BINF711 – Information Security

Project is worth 20% of the course grade

Milestones, Deliverables, and Dates

Milestone 2: Cryptography and Encryption Techniques.

- **Deadline: November 29th, 2025 @11:59 PM.**
- **Deductions will be made for late submissions.**
  - **Late Submission Penalties:**
    - The first two days (up to 48 hours late): A penalty of 50% will be deducted from your total grade.
    - From the third day to the seventh day (48 hours to 5 days late): A penalty of 75% will be deducted from your total grade.
    - Submissions beyond 5 days: Unfortunately, submissions will receive a 0 grade.
- **Teams of 2 to 3 students (Cross-tutorial teams are NOT allowed).**
- **Technologies:** Utilize programming languages such as **Python** or **Java** to create the application.
- **Submission Link:** **https://forms.gle/KysU9SK9LjEw56bg6**

Objective

This phase focuses on the encryption of passwords using **3 cryptographic techniques** and an analysis of their limitations and security threats.

1. **Password Encryption**
   - Implement encryption for stored passwords using two cipher techniques: **Playfair** and **Vigenère** Ciphers.
   - Research, select, and implement a different **encryption methodology**, aside from those studied in the course, that is suitable for password security. Analyze your chosen technique and explain your rationale for selecting it.

2. Research and Analysis

- Research and select the most recent and effective encryption methodologies suitable for password security. Reference all relevant papers and research articles related to password strength evaluation and encryption techniques that you used in your research to support your conclusions and analysis.
- **Limitations:** Assess the limitations of the chosen encryption techniques, considering factors such as computational overhead, susceptibility to attacks, and ease of implementation.

Reference all the resources you used in your research to find the most up-to-date security techniques.

Conclusion

This project aims to establish a comprehensive access control system through effective password management and encryption techniques. By combining a robust password strength analysis tool with secure cryptographic practices and role-based access control, we can enhance the security of user authentication processes.

Important Note!!

Plagiarism:

Any detected plagiarism will result in a 0% score with no second chances. This includes any similarities in the prototype design between groups. Any similar submission to online repositories, as well as using AI to generate any other required milestones, will also be penalized.