**Crypto report:**

**ECDH Generation of a mutual key in group of 3 users+ texts encryption/decryption with SALSA20 in CFB mode + Rabin signature**

* Almog Elbaz 213037369
* Guy Pariente 206132250
* Eyal Cohen 316148063
* Almog Kadosh 315699439

In response to increasing concerns over digital privacy and security, our group undertook a comprehensive project aimed at addressing these issues through the development of a secure communication protocol. This protocol employs Elliptic Curve Diffie-Hellman (ECDH) key generation for a group of three participants, offering improved security and efficiency. For secure text exchange, we implemented SALSA20 encryption in Cipher Feedback (CFB) mode, ensuring robust and consistent encryption. Furthermore, the Rabin signature scheme was adopted to ensure the integrity and authenticity of communications.

**Project Flow:**

The project was structured in several phases to ensure a systematic approach to implementing and testing the secure communication system:

1. **Design and Planning:**

This initial phase involved in-depth research and exploration of each topic to enhance our understanding. This thorough preparation enabled us to effectively integrate these components into a cohesive and secure communication system for three participants.

1. **Implementation:**

**ECDH (Elliptic Curve Diffie-Hellman):** Implemented an extended version of the ECDH protocol to support a group of three participants, facilitating secure mutual key generation.

**SALSA20 Encryption in CFB Mode:** Integrated SALSA20 as the encryption algorithm, using the shared key from ECDH for secure encryption and decryption of messages in CFB mode.

**Rabin Signature Scheme:** Implemented the Rabin signature scheme to authenticate messages, ensuring their integrity and authenticity.

1. **Testing and Evaluation:**

Conducted comprehensive testing to evaluate the efficacy of the encryption and decryption processes, the reliability of the ECDH key exchange among three users, and the effectiveness of the Rabin signature in detecting tampering and ensuring message integrity.

1. **Conclusions and Reports:**

We divided the workload, maintained effective communication, ensured mutual understanding among team members, and compiled our findings into a comprehensive report and presentation.

**Collaboration Techniques:**

Effective communication and collaboration were key to the success of our project. We utilized various tools and strategies to ensure every team member was aligned and informed:

* **Weekly Sync-ups:** Regular meetings facilitated discussions on progress, obstacles, and next steps, enabling real-time problem-solving and decision-making.
* **Cross-functional Reviews:** Conducted cross-functional reviews before integrating each component, allowing team members to provide insights and suggestions beyond their primary areas, thereby enriching the project's depth and coherence.

**Obtained Results:**

The system demonstrated a high degree of security in encrypted communications among the three participants, with several key outcomes:

* **Secure Key Exchange:** The extended ECDH protocol successfully generated a mutual shared key among three participants, ensuring secure encryption and decryption of all communications without exposing the key during transmission.
* **Effective Encryption and Decryption:** The use of SALSA20 in CFB mode provided robust encryption for text messages, effectively securing larger datasets and repeating patterns.
* **Robust Authentication:** The Rabin signature scheme effectively authenticated messages, ensuring their integrity and origin, proving particularly valuable in scenarios where non-repudiation and data integrity were critical.

**Conclusions and Reports:**

Implementing this secure communication protocol was both challenging and enlightening. We developed a robust solution that meets the fundamental needs of digital privacy and security. The integration of ECDH key exchange, SALSA20 encryption, and the Rabin signature into a single protocol represents a powerful method for securing digital communications. This project not only improved our technical skills and understanding of cryptographic principles but also highlighted the importance of collaboration and communication in tackling complex issues. Our results contribute to the ongoing discussion on digital security, providing a practical framework for secure communication that can be adapted and expanded. This work sets the stage for future explorations into more complex scenarios, such as dynamic group communications or the incorporation of additional security measures to mitigate potential vulnerabilities in CFB mode. In conclusion, this project stands as a testament to the power of teamwork, strategic planning, and technical expertise in addressing the ever-present challenges of digital security.