GEMBOS
Global Encrypted Mobile-Based Obscured SMS Application

Giray Aksakal, Berker Vergi, Mert Kahraman, Emir Moralı
Supervisors: Assoc. Prof. Dr. Ahmet Koltuksuz, Assist. Prof. Dr. Barış Yıldız

YAŞAR UNIVERSITY

Aim

GEMBOS is meticulously engineered to offer a secure and user-friendly SMS messaging application. It effectively addresses vulnerabilities inherent in conventional SMS messaging systems, particularly those pertaining to the SS7 protocol and Man-in-the-Middle (MiM) attacks.

Objectives

- **Enhance SMS Security:** Develop a robust messaging platform that addresses vulnerabilities in traditional SMS systems, such as SS7 exploits.
- **Implement Advanced Cryptography:** Leverage state of the art algorithms, including **DHKE** for secure key exchange and **ECC** for efficient key generation, to ensure strong encryption and data integrity.
- **Ensure Mutual Authentication:** Adhere to the **ISO/IEC 9798-3** standard to provide reliable service.
- **Comply with Legal Requirements:** Incorporate a master key mechanism and store messages in encrypted form in a secure database to align with data retention and legal standards.
- **Deliver a User-Friendly Experience:** Design a secure yet intuitive application that provides users with a seamless messaging experience with maintaining the highest level of security.

Implementation

GEMBOS integrates advanced cryptographic protocols to ensure secure and efficient communication, even without an internet connection is needed.

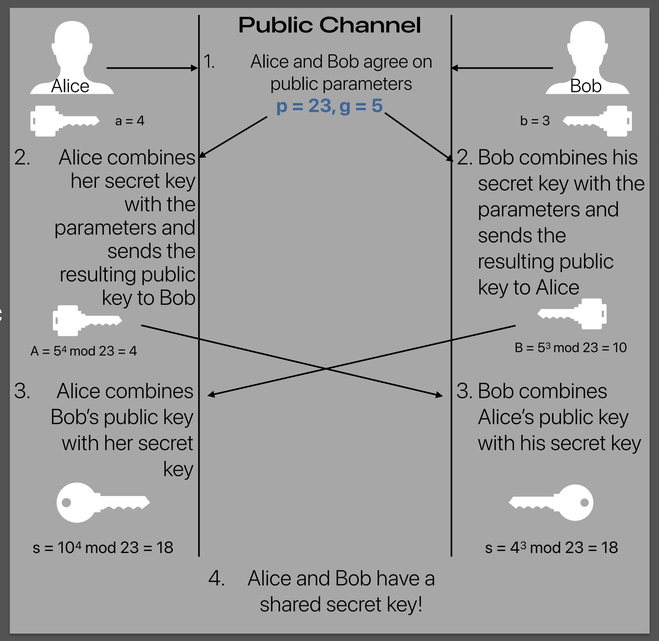
The **Diffie-Hellman Key Exchange Algorithm** is utilized for secure key exchange between users, enabling the establishment of a shared secret key over an insecure channel.

For enhanced security and efficiency, **Elliptic Curve Cryptography** (ECC) is employed for key generation, offering strong encryption with minimal computational overhead.

To ensure mutual authentication and prevent replay attacks, GEMBOS adheres to the **ISO/IEC 9798-3** standard, a proven method for entity authentication using cryptographic techniques.

To further enhance security, GEMBOS implements the **ISO/IEC 9798-3** standard, ensuring mutual authentication between entities and protecting against replay attacks. Together, these technologies create a comprehensive cryptographic framework that guarantees the confidentiality, integrity, and authenticity of user communications.

Diffie-Hellman Key Exchange



Evaluation

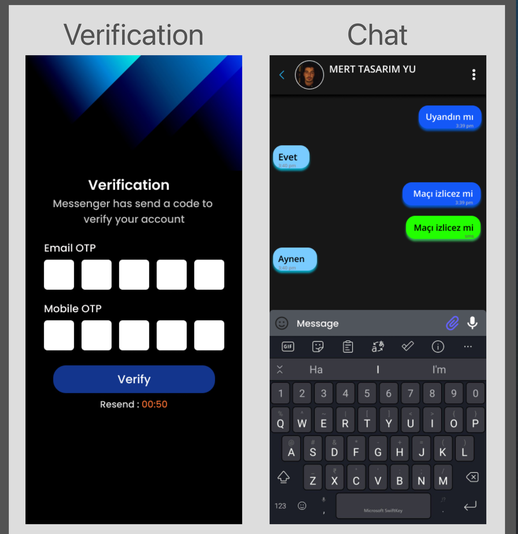
To assess the effectiveness and reliability of GEMBOS, a evaluation process consisting of following key aspects will conducted:

- Performance Metrics: Encryption and decryption speed, key exchange latency and overall system responsiveness.
- Security Testing: Cryptographic implementations such as DHKE and ECC, are validated to ensure the integrity and confidentiality of user communications. Addition to these validations adherence to ISO standards, data storage security and master key mechanism will be tested.
- User Experience: Feedbacks will be collected to refine and optimize user interface.

Conclusion

GEMBOS delivers a secure and user-friendly messaging platform by leveraging advanced cryptographic techniques and adhering to strict authentication standards. By adressing vulnerabilities in traditional SMS systems and ensuring compliance with legal requirements, GEMBOS provides a robust solution for safe and efficient communication, setting a new standard for secure messaging applications.

User Interface



Scan For More

References

1.Küsters, R., & Rausch, D. (2017, May). A framework for universally composable Diffie-Hellman key exchange. In *2017 IEEE Symposium on Security and Privacy (SP)* (pp. 881-900). IEEE.

2. Yusfrizal et al. (2018, August). Key management using combination of Diffie–Hellman key exchange with AES encryption. In *2018 6th International Conference on Cyber and IT Service Management (CITSM)* (pp. 1-6). IEEE.