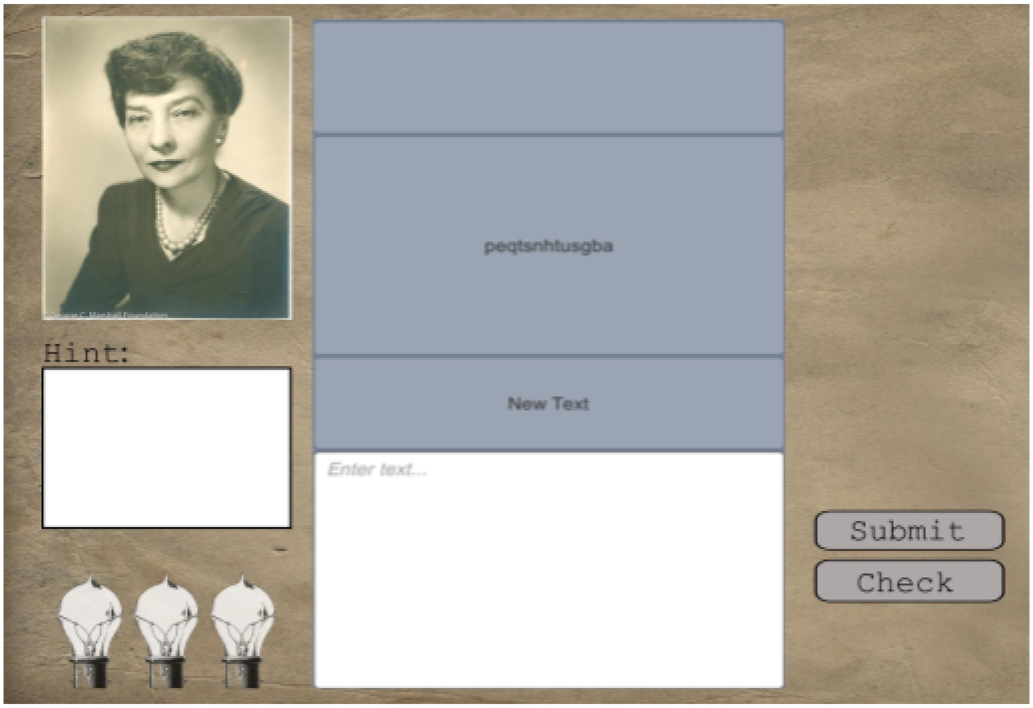


Fig 18: Digital Prototype

The final version of the title and menu scenes are separated, and the previous design of the game workspace was based on paper on a desk. We cut down the desk part and left the paper background to make it neat and clean.

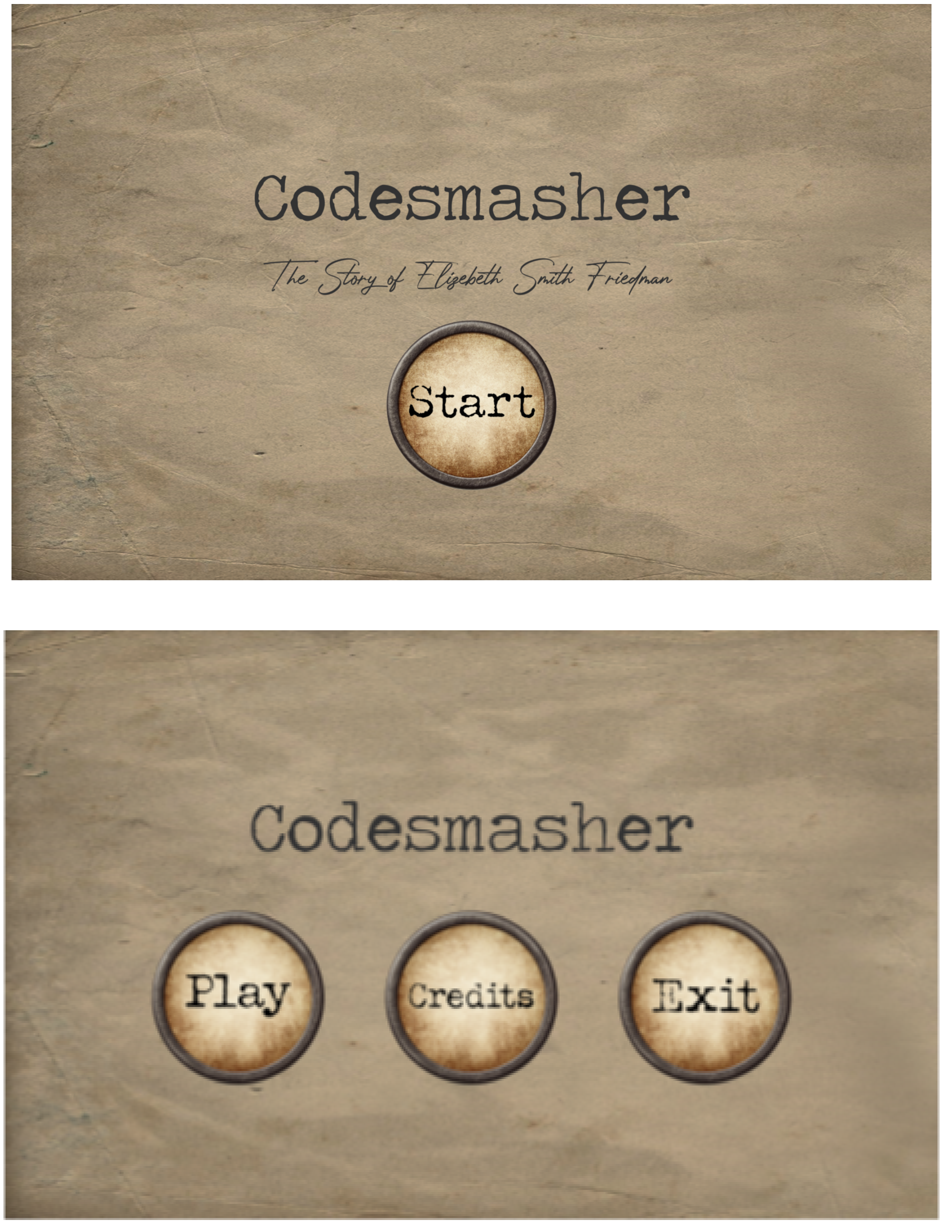
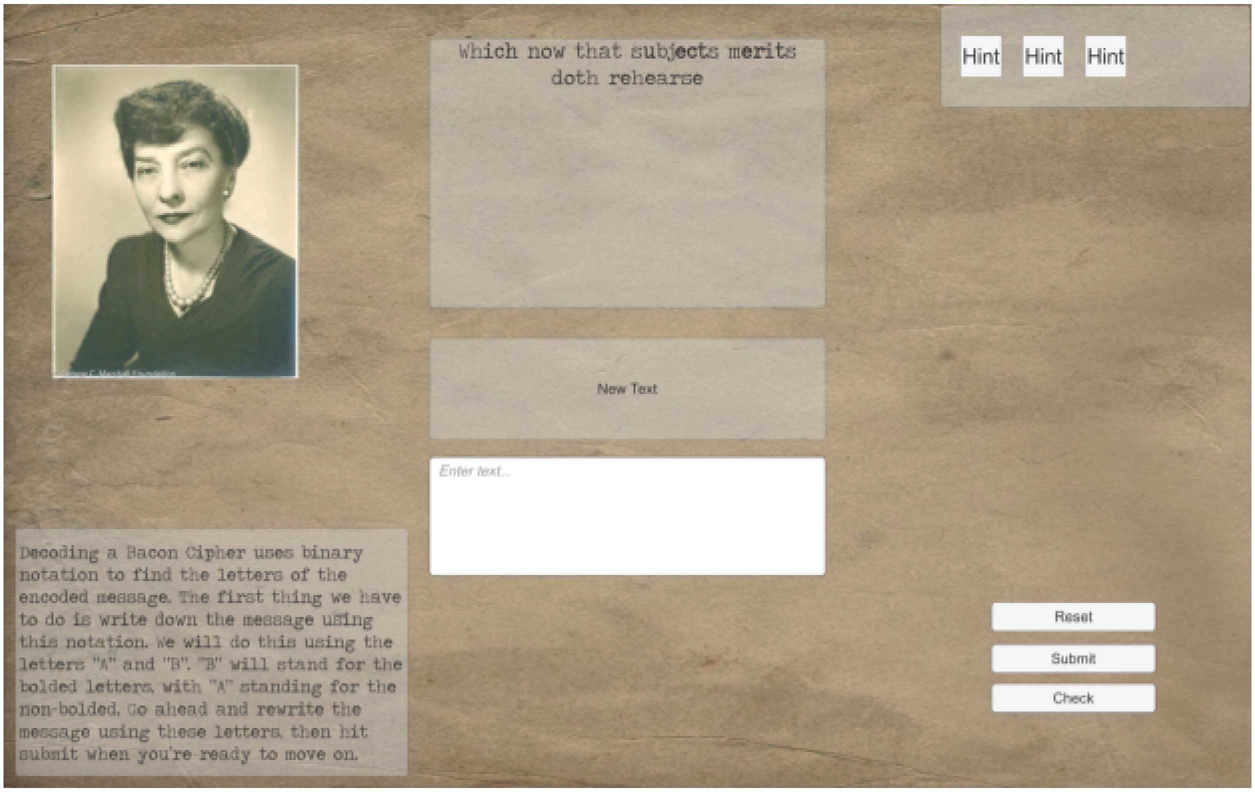


Fig 19-20: Title Scene in Game

As for the bacon cipher, despite the check button we added from the mockup version, we added a new Reset button which can turn the answer panel into the last successful submit as each step of decoding the bacon cipher is connected to the following step. Also, the tutorials are no longer one sentence for a step. It is much more detailed compared to the ones before, more like an informal conversation.

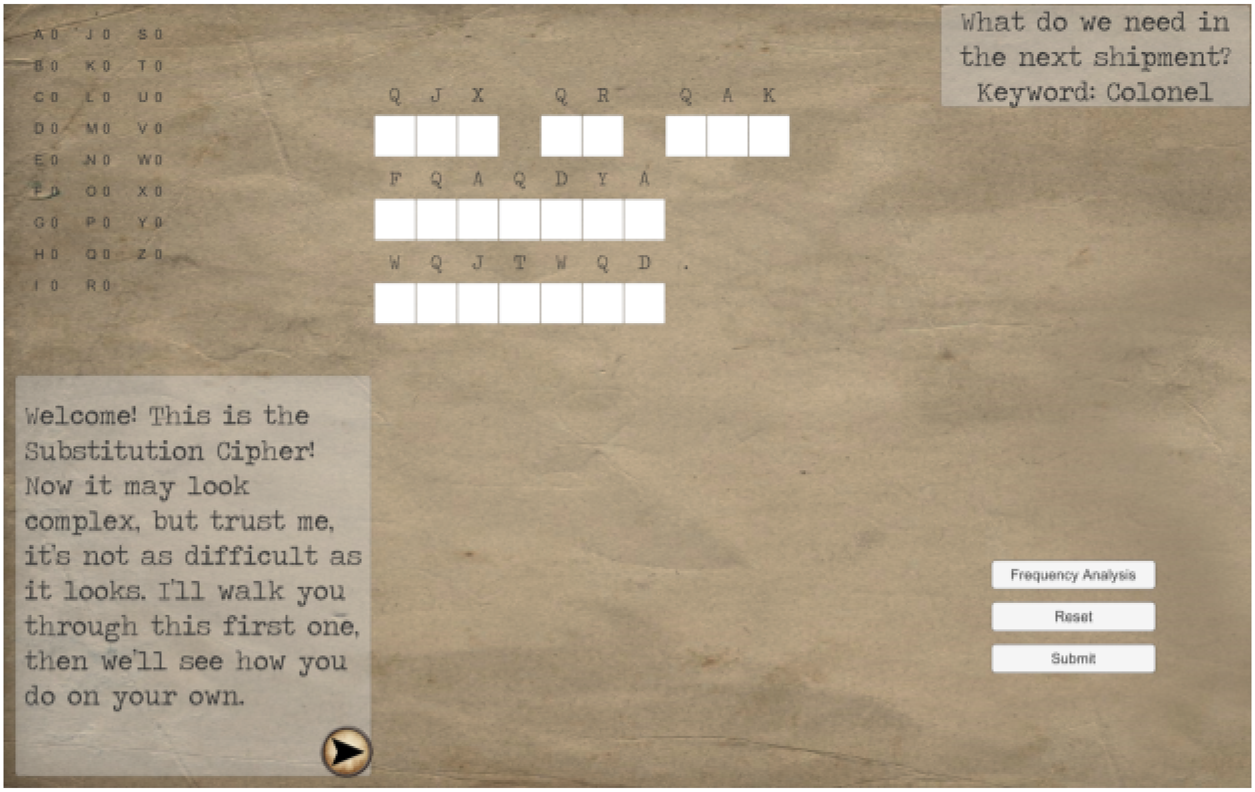


Which now that subjects merits doth rehearse

Decoding a Bacon Cipher uses binary notation to find the letters of the encoded message. The first thing we have to do is write down the message using this notation. We will do this using the letters "A" and "B". "B" will stand for the bolded letters, with "A" standing for the non-bolded. Go ahead and rewrite the message using these letters, then hit submit when you're ready to move on.

Fig 21: Bacon Cipher Interface in Game

The user interface for substitution cipher changed a lot. The ciphered text and answer panel are combined together and the frequency analysis panel was added to help players know the frequency of each letter. As for the tutorial part, because the substitution cipher doesn't have clear steps, this part is made into paragraphs.



A 0	J 0	S 0
B 0	K 0	T 0
C 0	L 0	U 0
D 0	M 0	V 0
E 0	N 0	W 0
F 0	O 0	X 0
G 0	P 0	Y 0
H 0	Q 0	Z 0
I 0	R 0	

What do we need in the next shipment? Keyword: Colonel

QJX QR QAK

FQAQDYA

WQJTWQD.

Welcome! This is the Substitution Cipher! Now it may look complex, but trust me, it's not as difficult as it looks. I'll walk you through this first one, then we'll see how you do on your own.

Fig 22: Substitution Cipher Interface in Game

Audio Design

Unfortunately due to time restraints we were unable to implement audio to our build at the time of writing this. With that being said, we do have a solid idea of what audio we want to add, and may implement it into later builds on itch.io. First, we want music to be playing in the background of the game that is not too distracting to the player. We also want this music to fit with the aesthetic and the subject material of our game. To do so, we chose several jazz songs from the early 1910s into the 20s. This way, the music being played could have possibly been music that Elizebeth listened to herself. Also, since the majority of the songs were written and recorded before 1925, they would be within the public domain. Secondly, we want some sort of interface sound to interact with the player. The obvious choice for this would be the sound of a typewriter keyboard when the player types and clicks on buttons around the interface.

Technical Design

All ciphers in *Codesmasher* are generated from answers and plain texts automatically, so that we didn't need to set up every cipher each time we want a new one. It also prevented us from making any mistakes while doing so.

Bacon Cipher

The bacon cipher requires the combination of answers and plain texts. To get the code, we first transform the answer into an AB string and make it the same length of the plain text so that we can save it directly as a step answer. Then, spaces will be inserted into the AB string as they are in the plain text. Finally, we inserted bolded characters as Bs in the plain text to make the ciphered message using rich text function in unity.

Substitution Cipher

We used a string of the alphabet to contain the whole 26 letters in English to form the substitution cipher. A dictionary of how they are substituted is made by the string and a randomly shifted string of it. Then we use the dictionary to make the message encoded. After that, each letter in the ciphered message will call a prefab and set the text to that prefab. After typing in the box in the prefab, another dictionary for the answer will be filled in and every other prefab that has the same ciphered letter will automatically fill in the box with the same letter. To check the answer, we use the answer dictionary to translate the ciphered message and compare it with the original one.

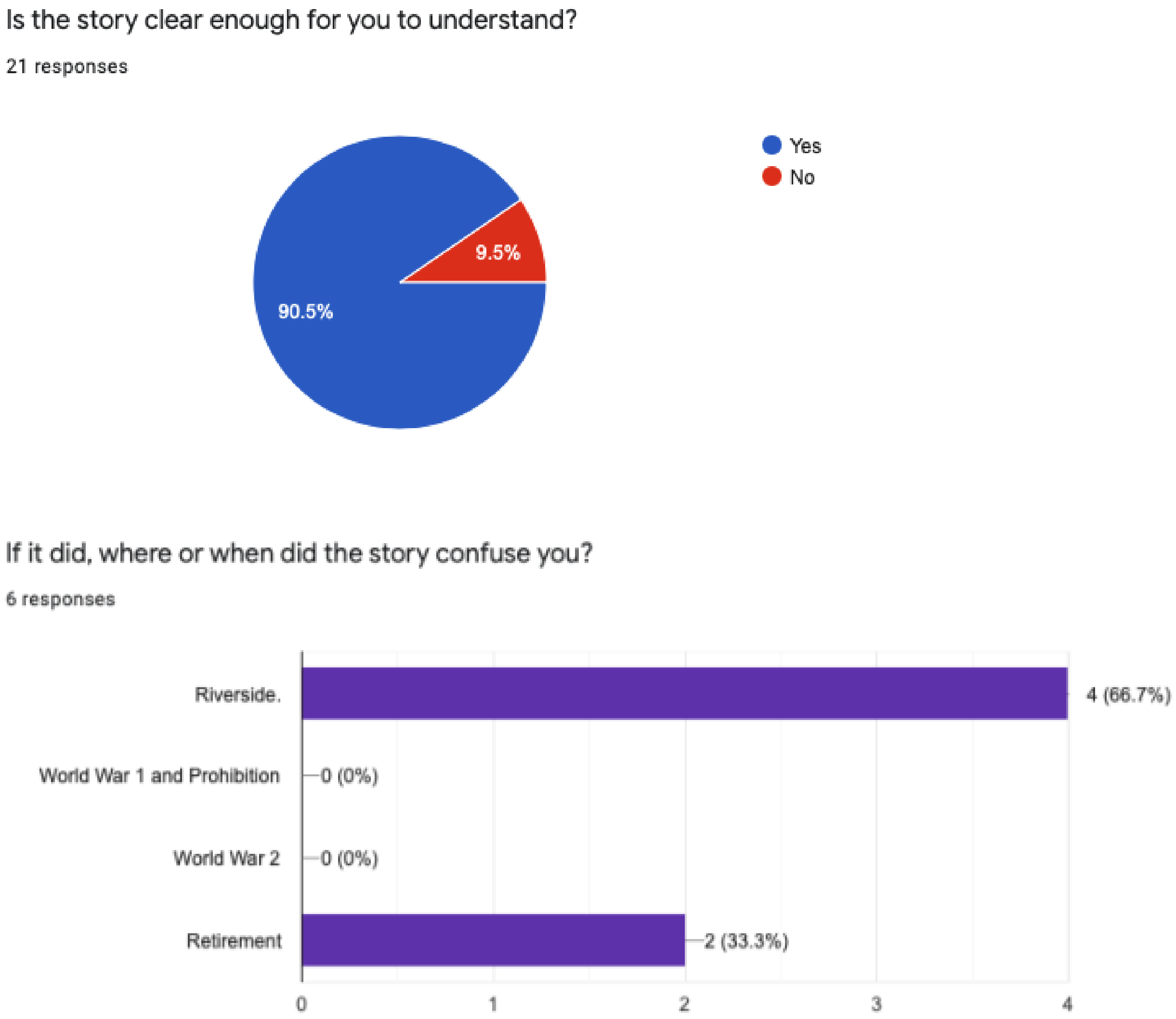
Assessment

To get reviews from our target audience and make sure our experience goals were accomplished, we ran several play testing sessions after testing it ourselves and clearing up any bugs. Through our testing, we gained great feedback from a number of testers, who helped to adjust the difficulty and make the tutorial clear and readable. In addition, in case testers fail to complete our game or misunderstand, especially because most of them are non-native speakers of English, we helped them during the whole process, giving them hints when they were stuck. Our assistance during play may influence their judgement of the difficulty of our game, but it was still better for our uses to see them get through the whole game.

In total, we got 21 playtesters who went through the process. We made one-on-one testing and each test took about 1 hour. We recruited playtesters from our friends and other students who showed interest in our game.

Playtesting About the Story

To combine the history of Elizebeth and the ciphers, we made the story several parts and put the ciphers in between.



Is the story clear enough for you to understand?

21 responses

If it did, where or when did the story confuse you?

6 responses

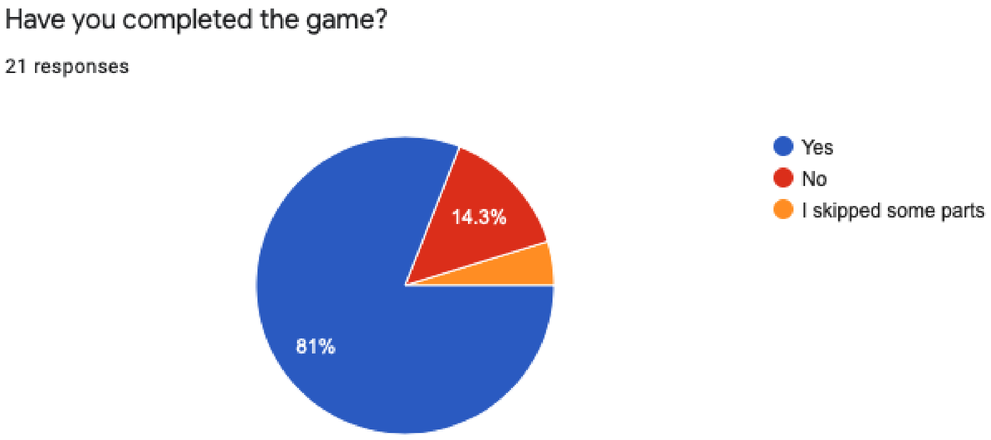
Fig 23-24: The Results of Playtesting in Story

From the responses we received, over 90% of the playtesters thought the story part of *Codesmasher* was clear enough to understand. And for those who didn't, 4 out of 6 testers chose Riverside, the beginning of Elizebeth's cryptology career and when she was decoding bacon ciphers, as the part that made them confused. The remaining testers that answered this question all chose the retirement period as the most confusing part.

From the feedback of the long text question about the story, most testers told us they actually enjoyed the story in the game and thought it is clear enough to understand. One tester wanted more languages in the story part for non-native speakers, since the story in *Codesmasher* is quite long and requires time to read. Another tester liked the way *Codesmasher* tells the story as if Elizebeth herself is talking to you.

Playtesting About the Code System

Most playtestings of the code system were trying to balance the difficulty of each cipher. Mostly, questions were asked about where players stopped and why. Although most of the testers got stuck somewhere during the game, still over 80% of the testers completed the whole game. 19 out of 21 players went through the bacon ciphers while 16 out of 21 passed the substitution ciphers. Only two testers were unable to complete any.



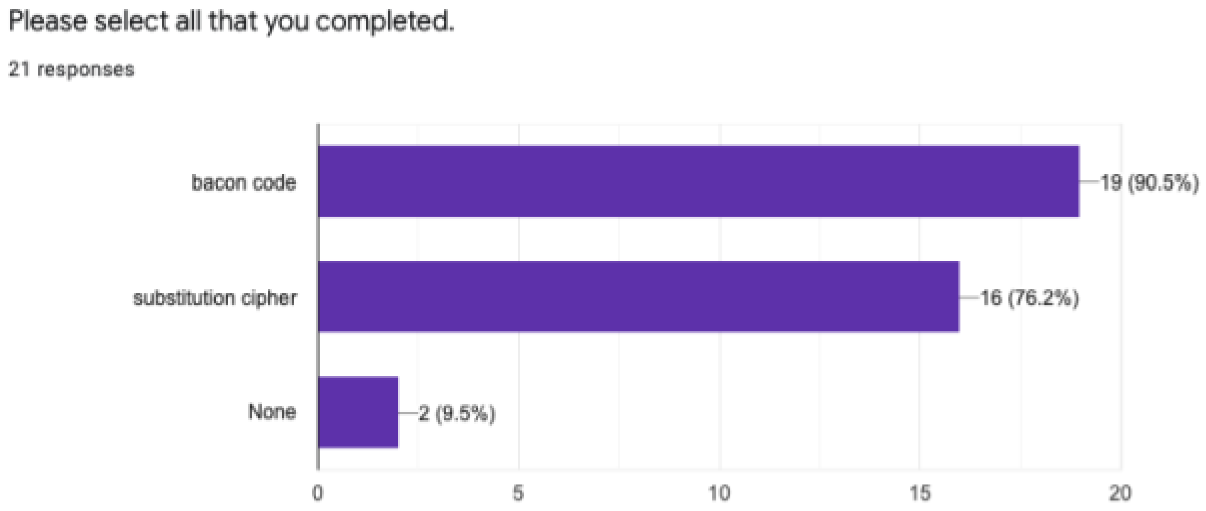
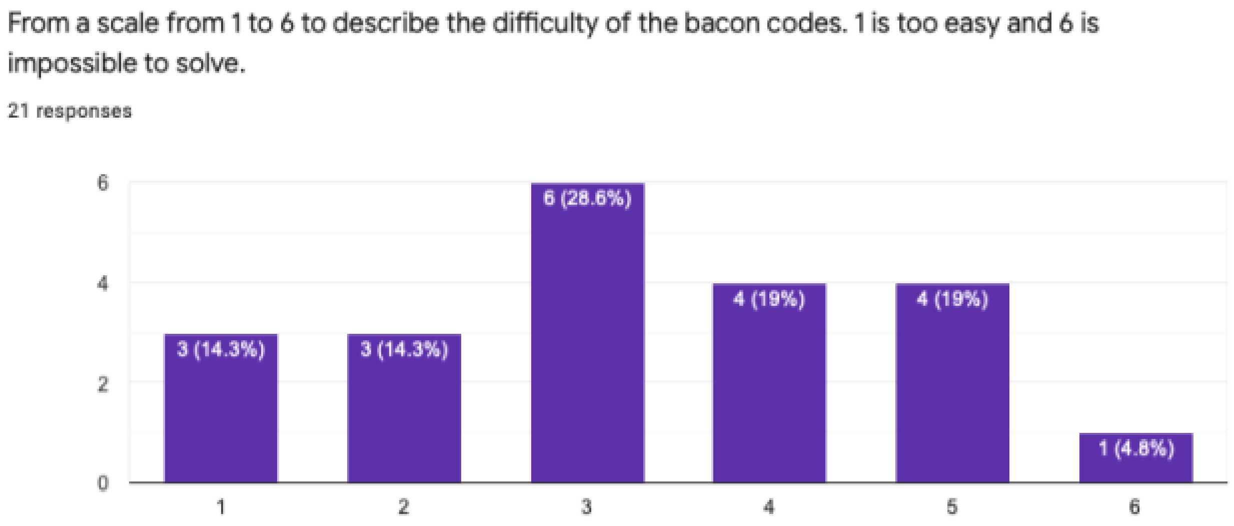


Fig 25-26: The Results of Playtesting in Whole Game Difficulty

Bacon Cipher

For the bacon cipher, only 1 out of 21 testers thought it was too difficult and were unable to solve it. But other testers were evenly distributed on every difficulty level, with the majority of them agreeing that the difficulty level is above a 3.

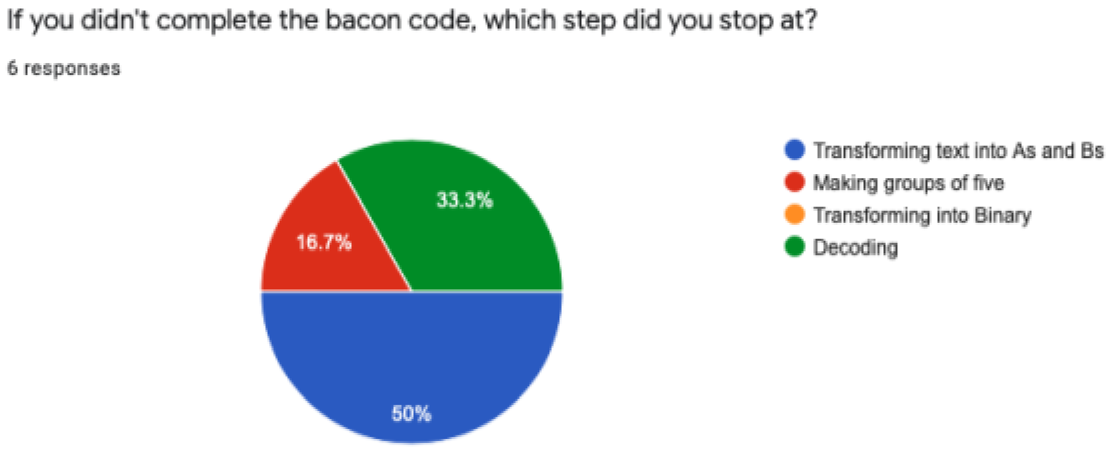


From a scale from 1 to 6 to describe the difficulty of the bacon codes. 1 is too easy and 6 is impossible to solve.

21 responses

Fig 27: The Playtesting Results of Difficulty in Bacon Cipher

For those who didn't finish the bacon cipher, 50% of the testers stopped at transforming the text into As and Bs, which was the main problem we could see while playtesting. The type writer font we chose has some characters that look bolder than others, which makes it hard to identify if they are bolded because of the bacon cipher, or because of the font.



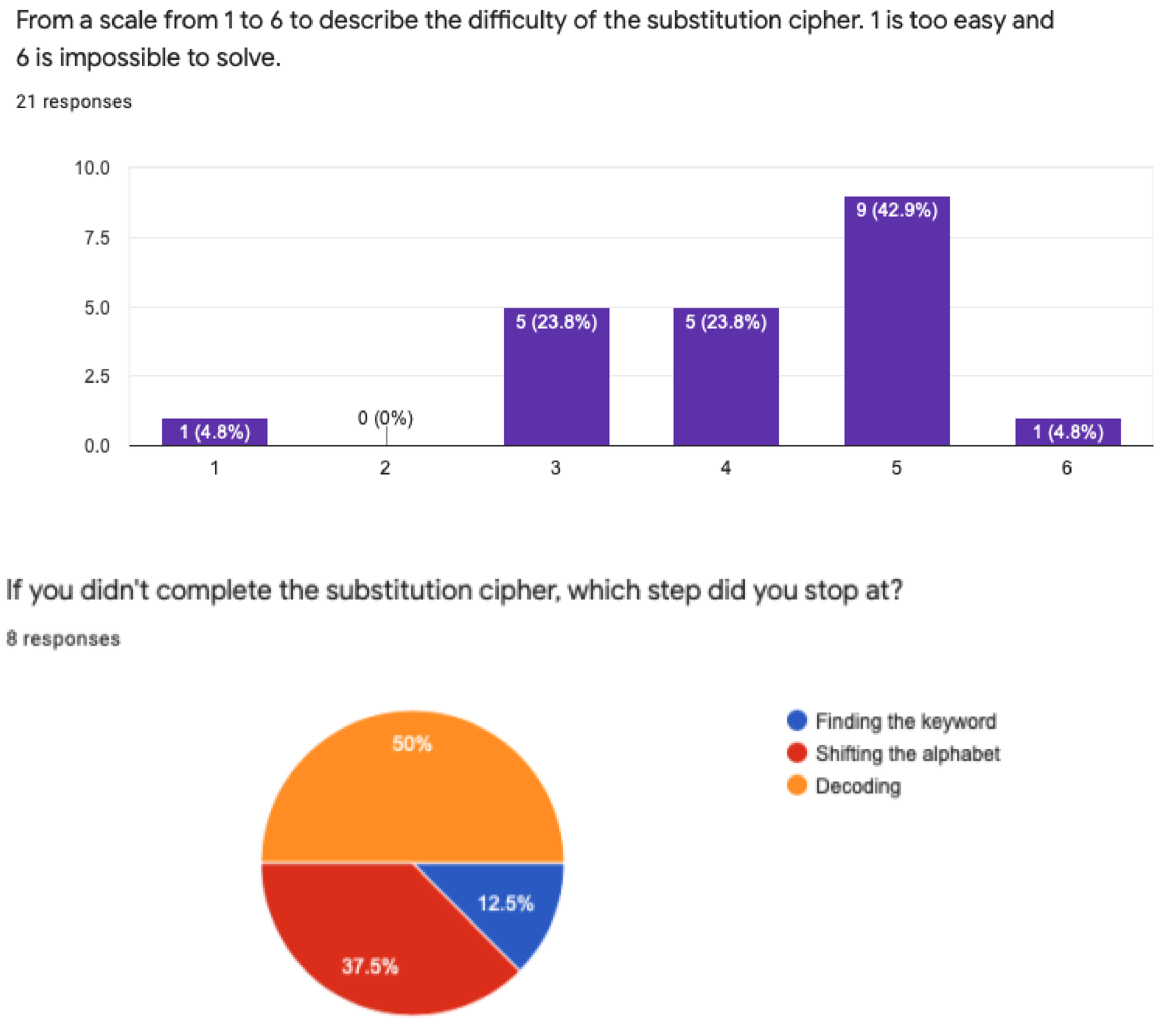
If you didn't complete the bacon code, which step did you stop at?

6 responses

Fig 28: The Playtesting Result of Steps in Bacon Cipher

Substitution Cipher

For the substitution cipher, most players thought it was quite difficult yet not impossible to solve, and the hardest part for them was decoding the cipher.



From a scale from 1 to 6 to describe the difficulty of the substitution cipher. 1 is too easy and 6 is impossible to solve.

21 responses

If you didn't complete the substitution cipher, which step did you stop at?

8 responses

Fig 29-30: The Playtesting Results of Substitution Cipher

Post Mortem

Future Work and Distribution

Enigma Cipher

As mentioned earlier, the enigma cipher was at first designed to be part of our game. However, it was scrapped during development as it would not only prove difficult for our players to solve, but was also very difficult to program as a digital tool. We didn't want *Codesmasher* to be too serious to have fun with. Players shouldn't be upset after playing our game. So in the future, we would like to add a simplified version of the enigma cipher, telling players how Elizebeth dealt with it and let them try parts of the decoding process instead of the entire thing.

More Interaction

In the current version of *Codesmasher*, we have story and code elements in the game. However it still looks more like a tutorial rather than a full game. To this, we plan to add more interactions into *Codesmasher* in later versions. The stories will not be only told with texts and photos, but also in the form of dialog, images, and interactive backgrounds. Players may enjoy it more like a detective game and have fun with discovering the stories rather than passively gaining the information.

George C. Marshall Research Library

The final piece of future work and distribution that we are looking towards is to make some sort of connection with the George C. Marshall Research Library. As mentioned earlier in this paper, the GCM Research Library contains an extensive archive of both Elizebeth and William Friedman's work. This includes interviews, memoirs, pictures and documents from the Friedman's career, many submitted by Elizebeth herself when she was alive. We believe that it would be a great opportunity to reach out to the GCM Research Library once our game is polished and published and see if they would have any interest in working with us or hosting our game in Elizebeth's collection. Our original goal was to bring more awareness to Elizebeth and her work, and a connection to the GCM Research Library would be a great first step.

Conclusion

While the game is a good way to tell Elizebeth's story, it may not be a very fun game to play. As can be seen in our evaluations, the majority of players seemed to enjoy the story of Elizebeth Smith Friedman, but many more people had trouble with the decoding process or found it boring. In addition, even those that completed the game, most of them required additional assistance from us in order to solve the different puzzles. In the future, we hope to continue developing this game to make it more accessible to a casual audience by lowering the difficulty of the ciphers as much as possible, adding music and additional player interaction, and overall polishing the player experience. We plan on uploading this game to itch.io for people to view while we continue modifying and polishing it, and if all goes well, reach out to the George C. Marshall Research Library to establish a possible connection between the collection of the Friedman's work and our game. All in all, the main takeaway from this project is that Elizebeth Smith Friedman was a fascinating woman and an extremely talented codebreaker that contributed a great deal to the art of cryptography and likely saved countless lives in both World Wars. It is our hope that with our game we will be able to bring more knowledge and appreciation to one of the many talented women from our history.

Bibliography

Fagone, J. (2018). *The woman who smashed codes: A true story of love, spies, and the unlikely heroine who outwitted America's enemies.* New York City, New York: Dey St., an imprint of William Morrow.

Kahn, David (1967). *The Codebreakers: The Story of Secret Writing.* New York, NY: Macmillan Co. Inc. p. 806.

Haynes, Suyin (January 11, 2021). "How America's 'First Female Cryptanalyst' Cracked the Code of Nazi Spies in World War II—and Never Lived to See the Credit". Time.

Pollak, Michael (April 26, 2013). "Answers to Questions About New York". The New York Times.

Friedman, William F.; Friedman, Elizebeth S. (1957). *The Shakespearean Ciphers Examined: An Analysis of Cryptographic Systems Used As Evidence That Some Author Other Than William Shakespeare Wrote the Plays Commonly Attributed to Him.* Cambridge: Cambridge University Press.

Joyce, Maureen (November 2, 1980). "Elizebeth Friedman Dies, Cryptanalyst, Pioneer in the Science of Code-Breaking". The Washington Post.

"Elizebeth S. Friedman — 1999 Hall of Honor Inductee"

"Senate Passes Wyden-Fischer Resolution Recognizing WWII Codebreaker Elizebeth Friedman". wyden.senate.gov. April 2, 2019.

"Eleventh National Security Cutter Named for Elizebeth Smith Friedman". U.S. Coast Guard.

Helen Fouché Gaines, *Cryptanalysis: a Study of Ciphers and Their Solutions* (1989)

Wobst, Reinhard (2001). Cryptology Unlocked. Wiley.

"EnigmaHistory". cryptomuseum.com.

Simkim, John. "Enigma Machine". *Spartacus Educational.* Spartacus Educational

Singh, Simon (2000). The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography

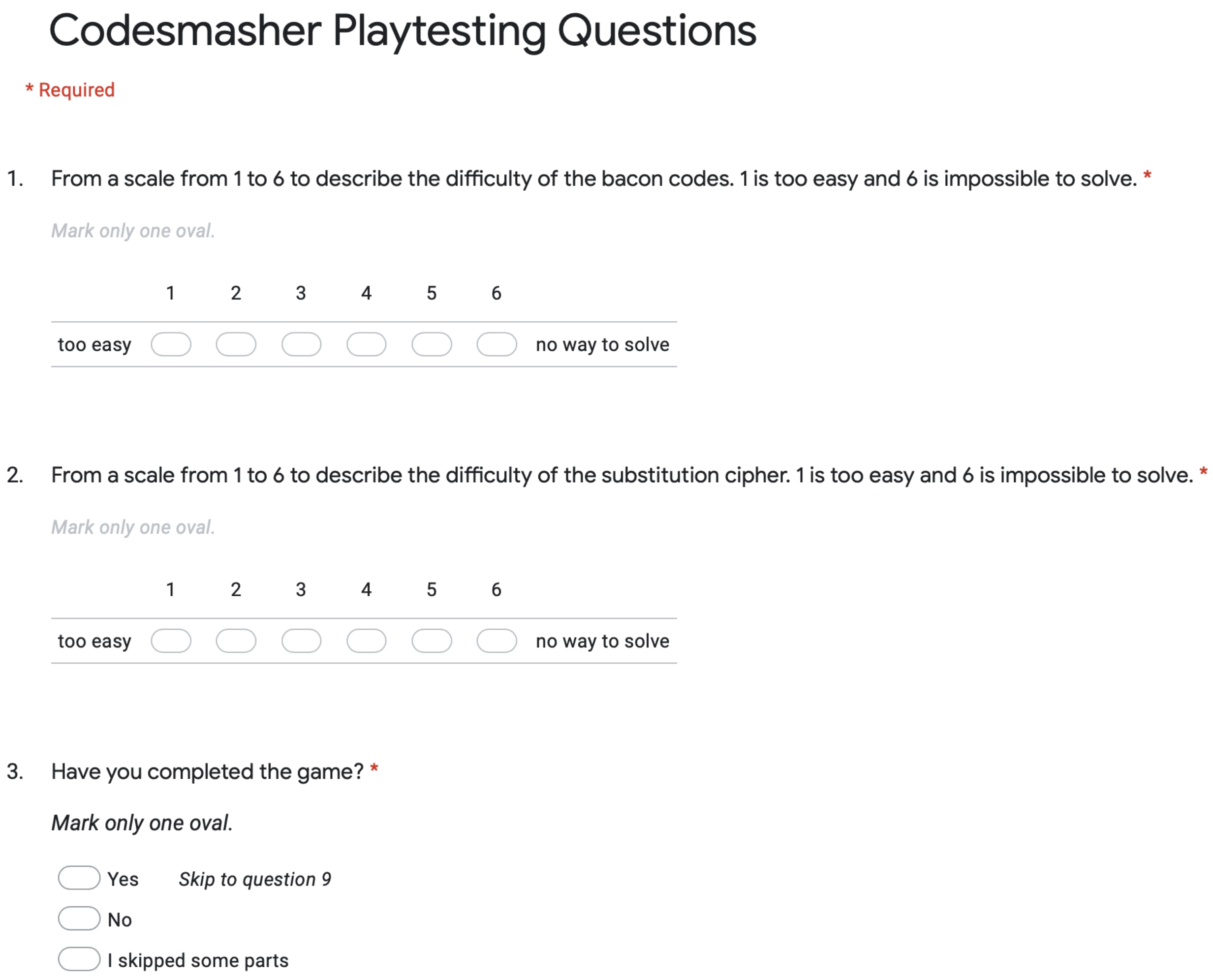
Brown, Matthew. (2018) *Cypher* [Computer software]

Murphy, Matthew. (2016) *Cryptogram* [Mobile application software]

Lisi, Luke; Bradford, Kevin (2015) *The Guides* [Mobile application software]

Lisi, Luke; Bradford, Kevin (2017) *The Guides Axiom* [Mobile application software]

Appendix: Playtesting Questionnaire



Codesmasher Playtesting Questions

* Required

1. From a scale from 1 to 6 to describe the difficulty of the bacon codes. 1 is too easy and 6 is impossible to solve. *

Mark only one oval.

	1	2	3	4	5	6	
too easy	○	○	○	○	○	○	no way to solve

2. From a scale from 1 to 6 to describe the difficulty of the substitution cipher. 1 is too easy and 6 is impossible to solve. *

Mark only one oval.

	1	2	3	4	5	6	
too easy	○	○	○	○	○	○	no way to solve

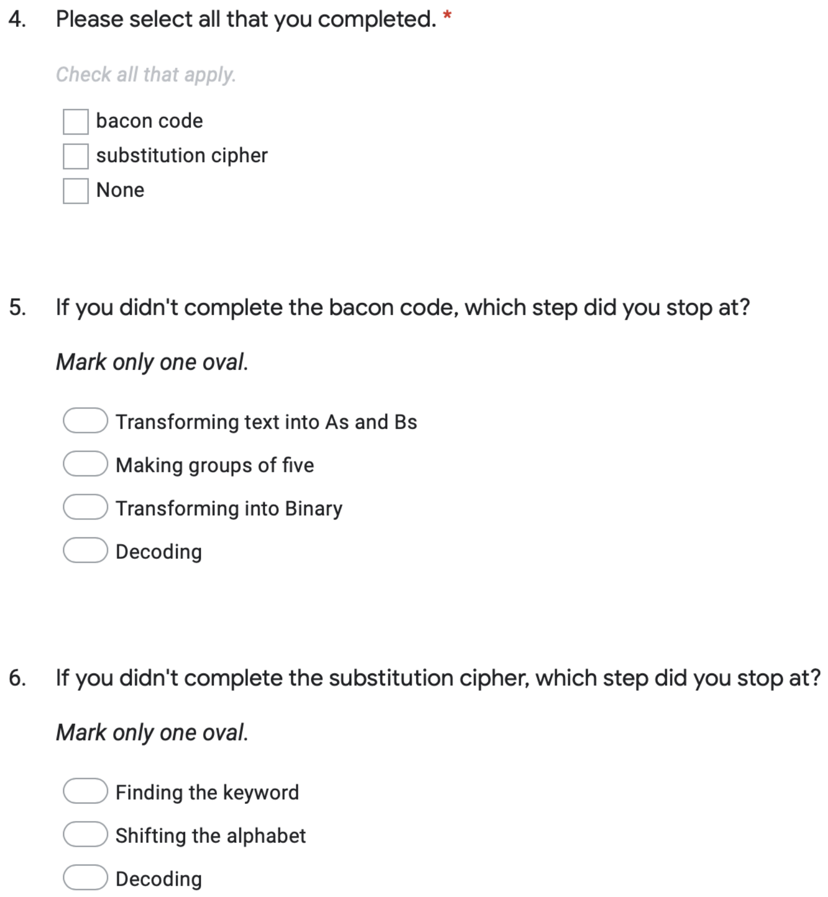
3. Have you completed the game? *

Mark only one oval.

○ Yes *Skip to question 9*

○ No

○ I skipped some parts



4. Please select all that you completed. *

Check all that apply.

□ bacon code
□ substitution cipher
□ None

5. If you didn't complete the bacon code, which step did you stop at?

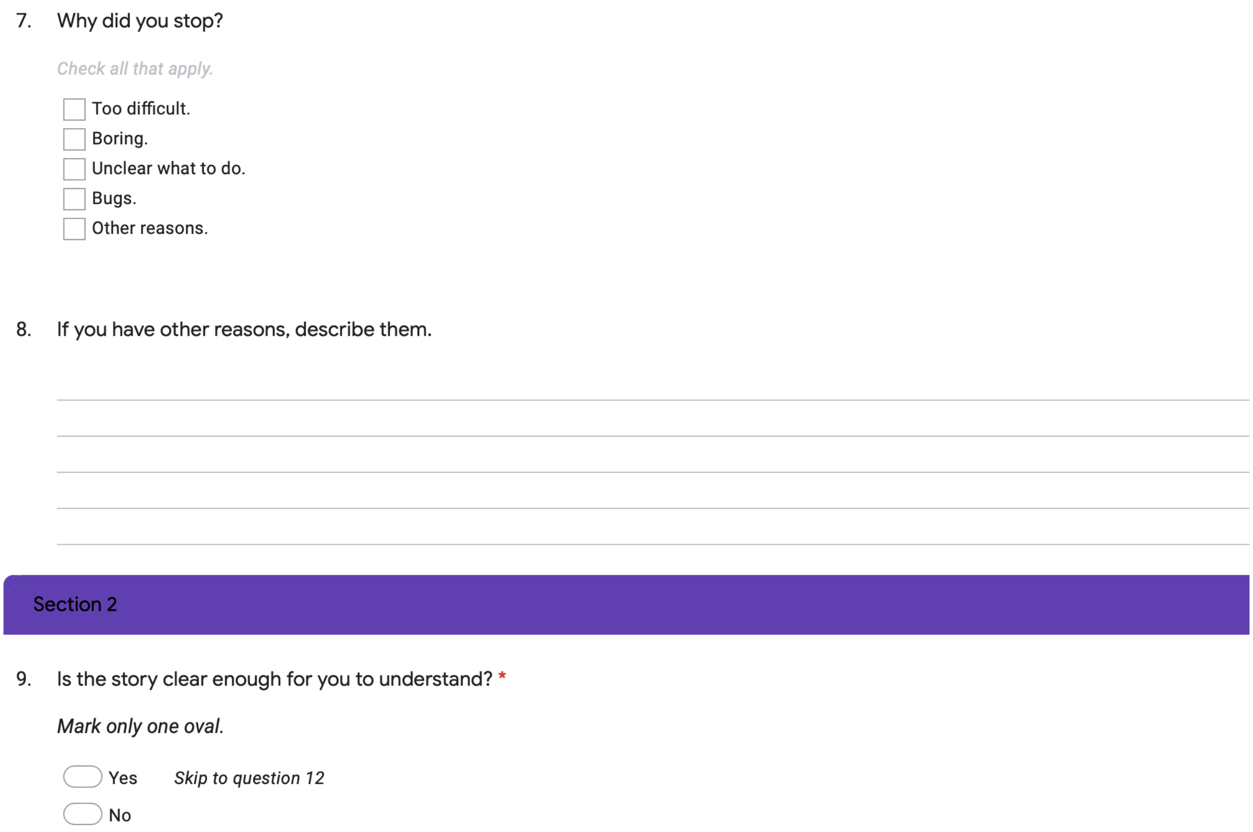
Mark only one oval.

○ Transforming text into As and Bs
○ Making groups of five
○ Transforming into Binary
○ Decoding

6. If you didn't complete the substitution cipher, which step did you stop at?

Mark only one oval.

○ Finding the keyword
○ Shifting the alphabet
○ Decoding



7. Why did you stop?

Check all that apply.

□ Too difficult.
□ Boring.
□ Unclear what to do.
□ Bugs.
□ Other reasons.

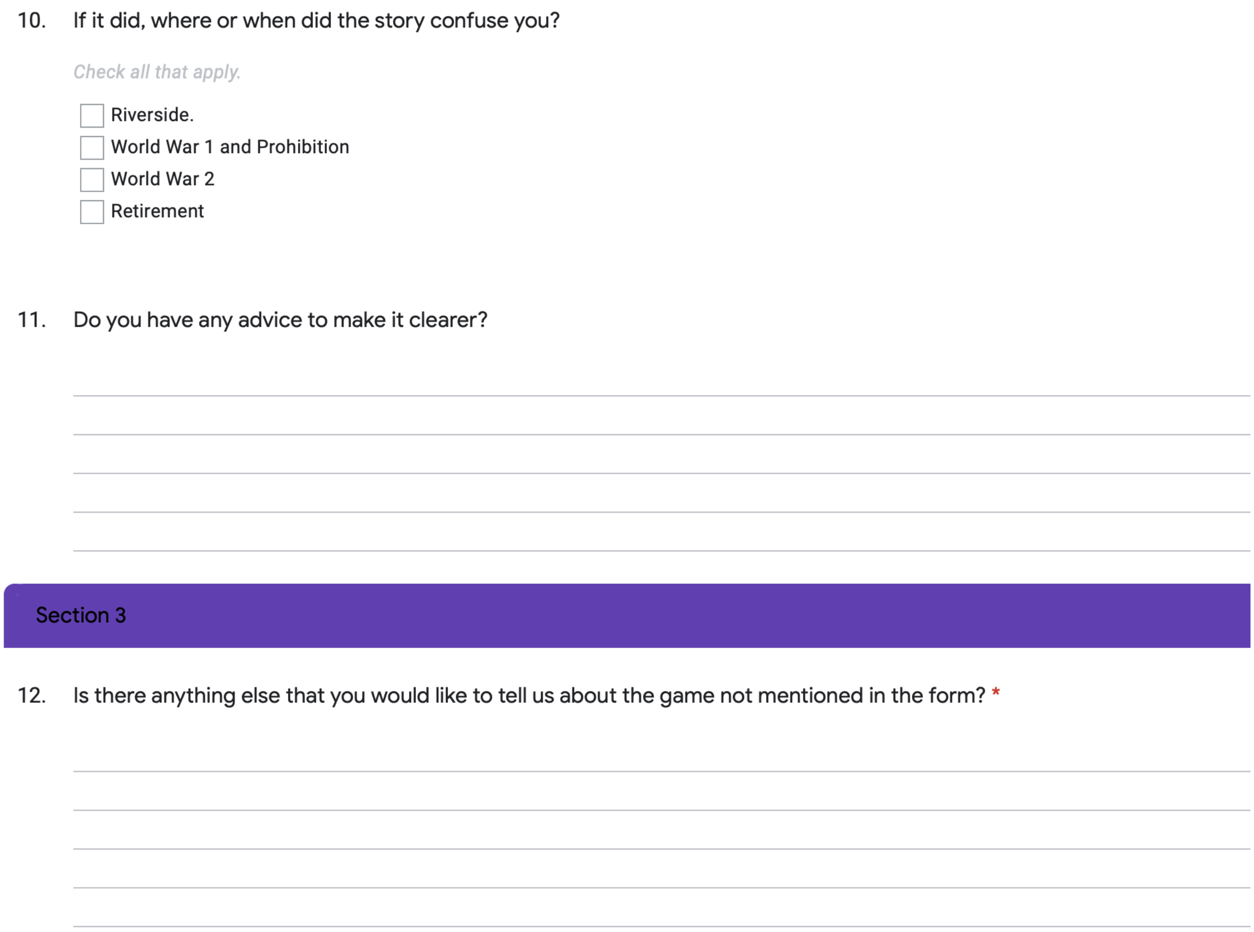
8. If you have other reasons, describe them.

Section 2

9. Is the story clear enough for you to understand? *

Mark only one oval.

○ Yes *Skip to question 12*
○ No



10. If it did, where or when did the story confuse you?

Check all that apply.

□ Riverside.
□ World War 1 and Prohibition
□ World War 2
□ Retirement

11. Do you have any advice to make it clearer?

Section 3

12. Is there anything else that you would like to tell us about the game not mentioned in the form? *