MAT 260 Final Project Guidelines and Rubric

Course Outcomes

In this project, you will demonstrate your mastery of the following course outcomes:

- Investigate properties of modular arithmetic, statistics, probability, permutation functions, algorithms, binary numbers, base 26, primes, factorization, the Euclidean algorithm, and Fermat's little theorem as they pertain to classical cryptographic techniques, symmetric computer-based cryptography, and public key cryptography
- Discuss the historical backdrop to the subject of cryptology

Overview

To effectively encrypt or decrypt information using cryptography, you must first understand the cipher or cryptosystem that is being used. There are many different cryptographic systems that one can choose to protect sensitive information, but the key to unlocking these hidden messages lies in mathematical principles that the system is built upon.

The final project for this course is a cryptosystem analysis. You will start by selecting a cipher or cryptosystem and research the historical context, development, and properties of your chosen system. Next, you will analyze the system by describing the details of the algorithm the system uses, breaking down the underlying mathematical principles behind the algorithm, illustrating a potential attack that could be made against the system and how feasible the attack would be in breaking the encryption.

Directions

To complete this project, you will select a cipher or cryptosystem to study. You will work with this selection throughout the course, starting with the first milestone assignment. You'll research this cipher or cryptosystem, from its historical background and foundations to the more specific mathematical principles and avenues of attack that can be used against it.

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.
4. Describe the **algorithmic encryption/decryption details** of your selected cryptographic system.
5. Break down the **underlying mathematical principles** that the algorithm uses.
6. Illustrate one or more **potential avenues of attack** that could be used against your cipher or cryptographic system.
7. 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 three- to five-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.

Final Project 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%)	10

Criteria	Exemplary	Proficient	Needs Improvement	Not Evident	Value
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%)	13
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%)	13
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%)	13
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%)	13

Criteria	Exemplary	Proficient	Needs Improvement	Not Evident	Value
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%)	13
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%)	13
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%)	6
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%)	6
				Total:	100%