MAT 260 Milestone Two Guidelines and Rubric

Overview

In this milestone, you will continue your analysis of the cipher or cryptosystem you selected in Milestone One. You will expand upon the conceptual descriptions provided in the previous milestone by analyzing the mathematical principles and algorithmic details of the selected system. You will also describe potential attacks that could be used against the cryptographic system. Since potential attacks may have different likelihoods of success, you will also analyze the feasibility of these attacks to understand how vulnerable the system is to such an attack avenue.

Directions

This assignment requires you to analyze your selected cipher or cryptosystem and describe its mathematical principles. Your analysis of your selected cipher or cryptosystem in Milestone Two will include presenting the algorithmic details of encryption and decryption of the system, a description of the underlying mathematic principles it uses, a description of a possible attack on the system, and an analysis of the attack's feasibility.

Specifically, your submission must address the following rubric criteria:

1. Describe the **algorithmic encryption/decryption details** of your selected cryptographic system.
2. Break down the **underlying mathematical principles** that the algorithm uses.
3. Illustrate one or more **potential avenues of attack** that could be used against your cipher or cryptographic system.
4. Evaluate the **feasibility of the potential attack** you selected in terms of the computational complexity and/or likelihood of success.

What to Submit

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

Milestone Two Rubric

Criteria	Exemplary	Proficient	Needs Improvement	Not Evident	Value
Algorithmic Encryption/Decryption Details	Exceeds proficiency in an exceptionally clear, insightful, sophisticated, or creative manner (100%)	Describes the algorithmic encryption/decryption details of the selected cryptographic system (85%)	Shows progress toward proficiency, but with errors or omissions; areas for improvement may include providing sufficient details of the encryption or decryption algorithms (55%)	Does not attempt criterion (0%)	20
Underlying Mathematical Principles	Exceeds proficiency in an exceptionally clear, insightful, sophisticated, or creative manner (100%)	Breaks down the underlying mathematical principles used in the algorithm (85%)	Shows progress toward proficiency, but with errors or omissions; areas for improvement may include accurately identifying the mathematical principles or providing sufficient details about the mathematical principles (55%)	Does not attempt criterion (0%)	20
Potential Avenues of Attack	Exceeds proficiency in an exceptionally clear, insightful, sophisticated, or creative manner (100%)	Illustrates one or more potential avenues of attack against the selected cryptographic system (85%)	Shows progress toward proficiency, but with errors or omissions; areas for improvement may include identifying a potential avenue of attack or providing a sufficient explanation of the attack technique (55%)	Does not attempt criterion (0%)	20
Feasibility of Potential Attack	Exceeds proficiency in an exceptionally clear, insightful, sophisticated, or creative manner (100%)	Evaluates the feasibility of the selected potential attacks in terms of the computational complexity needed and the likelihood of the success for the attack (85%)	Shows progress toward proficiency, but with errors or omissions; areas for improvement may include providing an assessment of attack likelihood or accurately computing the likelihood of attack success (55%)	Does not attempt criterion (0%)	20

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%