**Name of Lesson\*:** Cryptology in History

\*Not a single lesson, rather this is a description of the cryptology strand incorporated into a multi-strand team project.

**Teacher:** Alexis Lund

**Level:** High School, Honors World History, grade 10

**Duration:** varied by activity over multiple days

**Project Description:**

At the close of the Roman Banquet, an end of the year competition will be introduced. It is a gamified team challenge called “The Great Empire Race”. This will engage students during the final several weeks of school while they finalize their independent research term papers.

* Students will be divided in to teams representing the major empires (in a general sense) studied through the course of the year.
	+ Teams will be sorted based on several factors: a ranked list of empires each student submits as the one’s they are most interested and teacher prerogative to create mixed-ability groups.
	+ See Appendix A, List of Empires with grouping notes
* Within the framework of this competition, students will be competing in various challenges in and out of class; these will be activities designed around aspects of cultural and societal history, which include aspects of art, math, science, and technology.
	+ As a subset will be the challenges in cryptography and cryptanalysis briefly explained here.
	+ All challenges will earn teams “Libation Points” (LPs) which will be granted to their group’s chosen “patron god/goddess”.
		- LPs will be granted dependent on each particular challenges. During timed challenges it will be in decreasing levels as each team finishes. When asked to decrypt other’s encryptions, LPs will also be awarded to the team whose ciphertext takes the longest average time for the teams to crack. Bonus activities will carry a small number of extra LPs for each team/individual who completes that activity.
* Announcement of the “World’s Greatest Empire” will be made during the schedule exam time in finals week.
	+ The “Mandate of Heaven” (i.e. the grand prize) will be granted to the winning team at the conclusion of the individual presentations of the findings of their term papers.

**General Objective:** To introduce basic cryptography and cryptanalysis, especially cipher usage, to students as enrichment during a culminating team activity on ancient empires.

**Learning Outcome(s):**

Skills development:

* Students will be able to encrypt and decrypt basic messages (Caesar, Scytale)
* Students will be introduced and practice with more complex cryptography and cryptanalysis methods (Vigenère).

Concept formation:

* Understand the importance of cryptology and protecting certain information for privacy and security reasons.

Process orientation:

* Small groups in competition will encourage teamwork and develop communication skills.
* Timed activities will encourage time and stress management.
* Longer term activities will encourage another form of time management and prioritization.

**Rationale for Lesson:**

To be an informed citizen of an increasingly digital world, students need to understand the historical basis of modern encryption.

**Instructional Procedures:**

 Focusing Event:

* Roman Banquet
	+ A simple Caesar cipher message will be picked up in the back of class, as a quiet activity, upon completion of the unit test on Rome, the final major unit of the year. It will be an elaborate invitation to a Roman banquet, which they know about per directions and a sign-up given at the introduction of the Roman unit.
		- See Appendix B, Roman Banquet Invitation plaintext and ciphertext
		- Students will be given a link to a video which will explain how to decipher the message, this will take the form of a QR code on the invitation.
			* The invitation and explanatory video will serve as their initial introduction to basic cryptography.

Teaching Methods and Student Activities:

* The cryptography lessons will be completed in a flipped form via an instructional videos assigned as homework, such as the video assigned prior the Roman Banquet.
	+ See resources and materials list below for suggested videos which can be assigned for each topic.
* Challenges with cryptology aspects:
	+ Initial challenges will use simple substitution ciphers (focus on the Caesar):
		- Solve to get Roman Banquet invite. Invitation includes instructions which will allow students priority in group assignments.
		- Following the flag creation challenge, groups will be asked to use a Caesar cipher to encrypt the name of an influential person from their empire.
			* The complete set will be handed to all groups to solve as a group during a timed in class activity.
			* A bonus cipher will be given to each group, another name from their unit which is enciphered using an Atbash cipher.
		- This activity will highlight the ease with which simple substitution ciphers can be cracked and the need for the more complex polyalphabetic ciphers.
	+ Mid-level challenges will use polyalphabetic ciphers (focus on the Vigenère):
		- Following the sculpting challenge, students will be given a link to a video about Vigenère ciphers to watch as homework for the next class.
		- Students will be given excerpts of similar lengths from a poem of their respective empire. These will all be encrypted using the keyword: CODEX, which they will be given to initiate the timed challenge. Students will have the class block to decipher their poem and look-up the author.
		- The next Vigenère challenge will incorporate a Scytale cipher.
			* The Scytale will not be fully explained, rather students will be given a strip of paper with seemingly random letters and a QR code which links to a video which demonstrates without words how to use a strip and rod. The only verbal directions will be “you are presently supported by the key”. The rod/key in question is the leg of their chairs.
				+ When solved, this is the keyword for their next challenge. It will be the word “Ottoman”
			* This keyword will allow them to decrypt instructions which will give them a distinct advantage in the architecture challenge. They will be instructed to bring cardstock paper and masking tape (in class they will be given regular weight printing paper, tacks, and rubber bands).
	+ Follow-up Scytale challenge:
		- Each group will select one significant person from their empire and create a Scytale cipher strip of this name for each group in their class.
		- Each group will be given a set of dowels of various widths. They will use these to encrypt their name (they do not need to use the same rod for all groups) and the decrypt all the names they are given by other groups.
	+ A bonus final challenge will be a Vigenère with no key
		- This will be given at the final class of review week, as well as a video explaining how to approach solving a Vigenère without a key. Groups will have until the day of the scheduled exam time to work together to solve it.
		- Bringing in the solved puzzle to the exam time will give the team bonus LPs which may impact the final standings for the competition.
	+ Possible additions to work on and include:
		- Polybius square written or the tap code as modified by POWs in Vietnam.
		- Multiple encoded messages and a scytale to serve as authentication of one.
		- Mixed alphabet ciphers added as a midpoint between simple substitution (Caesar) and polyalphabetic.
		- Challenge can be upped by removing spaces and blocking text.
		- Another very difficult reach cipher to add (maybe in place of the Vigenère with no key) is the Playfair cipher.

Closure:

* The final standings will not be known until the day of the scheduled exam when any group who has solved the final Vigenère will hand in the deciphered message. LPs points will be updated live and the final winner of “The Great Empire Race” will be announced. There will be much pomp and circumstance as the “Mandate of Heaven” (paper crowns, certificates, and candy) is bestowed onto the winning team.

**Evaluation Procedures:**

This is a non-grade activity. Students will be given participation points for their final grade based on their participation in class activities and their ability to show evidence their completed the given homework assignments (usually check notes or another deliverable, such as the ranked list of empires request on the Roman Banquet invite).

**Materials and Resources:**

Possible resources, including several videos I did not select but which could serve as replacements for those I did. Not all materials have been produced, such as the encrypted poems for the Vigenère decryption.

Video Resource: “Intro to Cryptography”, Theoretically. <https://youtu.be/f2F9UM1y7fw>

Video Resource: “Cryptography 101 - The Basics”, Pico Cetef. <https://youtu.be/fNC3jCCGJ0o>

Video Resource: “Caesar Cipher”, Khan Academy. <https://youtu.be/sMOZf4GN3oc>

Video Resource: “Substitution ciphers: Ancient, Renaissance”, University of Nottingham. <https://youtu.be/diqXRyhKatw>

Video Resource: “Scytale / Skytale – Kryptologie”, René Zgraggen. <https://youtu.be/KJpYA7pyFwQ>

Video Resource: “268 Scytale Cipher”, Rezky Wulandari. <https://youtu.be/1tA0WO6LMqY>

Video Resource: “Polyalphabetic Cipher”, Khan Academy. <https://youtu.be/BgFJD7oCmDE>

Video Resource: “Vigenère Cipher - Encryption”, Theoretically. <https://youtu.be/izFivfLjD5E>

Video Resource: “Vigenère Cipher - Decryption (Known Key)”, Theoretically. <https://youtu.be/oHcJ4QLiiP8>

Video Resource: “Vigenère Cipher - Decryption (Unknown Key)”, Theoretically. <https://youtu.be/LaWp_Kq0cKs>

Appendix A: List of Empires with grouping notes

Appendix B: Roman Banquet Invitation plaintext and ciphertext

Appendix A

A List of Empires with grouping notes

Empire Groups for “The Great Empire Race”

1. Mesopotamia (Sumer, Akkad, Babylon, Assyria, Persia)
2. Egypt
3. China
4. India
5. Greece (inclusive to all major poleis)
6. Rome

Note: for unequal sized groups, scores of the smaller groups should be normalized from activities where individual points are earned. Otherwise no adaptation should be required.

\*2016-2017 school year, 29 students, 6 groups

Appendix B

Roman Banquet Invitation plaintext and ciphertext

**Plaintext:**

Lucius Lundius to the Noblewomen of Honors World History, her students, many greetings!

You are cordially invited to a Roman Banquet held in your honor during our next class. Please, remember to bring a food item to share and come prepared per directions given in class (Roman profile, Latin quote, and Banquet attire).

Postscript: if you have decrypted this note, bring an ordered list of your favorite of the empires we have studied.

*(on the reverse)*

Deliver at St. Mary’s to our meeting room on the date of the Roman exam, from their teacher Lucius Lundius



*(this QR code replaces a wax seal and takes the students to a video about Caesar ciphers)*

**Ciphertext, key=5:**

Qzhnzx Qzsinzx yt ymj Stgqjbtrjs tk Mtstwx Btwqi Mnxytwd, mjw xyzijsyx, rfsd lwjjynslx!

Dtz fwj htwinfqqd nsanyji yt f Wtrfs Gfsvzjy mjqi ns dtzw mtstw izwnsl tzw sjcy hqfxx. Uqjfxj, wjrjrgjw yt gwnsl f ktti nyjr yt xmfwj fsi htrj uwjufwji ujw inwjhyntsx lnajs ns hqfxx (Wtrfs uwtknqj, Qfyns vztyj, fsi Gfsvzjy fyynwj).

Utxyxhwnuy: nk dtz mfaj ijhwduyji ymnx styj, gwnsl fs twijwji qnxy tk dtzw kfatwnyj tk ymj jrunwjx bj mfaj xyzinji.

*(on the reverse)*

*Ijqnajw fy Xy. Rfwd’x yt tzw rjjynsl wttr ts ymj ifyj tk ymj Wtrfs jcfr, kwtr ymjnw yjfhmjw Qzhnzx Qzsinzx*

