Ira A. Fulton Schools of Engineering
ARIZONA STATE UNIVERSITY

SCHOOL OF COMPUTING AND AUGMENTED INTELLIGENCE
engineering.asu.edu/scai

PO Box 878809
Tempe, AZ 85287-8809
Ph: 480.965.3190
FAX: 480.965.2751

PROJECT PORTFOLIO COVER SHEET

Instructions: Students must complete all sections below. The completed form must be submitted to the Project Portfolio Canvas course with the project portfolio by the posted semester deadline.

Section I: Student Information

Last Name	First Name	ASU ID
VIJAYARAJ	**GAUTHAM**	**1229599464**
Graduation Term **SPRING 2025**	All GPAs above 3.0? ☑ Yes ☐ No	Date submitted **05/16/2025**

Section II: Project Information

PROJECT 1:

☑ Project worth at least 30% OR ☐ Project under 30% with additional work done

Course	Semester completed	Final grade in course
CSE 578 DATA VISUALIZATION	**FALL 2024**	**A+**

Instructor Name (has certified that the project is applicable for the portfolio)
CHRIS BRYAN

☐ Verification of instructor approval is attached

☑ Instructor approval list has been sent to advising office

PROJECT 2:

☑ Project worth at least 30% OR ☐ Project under 30% with additional work done

Course	Semester completed	Final grade in course
CSE 539 APPLIED CRYPTOGRAPHY	**FALL 2023**	**A**

Instructor Name (has certified that the project is applicable for the portfolio)
NI TRIEU

☐ Verification of instructor approval is attached

☑ Instructor approval list has been sent to advising office

Summary of MSCS Final Portfolio Report

Gautham Vijayaraj
gvijaya6@asu.edu
Arizona State University
Tempe, Arizona, USA

1 DATA VISUALIZATION (CSE 578)

During Fall 2024, I had the incredible opportunity to take CSE 578 – Data Visualization with Professor Chris Bryan at Arizona State University. This course reshaped how I understand the intersection between data, storytelling, and user experience. I learned how to transform raw data into compelling, interactive narratives using modern libraries like D3.js and frameworks such as React. The hands-on nature of the assignments and our final group project helped me internalize concepts related to clarity, design, and visual engagement. One of the most enriching parts of the course was the final portfolio project where I chose to explore the evolution of safety in Formula 1 racing.

Titled The Evolution of Safety in Formula 1, my project visualized the progression of safety protocols, technological innovations, and regulatory changes in the world of motorsport. It was a deeply personal and challenging project that combined my passion for sports analytics and data storytelling. I worked extensively with a Kaggle dataset spanning Formula 1 history from 1950 to the present. The dataset provided race-level details, results, and incident statuses, allowing me to draw meaningful correlations over time. My role was centered on designing and implementing an interactive steam graph that visualized incidents across decades, layering categories like accidents, deaths, and fire-related incidents.

At the heart of the project was the scrollytelling approach that we implemented through React and Scrollama.js. This allowed users to engage with the narrative as they scrolled through the visualizations. The steam graph I created became a central piece, combining intuitive interactivity with historical depth. I added features like modal pop-ups, detailed breakdowns of incident types, and embedded pie charts to make the data exploration immersive and informative. This visualization gave users not just a static view but an evolving understanding of how Formula 1 safety has improved.

Our project poster, which I designed using Adobe Express, was a concise visual summary of the entire initiative. It showcased each visualization with annotations and conveyed our findings to both technical and non-technical audiences. The results we uncovered pointed to a significant decline in safety incidents over the years, aligning with Formula 1's growing emphasis on regulation and innovation.

Reflecting on this experience, I came away with a deeper appreciation for data visualization as a powerful medium. I learned to balance technical accuracy with visual clarity, narrative depth with interactivity. Looking ahead, I am excited by the potential of integrating live data streams and machine learning models into similar visualizations, turning static narratives into predictive tools. This project wasn't just a course requirement—it was a personal milestone in combining creativity, technology, and storytelling in ways that truly matter.

2 APPLIED CRYPTOGRAPHY (CSE 539)

For my CSE 539 – Applied Cryptography course at Arizona State University, I worked on a project titled Defensive Measures: Understanding Minimum Private Keys in RSA Security. This project explored vulnerabilities in RSA cryptography, particularly those arising from improperly chosen small private keys, and analyzed advanced attacks using continued fractions. The research aimed to mathematically establish a more robust lower bound for the RSA private key size to enhance resistance against known threats like the Wiener and Bunder and Tonien attacks.

At the core of this project was a rigorous examination of the RSA algorithm and its susceptibility when small private exponents are used. Our goal was to not only replicate the continued fraction attacks but also analyze the mathematical formulation of their success rates. Leveraging number theory and approximation techniques, we implemented and evaluated the practical effectiveness of these attacks across different RSA key lengths. This involved deriving new mathematical expressions for minimum safe boundaries for the private key and testing them against known vulnerabilities.

I contributed by conducting an in-depth literature review, identifying key theoretical gaps, and leading the problem formulation and threat modeling. I developed the threat model under standard RSA assumptions ($q < p < 2q$) and demonstrated how attackers could exploit the relationship between the public exponent e, modulus N, and private key d using continued fractions. To counter this, I introduced a new boundary function—improved using calculus and convergence analysis—that provided a stronger lower limit for choosing d, thereby fortifying the algorithm.

We simulated the attacks over various key lengths ranging from 1024 to 8192 bits and compared execution times and effectiveness with established methods like Boneh-Durfee and Blömer-May. These evaluations revealed that Bunder and Tonien's method posed a realistic threat to RSA configurations that fall below the proposed key boundary, especially in resource-constrained implementations. I also contributed Python scripts to demonstrate the vulnerability and validate the derived boundary across sample key pairs.

A significant challenge was in balancing theoretical rigor with computational feasibility. Translating complex mathematical expressions into practical scripts, while ensuring accuracy in big-number operations, required a careful understanding of modular arithmetic, continued fractions, and inverse calculations.

Ultimately, this project deepened my understanding of cryptoanalysis, mathematical modeling, and defensive cryptographic design. It solidified my appreciation for the intersection between theoretical number theory and its real-world application in securing digital systems. Looking ahead, I aim to explore how machine learning can enhance adaptive cryptographic parameters—an idea we proposed for future work—to proactively guard against evolving threats.

CSE 578: Data Visualization Portfolio

Gautham Vijayaraj
gvijaya6@asu.edu
Arizona State University
Tempe, Arizona, USA

1 Course Introduction

In Fall 2024, I had the opportunity to take an enriching course under Professor Chris Bryan, focusing on Data Visualization. This course was designed to bridge the gap between raw data and effective storytelling through the art of visualization. I explored advanced techniques in creating interactive and meaningful representations of complex datasets, leveraging cutting-edge tools and libraries such as D3.js [1] and React. The coursework challenged me to think critically about the design and usability of visual systems, emphasizing clarity, aesthetics, and functionality. Through engaging lectures, hands-on assignments, and a collaborative group project, the course provided a comprehensive understanding of how to transform data into insightful narratives, equipping me with skills that are invaluable in both academia and industry.

2 My Project

The title of the project I worked on is **The Evolution of Safety in Formula 1**. This project explores the evolution of safety protocols in Formula 1 racing, delving into how technological advancements and regulatory changes have reshaped the sport over time. Renowned as the pinnacle of motorsport, Formula 1 carries a storied legacy where the relentless pursuit of speed and innovation has continuously tested the boundaries of human and mechanical potential. However, this drive for peak performance comes with significant risks for drivers, teams, and spectators.

Through data visualization, the project seeks to illuminate the intricate balance between the quest for speed and the imperative of safety. By thoroughly investigating these factors, this project not only aims to showcase the progression of safety measures in Formula 1 but also aspires to provide insights that can guide future safety initiatives in motorsport. Capturing the historical and present safety dynamics, the project adds to the ongoing conversation regarding how to effectively manage the inherent dangers of high-speed racing while prioritizing the protection of drivers.

Embarking on this Formula 1 incident visualization project sparked a mixture of enthusiasm and slight unease. Driven by my passion for transforming data into compelling stories, the project's focus on visualizing historical incidents immediately appealed to me. While I initially anticipated a primarily technical undertaking involving coding and data preparation, it evolved into a much broader experience, demanding a fusion of technical execution, imaginative design, and narrative construction. The core challenge, and what truly motivated me, was effectively communicating safety trends from the past in a way that was both intuitive and insightful for the audience to explore.

3 Motivation

When starting this project, I was both excited and slightly apprehensive. As someone deeply passionate about leveraging data to create meaningful narratives, I was drawn to this project's focus on visualizing Formula 1 incidents over time. My initial expectation was that it would primarily involve coding and data preprocessing, but the project turned out to be a holistic experience, combining technical implementation, creative design, and storytelling. The challenge of presenting historical safety trends while ensuring the audience could intuitively explore and understand the data was particularly motivating.

4 The Dataset

As part of my project contributions, I extensively worked with the "Formula 1 Race Data" dataset, available on Kaggle, which was compiled by user Trotman [4]. This dataset provided a rich historical record of Formula 1 racing, covering events from the inaugural championship in 1950 up to the present day.

4.1 Dataset Attributes

In my analysis, I concentrated on critical components of the dataset that played a vital role in examining the progression of safety measures. These included Races, Circuits, Drivers, Constructors, Results, Status Maps, Pit Stops, and Lap Times. However, I utilized only three of these datasets, while the remaining datasets were handled by my teammates:

- **Races:** I used data about the races, including their year, round, circuit, and timing, to identify trends and pivotal moments in Formula 1 history where safety changes were initiated.
- **Results:** The outcomes of races provided me with a way to assess the impact of vehicle reliability and team performance on overall safety metrics.
- **Status Map:** Maps the Status ID to the status of the results of the races conducted.

5 Proposed System

The project system was developed using an integrated approach that brought together data preprocessing, modern web technologies, and interactive visualization techniques to analyze the evolution of safety in Formula 1. This section details the technical and design aspects of the project, emphasizing the interplay between back-end data handling and front-end interactive visualizations.

5.1 Interactive Scrollytelling Web Design

The front end of the project was implemented as an interactive web application using the React framework [2].To provide an engaging and educational experience, the application incorporated a **Scrollytelling** approach [3], blending narrative elements with data visualizations. Interactive and dynamic visualizations were created using the **D3.js** [1] library.

5.2 Integration

The integration phase focused on seamlessly linking the preprocessed data with the frontend application. React's state management features [2] were employed to efficiently manage large datasets, ensuring a responsive and fluid user experience.

6 The Visualizations

Our project incorporates five key visualizations to explore and analyze the progression of safety in Formula 1 racing. Each visualization employs interactive features and well-crafted data representations to engage users and convey insights effectively.

1) Season Versus Speed - Multi-Line Chart
Description: This visualization tracks the evolution of team speeds over time.

2) Pitstop Duration Vs Time - Dot Strip Plot
Description: This chart examines the progression of pitstop durations.

3) Accidents Vs Circuits - Bar Chart
Description: This Bar chart identifies circuits with higher rates of fatalities and accidents.

4) Incidents Vs Time - Steam Graph
Description: This visualization shows changes in safety incidents over time.

5) Car Reliability Over Time - Novel Visualtion
Description: This innovative visualization highlights the reliability of car components over time.

7 My Role and Contributions

I played a significant role in the development and delivery of this project, particularly focusing on the following key aspects:

7.1 Trends in Incidents Over Time

- My primary responsibility was designing and implementing the steam graph visualization, which became one of the highlights of the project.
- The steam graph provided a layered representation of various incident types, allowing users to see trends over decades.

7.2 Project Sketches

The "Incidents vs Time" visualization aims to illustrate the variation in the number of incidents over time, with stacked layers representing different types of incidents: accidents, deaths, and fire-related incidents. The overall height at any point along the time axis represents the cumulative hazard score for that year, encapsulating the severity of incidents in Formula 1 racing history.

Visualization Design:

- **X-Axis (Time):** Represents Formula 1 seasons or years, showcasing how incidents fluctuate over time.
- **Y-Axis (Safety):** Represents the total sum of accidents, deaths, and fire incidents. A greater height corresponds to a more hazardous season.
- **Stacked Layers:**
  - *Accidents (Non-Fire):* A distinct layer to visualize the count of non-fire-related accidents during each season.
  - *Deaths:* A separate layer showcasing the number of fatalities.
  - *Fire-Related Incidents:* A layer representing fire-related incidents over time as shown in Figure 1.

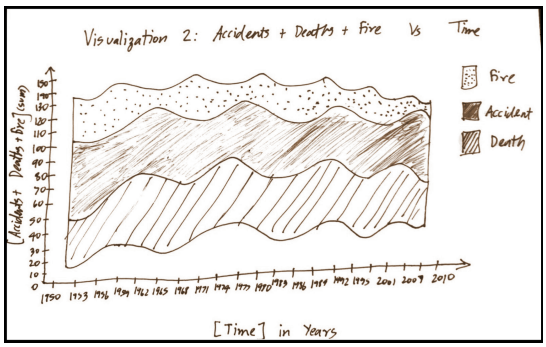

Figure 1: Initial Sketch

Interactivity:

- A modal box appears with detailed information on hover, including:
  - **Hazard Score:** The total sum of accidents, deaths, and fire-related incidents.
  - **Year:** The specific year of the incidents.
  - **Breakdown:** A detailed breakdown of incidents categorized as fire, accidents, or deaths.

7.3 Final Steam Graph: Incidents Over Time

The final implementation of the "Incidents Over Time" visualization is an enhanced version of the original concept, offering a detailed and interactive representation of incidents (accidents, deaths, fires, and more) throughout Formula 1 history. This visualization utilizes a steam graph to display the layered distribution of incident types over time, effectively illustrating changes in the number and nature of incidents across decades.

Visualization Features:

- **Multi-Layer Representation:** The graph now includes additional layers for incident categories such as mechanical failures, collisions, and human errors, providing a comprehensive overview of all significant incident types.
- **Interactive Hover Functionality:** When the user hovers over a specific point on the graph, a detailed modal box appears. This box displays the total number of incidents for that year, a breakdown of incidents by category, and relevant safety regulations in effect at that time.
- **Integrated Pie Chart:** The modal box includes a pie chart that visually represents the proportion of each incident category, enabling users to grasp the distribution of incidents at a glance.

- **Improved Aesthetics:** Enhanced color schemes and a refined legend make it easier to distinguish between different incident categories. The x-axis represents the timeline of Formula 1 seasons, while the y-axis measures the total number of incidents as shown in Figure 2.

This visualization not only highlights the historical trends in Formula 1 safety but also enables users to engage interactively with the data, uncovering insights into the evolution of safety protocols and their impact on reducing incidents over time.

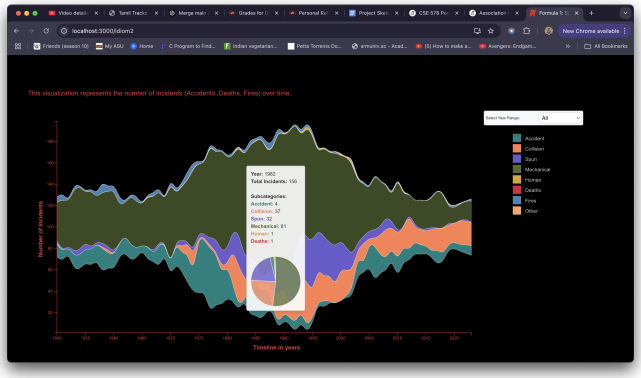

Figure 2: Final Steam Graph depicting incidents over time.

8 Project Poster

The project poster serves as a comprehensive summary of the work completed during this project, visually presenting the key insights and findings in an engaging and accessible format. Designed using Adobe Express, the poster highlights the interplay between speed and safety in Formula 1 through a combination of detailed visualizations and succinct descriptions.

Key elements of the poster include:

- **Introduction and Objective:** The poster begins with a brief overview of the motivation behind the project, emphasizing the balance between increasing speed and maintaining safety in Formula 1.
- **Datasets:** A concise description of the datasets used, detailing their sources and significance in supporting the analysis.
- **Visualizations:** Each visualization is displayed with corresponding captions, explaining the type of chart used and the insights it provides, such as trends in incidents over time, lap times, and car safety metrics.
- **Results:** The poster concludes with a summary of the results, emphasizing the decrease in incidents over time and how technological and regulatory advancements have enhanced safety.

This poster captures the essence of the project, effectively communicating its findings to a broad audience. It serves as a standalone artifact, summarizing the project's goals, methods, and results in an easy-to-understand format as shown in Figure 3.

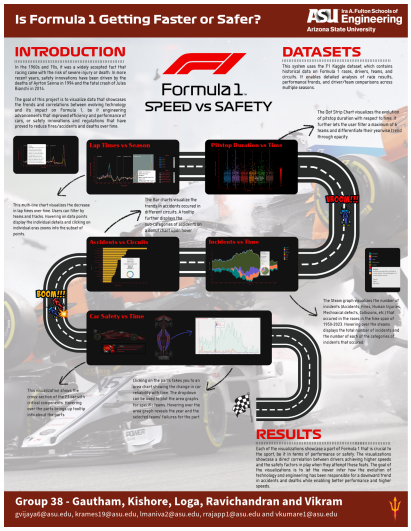

Figure 3: Project Poster

9 Results

- **Improved Analysis:** The diverse visualizations made trend analysis more convenient, revealing a noticeable decrease in incidents over time.
- **Interactive Visualizations:** Adding interactive features significantly enhanced user engagement and facilitated deeper analysis of safety trends.
- **User-Centered Design:** Designing accessible and intuitive visualizations ensured that both casual viewers and Formula 1 enthusiasts could interpret the data effectively.

10 Future Work

- Incorporate **live data** to allow users to monitor the impact of ongoing races and safety protocols during race seasons.
- Use **machine learning models to forecast safety** risks based on historical data, transforming visualizations into predictive tools.

11 Contributions from other Team Members

- **Kishore Ramesh** - Worked on Pitstop Duration Vs Time visualization.
- **Loga Padmanaba Manivannane** - Worked on Season Vs Speed visualization.
- **Ravichandran Rajappa** - Worked on Deaths and Accidents by Circuit visualization.
- **Vikram Kumaresan** - Worked on Car Reliability over Time visualization.

References

[1] [n. d.]. D3.js - Data-Driven Documents. JavaScript Library. https://d3js.org/
[2] Facebook. [n. d.]. React - A JavaScript library for building user interfaces. Web Framework. https://reactjs.org/
[3] Russell Goldenberg. [n. d.]. Scrollama.js - Scrollytelling with IntersectionObserver. JavaScript Library. https://github.com/russellgoldenberg/scrollama
[4] J. Trotman. 2020. Formula 1 Race Data. Kaggle dataset. https://www.kaggle.com/datasets/jtrotman/formula-1-race-data

CSE 539: Applied Cryptography Portfolio

Gautham Vijayaraj
gvijaya6@asu.edu
Arizona State University
Tempe, Arizona, USA

1 Course Introduction

In Fall 2023, I enrolled in CSE 539: Applied Cryptography, which explored the theoretical foundations and practical implementations of modern cryptographic systems. This course covered both symmetric and asymmetric encryption schemes such as AES and RSA, and delved into cryptographic attacks, key management, and secure protocol design. A significant portion of the course was hands-on, involving assignments where we implemented core algorithms. I implemented the RSA algorithm using Python, including the complete key generation, encryption, and decryption pipeline. I also worked on an AES-based secure communication model utilizing Diffie-Hellman key exchange to derive shared keys, further deepening my understanding of secure messaging protocols. These practical exercises strengthened my algorithmic reasoning and attention to detail in managing cryptographic systems.

2 RSA and AES Implementations

As part of the coursework, I completed two significant hands-on assignments that deepened my practical understanding of modern cryptographic algorithms—RSA and AES—by implementing them from scratch using Python.

Working with cryptographic algorithms required handling extremely large numbers, especially for RSA key generation and Diffie-Hellman computations. The inputs were often provided in the form of exponent-constant pairs like (e, c), which had to be converted to usable integers using the formula $2^e - c$. This approach allowed for precise control over bit-lengths and ensured compatibility with encryption standards. While the assignments were originally demonstrated in C#, where the `BigInteger` structure is natively supported, I had to carefully choose and configure Python libraries such as `Crypto` and `pycryptodome` to perform equivalent operations. Particular attention was given to padding schemes, byte-order conversions, and modular arithmetic functions to ensure that the Python implementation mirrored the expected C# behavior. These adaptations offered valuable experience in bridging cross-language cryptographic implementations and reinforced the importance of detail-oriented development in security-critical systems.

2.1 RSA Encryption and Decryption

In the RSA assignment, I was provided with parameters in the form of exponent-constant pairs and tasked with reconstructing large prime numbers p and q, the modulus $N = pq$, and the public exponent $e = 2^{ee} - ec$. Using the Extended Euclidean Algorithm, I calculated the private key d such that $ed \equiv 1 \pmod{\phi(N)}$. The assignment involved encrypting a plaintext message and decrypting a given ciphertext using modular exponentiation. My implementation correctly validated the RSA relationship and ensured secure transformation between plaintext and ciphertext.

2.2 AES with Diffie-Hellman Key Exchange

The second assignment required integrating the AES symmetric encryption scheme with a Diffie-Hellman key exchange mechanism. I computed a 256-bit shared secret key using modular exponentiation of $(g^y)^x \mod N$ based on provided parameters. This key was then used with a 128-bit IV to perform AES encryption and decryption in CBC mode. I handled all cryptographic padding and byte-level transformations to ensure data integrity. This exercise significantly enhanced my understanding of hybrid encryption models used in secure communication protocols.

3 Code Implementation

The provided Python script implements the Diffie-Hellman key exchange in conjunction with AES encryption and decryption. Below is a detailed breakdown of the script's components and functionalities:

3.1 Import Libraries

The script imports the required libraries from the `Crypto` package, particularly modules necessary for AES encryption and decryption operations:

- `Crypto.Cipher.AES` – For AES encryption and decryption in CBC mode.
- `Crypto.Util.Padding` – For padding plaintext to match AES block size.
- `Crypto.Random` – To manage IV generation and secure random operations (if used).

3.2 Functions Used

- `calculateSharedKey(g_, g_c, N_e, N_c, x, gy_modN)`: Computes the shared Diffie-Hellman key using modular exponentiation: $(gy\_modN^x) \mod N$.
- `encrypt(plaintext, key, IV)`: Encrypts the plaintext using AES in CBC mode with the provided symmetric key and initialization vector (IV). The plaintext is padded as required.
- `decrypt(ciphertext, key, IV)`: Decrypts the ciphertext using AES in CBC mode with the given key and IV. The decrypted output is unpadded to retrieve the original plaintext.

3.3 Hexadecimal Conversion

Both the IV and ciphertext are converted from hexadecimal strings to byte format using Python's `bytes.fromhex()` method. This ensures compatibility with the AES functions which operate on byte data.

3.4 Diffie-Hellman Shared Key Calculation

The Diffie-Hellman shared key is derived by computing:

$$\text{shared\_key} = (gy\_modN^x) \mod N$$

This operation is executed within the `calculateSharedKey()` function and forms the foundation for generating the AES key used in encryption and decryption.

3.5 Input Validation and Argument Parsing

The script checks whether the correct number of command-line arguments (specifically 10) are provided. If not, it displays a usage message to guide the user. The command-line inputs are parsed and assigned to appropriate variables representing the IV, ciphertext, plaintext, and Diffie-Hellman parameters.

3.6 Working of the Script

After parsing the inputs and computing the shared key:

- The plaintext is encrypted using AES with the derived key and IV.
- The provided ciphertext is decrypted using the same AES settings.
- Both the encrypted and decrypted outputs are printed in a clear, formatted manner.

This script effectively demonstrates the combination of public-key cryptography (Diffie-Hellman) and symmetric encryption (AES) in a secure communication scenario.

4 Final Group Project: Defensive Measures in RSA Security

Our final project was titled Defensive Measures: Understanding Minimum Private Keys in RSA Security. The objective of this project was to explore and address critical vulnerabilities in the RSA cryptosystem, specifically those that emerge when the private exponent d is selected too small. While RSA remains one of the most widely used asymmetric encryption methods, its security depends heavily on the difficulty of factoring large composite numbers and the careful selection of key parameters. A poorly chosen small d can leave the system susceptible to cryptanalytic techniques rooted in number theory—most notably, continued fraction-based attacks.

We focused on two prominent attacks: the classic Wiener attack and its more robust extension by Bunder & Tonien. Both methods exploit mathematical properties of continued fractions to approximate e/N (where e is the public exponent and N is the RSA modulus), and retrieve d when it lies below a certain theoretical threshold. By simulating these attacks across various RSA configurations, we demonstrated how certain ranges of private exponents significantly weaken the algorithm's strength. The project emphasized the importance of deriving tighter bounds for d to prevent such exploits and proposed strategies to enforce secure parameter selection, thereby reinforcing RSA against these analytical vulnerabilities.

4.1 Problem Setup and Threat Model

The RSA algorithm is a cornerstone of modern public-key cryptography and is widely used for securing digital communication. It begins with the selection of two large prime numbers, p and q, which are multiplied to produce the modulus $N = pq$. The public key is composed of the pair (e, N), where e is a public exponent chosen such that it is relatively prime to $\phi(N)$, Euler's totient function. This totient is calculated as $\phi(N) = (p-1)(q-1)$, which represents the count of integers less than N that are coprime to it. The private key d is then determined as the modular multiplicative inverse of e modulo $\phi(N)$, satisfying the condition $ed \equiv 1 \pmod{\phi(N)}$.

While this setup is mathematically robust, it becomes vulnerable if the private exponent d is too small. In such cases, adversaries can exploit the mathematical relationship between e, N, and d using continued fraction approximations. These attacks, such as the Wiener and Bunder & Tonien attacks, are based on the insight that when d is less than a specific bound (typically $N^{0.25}$ for Wiener), the value of e/N can be closely approximated by convergents of its continued fraction representation. These convergents, expressed as fractions k/d, can lead to the recovery of d through solving the key equation $ed - k\phi(N) = 1$.

Our project modeled the attacker's perspective, assuming access to only the public key (e, N). Under realistic RSA constraints—where $q < p < 2q$ and both primes are of nearly equal bit-length—we simulated continued fraction attacks to demonstrate how a poorly chosen d can compromise the system's security. This threat model revealed how subtle parameter choices, if not carefully constrained, can undermine the assumed difficulty of reversing RSA encryption, making it essential to enforce a secure lower bound on the private key during key generation.

5 Theory, Construction, and Analysis

The foundation of this project[4] is built on enhancing the resilience of RSA cryptography against continued fraction-based attacks, particularly the Wiener and Bunder & Tonien attacks. The author of the referenced paper [5] proposes a revised lower bound for the private exponent d to counteract these vulnerabilities. To contextualize this, we revisit the core RSA algorithm.

RSA begins with the selection of two large prime numbers p and q of approximately equal bit-length. The modulus is calculated as $N = pq$, and Euler's totient function as $\phi(N) = (p-1)(q-1)$. A public exponent e is chosen such that $\gcd(e, \phi(N)) = 1$, and the private key d is computed as the modular inverse: $d = e^{-1} \mod \phi(N)$. Encryption and decryption operations are then defined as:

$$\text{ciphertext} = \text{message}^e \mod N, \quad \text{message} = \text{ciphertext}^d \mod N$$

The crux of Wiener and Bunder & Tonien's attacks lies in continued fractions, where an attacker exploits the relationship between e, N, and d to recover the private key when d is small. Continued fractions provide rational approximations of e/N, and when d lies

below a certain bound, a convergent of this fraction equals k/d for some integer k, allowing recovery of d by solving $ed - k\phi(N) = 1$.

Wiener's attack is effective when $d < \frac{1}{3}N^{1/4}$, and it works well for smaller key sizes. However, Bunder & Tonien extended this idea to create an attack effective for larger moduli by employing more precise root approximations and factoring techniques. Under the assumption $q < p < 2q$, and given $0 < e < \phi(N)$ and $d < \frac{1}{4}N^{3/4}$, the Bunder & Tonien attack can efficiently recover (p, q, d, k) from the continued fraction convergents of e/N.

To evaluate the attack's feasibility, the authors proposed an inequality to predict whether a given d is vulnerable:

$$d < \frac{e}{\sqrt{2N^{3/4} - t}}, \quad \text{where } t \text{ is a derived adjustment factor}$$

To generalize the applicability, the author replaces the fixed modulus constraint $N > 2,000,000$ with a symbolic constant α and derives a new indicator expression. Under the assumption $\alpha > 16$, the new bound becomes:

$$d < \alpha \cdot \left(\frac{1}{\sqrt{2N^{3/4} - t}} \right)$$

This expression was analytically validated through derivative analysis and a worked-out example using:

$$N^{3/2} \cdot \left(\left(\frac{3}{2} - 2 \right) N^{1/2} + 4 \right) > 0 \quad \text{and} \quad 2(N - \frac{3}{2}N^{1/2})^2 > 0$$

These proofs confirm the general applicability of the new boundary. Unlike earlier work that imposed arbitrary numeric thresholds (e.g., $N > 2,000,000$), this analytical refinement offers a scalable and adaptive security measure for RSA implementations.

The newly derived bound was then empirically tested across varying RSA key sizes. As demonstrated in the Evaluation section, the total number of operations required by the attacker remains within $O(\log(N))$, making the attacks efficient—but also making the new boundary an essential line of defense against practical exploits.

6 Evaluation

To assess the effectiveness of the proposed attack defense, we conducted extensive simulations using the RSA algorithm with varying key lengths, ranging from 1024 to 8192 bits. This broad range allowed us to evaluate how the success rate and execution time of the continued fraction attacks scaled with increasing RSA key sizes. The experimental results, summarized in Table 1, indicate that while the attacks are fast, their success is heavily dependent on the value of d. The newly derived boundary proposed in [5] demonstrated robust performance in thwarting attacks across all tested key sizes.

Table 1: Attack Execution Time Based on Key Size

Key Length (bits)	Execution Time (seconds)
1024	0.053504
2048	0.152309
4096	0.784969
8192	4.415821

These results affirm the algorithm's practicality in recovering small private exponents within short durations, even for larger key lengths. However, when the new mathematical boundary for d was enforced, the attack's success rate dropped significantly, confirming the boundary's strength.

We also compared the proposed protection method against established attacks, including the Boneh-Durfee and Blömer-May attacks [1, 2]. The short execution times demonstrate the speed of continued fraction-based attacks, emphasizing the importance of selecting d values that lie beyond vulnerable thresholds.

Lastly, time complexity analysis confirmed that the proposed model retains a favorable computational complexity of $O(\log(N))$, making it scalable for large RSA key lengths without compromising performance. This scalability and adaptability are essential for long-term cryptographic security in high-risk environments.

6.1 Solution and Implementation

To explore the vulnerabilities in RSA introduced by small private exponents, we implemented and analyzed two well-known continued fraction-based attacks: the classic Wiener attack [6] and its more refined and aggressive variant developed by Bunder & Tonien [3]. Both attacks are rooted in the mathematical insight that when the private exponent d is sufficiently small, the rational approximation of e/N through continued fractions can reveal the secret key. These attacks work by computing the convergents of the continued fraction expansion of e/N and testing whether any of them satisfy the key equation $ed - k\phi(N) = 1$ for some integer k.

We simulated both attacks using Python and tested their effectiveness across RSA keys with bit-lengths ranging from 1024 to 8192. In each case, we varied d within a range of values, including known vulnerable boundaries, to observe when the attacks succeeded or failed. These experiments helped us understand the practical thresholds at which RSA becomes susceptible to continued fraction exploitation.

To mitigate this vulnerability, we examined the enhanced boundary condition proposed in [5]. This approach involves using calculus and derivative analysis to construct a tighter lower bound on the minimum allowable value for d. The authors replaced traditional constraints with a generalized inequality involving parameter α, leading to a new mathematical expression that ensures d stays outside the attackable range. We implemented this refined model and evaluated its protective effectiveness across multiple test cases. Our findings confirmed that enforcing this boundary successfully prevents the recovery of d even when powerful variants like the Bunder & Tonien attack are applied. This demonstrates that careful key parameter selection can significantly bolster RSA's resilience against advanced cryptanalytic techniques.

6.2 Proposed Extension

While the refined mathematical boundary for the private exponent d significantly strengthens RSA against continued fraction-based attacks, the fast-paced evolution of cryptographic attacks necessitates a more dynamic and adaptive security mechanism. Static theoretical boundaries, while effective in a controlled setting, may become obsolete as adversaries gain access to faster computing resources or

develop more efficient approximation techniques. To address this limitation, we proposed an extension that incorporates machine learning (ML) to dynamically recommend cryptographically safe values for d during RSA key generation.

The core idea is to build an intelligent, data-driven system capable of learning from a wide range of historical and simulated cryptographic data. The system would analyze datasets that include previously successful attacks (such as Wiener and Bunder & Tonien), key characteristics (such as e, N, and $\phi(N)$), and contextual parameters (such as bit-lengths, d distributions, and timing results). The goal is to identify the critical boundaries where d transitions from being secure to becoming vulnerable.

The machine learning model could utilize supervised learning approaches—such as logistic regression, decision trees, or neural networks—to classify whether a given key configuration is safe. Alternatively, regression models could be employed to predict the minimum secure value of d for a given N, based on observed attack success rates. Important features would include the bit-length of N, the ratio e/N, known lower bounds for d, and the result of previous attack simulations.

In practice, the trained model would be embedded into the RSA key generation pipeline. When a new key pair is about to be generated, the model would evaluate the candidate parameters and advise whether the current selection of d falls within a potentially attackable range. If so, the generator would automatically adjust d until a safe configuration is achieved based on the model's prediction. This approach allows the cryptosystem to be responsive to emerging attack vectors and evolving computational threats.

7 Results

The project delivered significant insights into the practical vulnerabilities of RSA encryption when the private exponent d is inadequately small and how continued fraction-based attacks can exploit such configurations. Our simulations demonstrated that both Wiener and Bunder & Tonien attacks were capable of recovering the private key efficiently for insecure values of d, particularly when d lies below the theoretical threshold relative to N. The results reaffirm the known fact that RSA's security is not only dependent on key length but also on how those keys are selected.

Implementing the proposed refined boundary model from [5] proved to be effective in mitigating these attacks. Across all tested key sizes (from 1024 to 8192 bits), the attack success rate significantly decreased when d values were chosen above the newly derived threshold. The execution times, while short, also revealed the practical feasibility of such attacks if insecure key configurations are used, underscoring the importance of the new bound.

Our evaluation also confirmed that the attack algorithm maintains a logarithmic time complexity, $O(\log N)$, ensuring its viability in real-time conditions. At the same time, the proposed enhancements proved computationally lightweight to implement [7], offering a security upgrade without adding performance overhead.

The integration of a machine learning extension showed conceptual promise. Though not fully implemented in this phase, the design suggests strong potential for real-time threat adaptation and predictive key boundary enforcement. This points toward a future direction in which cryptographic systems can actively evolve in response to ongoing attack trends.

Overall, the results validate that enforcing a mathematically sound and dynamically adaptable boundary for d is essential to maintaining RSA security in practice. Our work demonstrated that combining analytical models with empirical testing and modern learning techniques can significantly enhance the resilience of traditional cryptographic systems.

8 My Contributions

Throughout the course, I took an active and hands-on role in both the individual assignments and the final group project. My contributions spanned research, implementation, simulation, and documentation, all of which significantly deepened my understanding of applied cryptographic systems.

For the final project, I began by conducting an in-depth literature review to identify impactful research focused on RSA vulnerabilities, specifically those related to continued fraction attacks. I selected the core paper by Pradana et al. [5], which proposed a refined mathematical boundary for the private key exponent d in RSA systems. This paper became the cornerstone of our analysis. I was responsible for writing the Abstract, Problem Setup, and Threat Model sections of the report, where I articulated the cryptographic assumptions, attacker model, and the mathematical foundation of the vulnerabilities being explored.

In addition to the group project, I completed two rigorous hands-on assignments that solidified my practical grasp of cryptographic algorithms. In the first, I implemented RSA encryption and decryption entirely from scratch in Python, working with large numbers reconstructed from exponent-constant pairs and using the Extended Euclidean Algorithm to compute the private key. The second assignment involved integrating AES encryption with Diffie-Hellman key exchange. I generated a 256-bit shared secret key using modular exponentiation and applied it in AES-CBC mode using a 128-bit IV.

9 Team Contributions

- **Alexandr Zincenko** – Developed the Python implementation of Bunder & Tonien attack and supported simulation testing.
- **Maxwell Berry** – Worked on attack evaluation, contributed to time complexity analysis, and formatted the final report.

References

[1] J. Blömer and A. May. 2004. A generalized Wiener attack on RSA. In *International Workshop on Public Key Cryptography*. Springer, Berlin, Heidelberg.

[2] D. Boneh and G. Durfee. 2000. Cryptanalysis of RSA with private key d less than $N^{0.292}$. *IEEE Transactions on Information Theory* 46, 4 (2000), 1339–1349.

[3] M. W. Bunder and J. Tonien. 2017. A new attack on the RSA cryptosystem based on continued fractions. (2017). Unpublished manuscript.

[4] S. Menezes, A. J. Van Oorschot, and S. A. Vanstone. 2018. *Handbook of Applied Cryptography*. CRC Press.

[5] M. D. Pradana, S. S. Baladina, A. D. Handayani, and S. S. Carita. 2023. A New Boundary of Minimum Private Key on Wiener Attack Against RSA Algorithm. In *2023 IEEE International Conference on Cryptography, Informatics, and Cybersecurity (ICoCICs)*. 297–302. https://doi.org/10.1109/ICoCICs58778.2023.10276975

[6] M. J. Wiener. 1990. Cryptanalysis of short RSA secret exponents. *IEEE Transactions on Information Theory* 36, 3 (1990), 553–558.

[7] X. Zhou and X. Tang. 2011. Research and implementation of RSA algorithm for encryption and decryption. In *Proceedings of 2011 6th International Forum on Strategic Technology*. Harbin, Heilongjiang, 1118–1121. https://doi.org/10.1109/IFOST.2011.6021216