Security vs. Speed:

Evaluating AI in Time-Constrained Encryption

Project Proposal

Group 1 Members:

Margo Bonal

Luke Ruffing

Evan Thompson

Professor: Dr. Nader Mohamed

Course: CMSC-4200-AI

School: Pennsylvania Western University

Table of Contents

Project Title:

Security vs. Speed: *Evaluating AI in Time-Constrained Encryption*

Description:

In the ever-growing Computer Science Industry, AI introduces modern skillsets and task automation. AI can also solve problems of various sizes. Both popularity and usability attract users to implement artificial intelligence in their daily lives. Harvard Business Review (2024) speaks on this in their article on selecting AI Tools. "*Artificial intelligence has witnessed a remarkable surge, captivating researchers, product teams, and end users alike with its transformative potential*." However, AI ultimately highlights weaknesses in specific science and mathematics-based tasks.

As aspiring software engineers, our Group 1 team proposes to push AI's capabilities and comprehension when presented a task in Computer Science. We would like to see if AI is capable of providing and designing encryption solutions when given a computational time constraint. For example, can AI provide optimal data hashing solutions in terms of Big O? Can AI make decisions on security level vs computational cost? This topic of evaluating AI's ability to problem solve encryption solutions when held to time constraints explores both mathematical and algorithm processing while applying to an important computer science topic.

Problem Types to Investigate:

Our team proposes to analyze various problem types to provide a thorough thesis on our topic. Algorithm selection, Optimization, Complexity, and Security Analysis will represent the categories AI will be tested against. Limitations will be tracked to show the success rate of AI's problem-solving ability. Algorithm Selection will test AI's ability and knowledge of encryption algorithms, while Optimization will test the ability to select an algorithm for a specific purpose. The categories of Complexity and Security will examine AI's ability to create an encryption solution that meets a provided time complexity while ensuring data security. These 4 main problem types to investigate will provide an overall conclusion of AI's ability in data encryption.

AI Tools:

Our team proposes using OpenAI's ChatGPT, Microsoft Copilot, and Google Gemini for our analysis. Utilizing multiple AI agents will allow for comparison of success rates, solutions, and limitations. ChatGPT and Copilot both exist on the foundation of OpenAI's GPT (Generative Pre-trained Transformer) models, while Gemini exists via Google's own independent models. Although they share the same foundations, ChatGPT and Copilot are not simply copies of one another. Microsoft utilizes GPT models but adds layers to allow Copilot to meet their security needs and to integrate closely with the broader Microsoft ecosystem.

GPT-based models, developed by OpenAI, have overwhelming market share among large language models (Statcounter Global Stats, 2026). Given this, our selection of AI agents gives a variety of options: GPT-based, modified GPT-based, and non GPT-based. In comparing results, our team may be able to determine if one agent or foundation type is more successful or efficient for our application than the others.

Agent	Foundation
ChatGPT	GPT
Copilot	GPT (with additional Microsoft layers and modifications)
Gemini	Gemini

Expectations:

Project expectations are represented by the following:

- Part 1: Project Proposal
- Part 2: AI trials / Tool implementation
- Part 3: Project Paper, covering findings
- Part 4: Overall Project Class Presentation

Through previous experimentation, we expect AI to be able to select algorithms based on problem type. Another expectation of AI tool implementation is the creating and optimization in computational time. Current expectations allow us to believe that AI will be able to create these encryption algorithms with certain time constraints. However, our team proposes to find

tradeoffs in security and quality. Thorough research and documentation during our project will prove these expectations to be correct or faulty.

Importance:

Encryption is a very important field in computer science. Properly storing and maintaining data is directly tied to the foundational computing principles of the CIA Triad: *Confidentiality, Integrity, Availability.* As IT professionals, it is our responsibility to maintain this security and integrity. Artificial Intelligence introduces questions in regard to this data protection. Can it uphold principles that have been placed to ensure safety? Can AI provide solutions that both aid in optimization and efficiency? Our AI class team is not only passionate about data encryption and cryptography but also captivated by answering these artificial intelligence questions. Only through careful research can we find a conclusion on whether AI can effectively solve data encryption problems in the field of Computer Science or not.

References

Cervini, Farronato, Kohli, & Van Alstyne. (2024, Dec 18). *Is AI the right tool to solve that problem?* https://hbr.org/2024/12/is-ai-the-right-tool-to-solve-that-problem

Statcounter Global Stats. (2026). *AI chatbot market share worldwide*. Statcounter. https://gs.statcounter.com/ai-chatbot-market-share