**Cipher, Ciphers, and More Ciphers Project**

Ciphers have been used for centuries to send secure messages between people around the world. Wars have been fought over the suspected data in an encrypted message and relationships have blossomed from secret messages being exchanged in schools. In this project, you will choose a Symmetric Algorithm Cipher and learn everything there is to know about it. Learn the theory behind how it works and why it was created in the first place.

Afterwards you will write your own program that encrypts, and decrypts text based off that cypher. And last, but certainly not least, you will create your own cipher and code that one as well. Your cipher should use a Symmetric Algorithm and your program should be able to encrypt / decrypt text based off your creation.

**Project Specifics**

1. Choose a Symmetric Algorithm Cypher that you would like to research and then code. **Some examples are below, but there are many more**. ***EDIT: You are not allowed to use any of the ones listed below.*** Make sure to research Asymmetric Algorithms as well and prepare a one-page report. You will be asked questions about it during your presentation.
   1. Reverse Cipher
   2. Caesar Cipher
   3. Simple Substitution Cipher
2. Research everything there is to know about the Cypher you have chosen. Some questions you may be asked are below.
   1. How does the cipher encrypt text?
   2. Is there anything needed to decode the encrypted text?
   3. Why was this cipher created?
   4. When was this cipher created?
   5. Who was it created by?
   6. Is there a point in history where this cipher was known to be used and caused a major change in the way things work today?
3. Once you know everything there is to know about your cipher, write the encryption and decryption algorithm in the programming language of your choice. The program should take some type of text input (Either encrypted or not) and then the user should be able to choose if they want to Encrypt or Decrypt. After the choice has been made, either the decrypted or encrypted text should be displayed for the user.
4. Now that you have done some research into how Ciphers work, you will need to create your own cipher. It must be created using a Symmetric Algorithm. Make sure you fully understand how your Cipher works and then repeat step 3 with this newly created cipher. Make sure there’s an encryption and decryption part of your program.
5. Prepare both programs and everything you have learned about your cipher into a presentation. You will present everything you have learned about the cipher you originally chose as well as the cipher you have created. Your presentation should be informative and visually pleasing to receive full marks. Rubric on the back can be used during planning.

Rubric:

|  |  |  |  |
| --- | --- | --- | --- |
| Task | 4 | 2 | 0 |
| Symmetric Encryption | Student successfully programs a symmetric encryption in a programming language of their choice. Student can explain each part to the teacher when asked. | Depending on the input, student’s code may not work as intended.  However, student has made a valid attempt at programming a symmetric encryption algorithm and can explain portions of it. | Student’s code does not work using any input. The student is not able to explain their code. |
| Symmetric Decryption | Student successfully programs a symmetric decryption in a programming language of their choice. Student can explain each part to the teacher when asked. | Depending on the input, student’s code may not work as intended. However, student has made a valid attempt at programming a symmetric decryption algorithm and can explain portions of it. | Student’s code does not work using any input. The student is not able to explain their code. |
| Asymmetric Theory | Student can explain the theory behind an asymmetric encryption algorithm. They can respond to questions regarding asymmetric encryption.  AND  Student writes a one-page paper on asymmetric encryption. This paper must explain in peer-friendly language how asymmetric encryption works and dive into a specific example and use case. | The student can explain theory behind asymmetric encryption but may falter at some questions.  OR  Student submits a paper on asymmetric encryption but 1) not in peer-friendly language or 2) no exploration of a specific asymmetric encryption algorithm and use case scenario. | Student cannot explain asymmetric encryption when questioned. No paper submitted on asymmetric encryption. |
| \*\*[YOURNAME]\*\* Cipher | Student creates their very own cipher! They can explain the theory behind their cipher and demonstrate the encryption and decryption portions. Student responds to questions well and can explain their choices.  The encryption and decryption mechanisms work. | Student may have attempted to create their own cipher, but only either the encryption or decryption mechanisms work.  Student is unable to clearly articulate how their cipher works. | Student never created their own cipher OR just copied a cipher off the internet. They are not able to explain any of their decisions. |
| Presentation and Demonstration | Student makes an engaging presentation instructing their classmates on the algorithm. They can answer questions with confidence, and it is clear they know their material. | Student makes a thorough presentation but without energy. They may falter at questions. | Student does not present OR it seems students do not understand the material they are saying (reading directly off slides) and cannot respond to questions. |
| \*Bonus (0.5) | Options:   * Choose a teacher and send them an email using your cipher! You will somehow have to get them to tell me that you deserve this extra credit… (add message in English at end? other?) * Choose a friend and use your cipher to converse via text/snap/etc.! You will have to submit proof of your conversation (at least 1 day worth of texts). * Let me know of your ideas! | | |

Total: \_\_\_/20

Symmetric Algo Signups:

* Adam, Alexandro, Andrew – BIFID Cipher
* Nathan, Grant, Gabriel – Enigma Machine Cipher
* Nicholas, Jared, Lincoln – Beaufort Cipher
* Anne – Hill Cipher
* Maheen, Mayah, Elisa – Polybius Cipher
* Drew, Kevin – XOR Cipher
* Alicia, Mairead – Vigenère Cipher