MAT 260 Milestone One Guidelines and Rubric

Overview

This milestone is important as it gives you the opportunity to select a specific cryptosystem that you would like to spend more time researching, understanding, and demonstrating your expertise on throughout the course. In this milestone, you'll perform research to understand the historical context and development of your system that allows you to see how it fits within the larger class of techniques studied in the course. You'll also provide a conceptual explanation of how and why your cryptosystem works. This conceptual description is important, as it will serve as the starting point for a more detailed mathematical explanation of the algorithms used within your selected cryptosystem in a subsequent milestone.

Directions

This assignment requires you to select a cipher or cryptosystem to analyze. It's important to pick a cipher or cryptosystem that interests you, as you will use this selection for your next milestone and for your final project. Your analysis of your selected cipher or cryptosystem in Milestone One will include presenting the historical background of the system and describing its core concepts. You must include at least three references in your analysis.

Specifically, your submission must address the following rubric criteria:

1. **Select a cipher or cryptosystem** from the following list that you want to focus your project on:
    A. Shift Cipher
    B. Affine Cipher
    C. Vigenère Cipher
    D. Substitution Cipher
    E. Playfair Cipher
    F. ADFGX Cipher
    G. Enigma Cipher
    H. RC4 Stream Cipher
    I. Block Cipher
    J. Hill Cipher
    K. Data Encryption Standard (DES)
    L. Advanced Encryption Standard (AES)
    M. RSA Algorithm
    N. ElGamal Public Key System

Note: If you would like to do your project on a cryptosystem of interest that is not listed above, contact your instructor to check if it would be an appropriate topic for this project.

2. Summarize the **historical background** of your selected cipher or cryptosystem.
3. Describe the **properties** of your selected cipher or cryptosystem making sure to highlight the mathematical foundations that it operates on.

What to Submit

To complete this project, you must submit a one- to two-page Word document with 12-point Times New Roman font, double spacing, and one-inch margins. Be sure to cite sources according to APA style. Consult the Shapiro Library Citing Your Sources Guide for more information on citations.

Milestone One Rubric

Criteria	Exemplary	Proficient	Needs Improvement	Not Evident	Value
Cipher Selection	**N/A**	Identifies a cipher or cryptosystem to analyze for the project (100%)	Shows progress toward proficiency, but with errors or omissions; areas for improvement may include selecting an appropriate cipher or cryptosystem (85%)	Does not attempt criterion (0%)	20
Summarize Historical Background	Exceeds proficiency in an exceptionally clear, insightful, sophisticated, or creative manner (100%)	Summarizes the history and background of the selected modern cryptosystem (85%)	Shows progress toward proficiency, but with errors or omissions; areas for improvement may include providing a more detailed historical summary or contrasting the cryptosystem with other similar schemes (55%)	Does not attempt criterion (0%)	30
Describe Properties of the Cryptosystem	Exceeds proficiency in an exceptionally clear, insightful, sophisticated, or creative manner (100%)	Describes the core concepts of the selected cipher or cryptosystem highlighting its mathematical foundations (85%)	Shows progress toward proficiency, but with errors or omissions; areas for improvement may include providing a more detailed description of the scheme or making sure to highlight the key mathematical principles involved (55%)	Does not attempt criterion (0%)	30

Criteria	Exemplary	Proficient	Needs Improvement	Not Evident	Value
Articulation of Response	Exceeds proficiency in an exceptionally clear, insightful, sophisticated, or creative manner (100%)	Clearly conveys meaning with correct grammar, sentence structure, and spelling, demonstrating an understanding of audience and purpose (85%)	Shows progress toward proficiency, but with errors in grammar, sentence structure, and spelling, negatively impacting readability (55%)	Submission has critical errors in grammar, sentence structure, and spelling, preventing understanding of ideas (0%)	10
Citations and Attributions	Uses citations for ideas requiring attribution, with few or no minor errors (100%)	Uses citations for ideas requiring attribution, with consistent minor errors (85%)	Uses citations for ideas requiring attribution, with major errors (55%)	Does not use citations for ideas requiring attribution (0%)	10
				Total:	100%