# 🛠️ Cryptography Project Documentation

### 📌 1. Team Formation and Planning (Required) Team Information

1. **Team Name: Project Nightfall**
2. **Date Formed:10-05-2025**

### Team Members and Roles

| **Name** | **Role** | **Responsibilities** |
| --- | --- | --- |
| Joy | Frontend Developer | Built UI and JS logic (Caesar, Playfair), handled file I/O. |
| Mahedi | Algorithm Developer | Implemented XOR, Vigenère, RSA, AES logic; supported JS structure |
|  |  |  |
|  |  |  |

### 📌 2. Research Algorithms (Required) Documented Cryptographic Algorithms

| **Algorithm Name** | **Type (Simple/Intermediate/Advanced)** | **Potential Use Cases / Internet Applications** |
| --- | --- | --- |
| Caesar Cipher | Simple | Easy to understand and implement as an intro to encryption |
| | XOR Cipher | | --- |  |  | | --- | | simple | Demonstrates bitwise operations, efficient |
| | Vigenère Cipher | | --- |  |  | | --- | | Intermediate | Shows how keyword-based shifting improves over Caesar |
| Playfair Cipher | Intermediate | Adds complexity via digraphs and matrix system |
| RSA | Advanced | Simulated; demonstrates public-key concepts |
| AES | Advanced | Simulated; real-world relevance in Wi-Fi and secure apps |

### 📌 3. Algorithm Selection & Implementation (Required) Documented Algorithm Selection Rationale

| **Algorithm Name** | **Type** | **Rationale for Selection** |
| --- | --- | --- |
| Caesar Cipher | Simple | Easy to implement and understand |
| XOR Cipher | Simple | Demonstrates bitwise operation, fast to execute |
| Vigenère Cipher | Intermediate | Shows keyword-based Caesar variation |
| | Playfair Cipher | | --- |  |  | | --- | | Intermediate | Demonstrates digraph encryption |
| RSA | Advanced | Popular public-key method (simulated) |
| AES | Advanced | Real-world strength encryption (simulated) |

### 📌 4. Testing & Iteration (First Round) (Required) Documented Red-Teaming (First Round)

1. **Teams Who Red-Teamed Your Site:**
   * Team 1: Vuda

* Well-balanced choice of classical and modern ciphers
* Clean, user-friendly interface with helpful features
* Smart handling of file input and encoding issues
* Strong collaboration and clear project structure
* **Suggestion:** Consider adding real-time encryption previews to enhance interactivity
  + Team 2: Press "ENTER"
* Your toll is easy although useful
* Be more creative
* Suggestion:you guys can add ” Auto Capitalization Option”

1. **Feedback Received:**

* Based on peer feedback, we added **Live Preview** and **Auto Capitalization** to enhance interactivity and usability.

1. **Changes/Improvements Made:**

We can see results instantly — feels modern and responsive.and Real-time feedback helps users understand how encryption reacts to input changes.A checkbox that, when we enabled, automatically converts input text to UPPERCASE before encryption. That is useful for Caesar and Vigenère ciphers. saves us from having to manually turn their text into uppercase.

### 📌 5. Creative Enhancements (Required) Documented Creative Enhancements

1. **Selected Enhancements:**

**Interactive Learning System**

* **Quiz Module**: 4-question interactive quiz system with immediate feedback
* **Security Analysis**: Detailed vulnerability explanations and attack methods

### **Enhanced User Experience-**

* **Smart Content Toggle**: Users can show/hide educational details based on their learning needs
* **Multi-Modal Input**: Support for both typed text and file uploads
* **One-Click Learning**: Pre-loaded examples and instant encryption demonstration

### **Comprehensive Algorithm Education**

* **Historical Context**: Real-world usage and historical significance of each cipher
* **Mathematical Foundations**: Step-by-step breakdown of encryption mathematics

### **Interactive Feedback Systems**

* **Real-Time Validation**: Immediate quiz feedback with explanations

1. **Issues Encountered:**

* information overload problems
* Balancing technical accuracy with accessibility
* Visual hierarchy confusion
* Integration challenges with existing functionality
* Mobile responsiveness concerns

1. **Final Decisions/Solutions:**

* Added "Show Learning Details" checkbox for user control
* Educational content only renders when requested
* Maintains clean interface for basic demonstration use
* Placed interactive buttons alongside existing controls
* Quiz section appears on-demand rather than always visible
* Example loader fits naturally in input workflow
* Maintained original button styling for consistency

### **Graduated Learning Approach**

**Decision**: Created multi-layered information architecture **Implementation**:

* **Layer 1**: Basic algorithm name and result (always visible)
* **Layer 2**: How it works theory (toggle-able)
* **Layer 3**: Step-by-step process (toggle-able)
* **Layer 4**: Mathematical examples (toggle-able)
* **Layer 5**: Security analysis (toggle-able)
* **Result**: Serves beginners to advanced learners effectively

*.*

### 📌 6. Testing & Iteration (After Enhancements) (Required) Documented Red-Teaming (Second Round)

1. **Teams Who Red-Teamed Your Enhanced Site:**

-Team 1: Vuda

* Great effort
* Good to see as you have implemented team VUDA sugesstion.
* Now you can do your **Cryptography Web App** a clean, futuristic, and professional look

-Team 2:Press "ENTER"

* Nice modern touch
* Making user friendly by copying the result

1. **Feedback Received:**

-Team 1 praised the effort and suggested a clean, futuristic, professional look.

-Team 2 liked the modern design and user-friendly copy feature

1. **Further Refinements Made:**

* **Clean, Futuristic, and Professional Look (from Team 1)**
* Applied a sleek dark-gradient background with subtle glow effects.
* Increased spacing and visual hierarchy for clarity and professionalism.

**User-Friendly Copy Feature** (from Team 2)

* Added prominent “Copy” buttons for each algorithm result to easily copy text to clipboard.

### 📌 7. Documentation & Reflection (Required) Project Step Summaries

| **Step** | **Summary of What Was Done** |
| --- | --- |
| Team Formation | Formed team with frontend + algorithm expertise |
| Algorithm Research | Selected 6 diverse ciphers |
| Algorithm Selection | Chose based on simplicity, demo value, and real-world relevance |
| Implementation | JavaScript logic, HTML/CSS layout |
| Testing & Iteration (First Round) | |  | | --- |  | Peer feedback addressed: UI alerts, file handling, real/simulated clarity. | | --- | |
| Creative Enhancements | UI improvements, tooltips, file support |
| Testing & Iteration (Second Round) | Re-tested all features. Added new UI polish, refined functionality. |

### Individual Team Member Reflections

Each member writes one paragraph.

| **Name** | **Reflection (Contribution, Learnings, Challenges)** |
| --- | --- |
| Joy | I focused on developing the frontend interface and implementing the Caesar and Playfair cipher logic using JavaScript. I also added user-focused features like the Auto Capitalization toggle and helped integrate real-time encryption preview to improve interactivity. One challenge I faced was managing different input methods (keyboard vs. file upload) without bugs. I learned how to use the DOM effectively, how to handle FileReader in JavaScript, and how to design a clean, user-friendly layout that works for educational purposes. This project helped me understand how cryptographic logic can be demonstrated interactively on the web. |
| Mahedi | I was mainly responsible for implementing the XOR, Vigenère, RSA (mock), and AES (mock) algorithms in JavaScript. I made sure each cipher worked for both encryption and decryption, and handled edge cases like symbols and empty inputs. I also helped debug conflicts between live preview and file input, and improved the code structure to make it more maintainable. Through this project, I strengthened my understanding of cipher mechanisms and how to simulate them realistically in a static website. I also improved my problem-solving skills in front-end scripting and learned to communicate effectively within a team |
|  |  |
|  |  |
|  |  |

## 📦 Deliverables Checklist

* Cryptography Site Tool linked on each team member’s portfolio site (**3 pts**)
* Documentation and Reflections linked on each team member’s portfolio site (**7 pts**)