GEMBOS

Global Encrypted Mobile-Based Obscured SMS

Giray AKSAKAL & Berker VERGİ

Supervisor: Prof. Dr. Ahmet Hasan KOLTUKSUZ

YAŞAR UNİVERSİTY

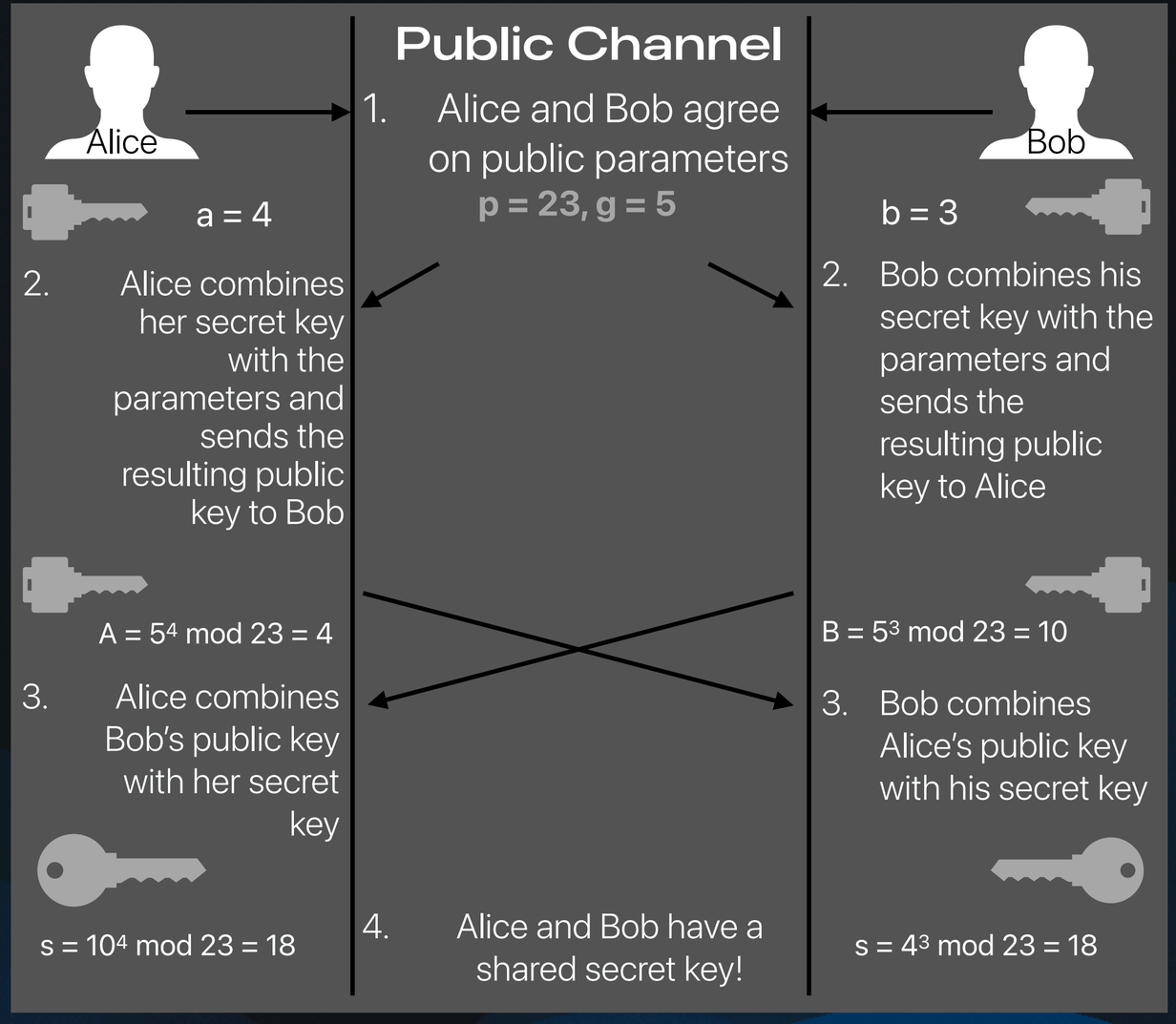
Aim

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.

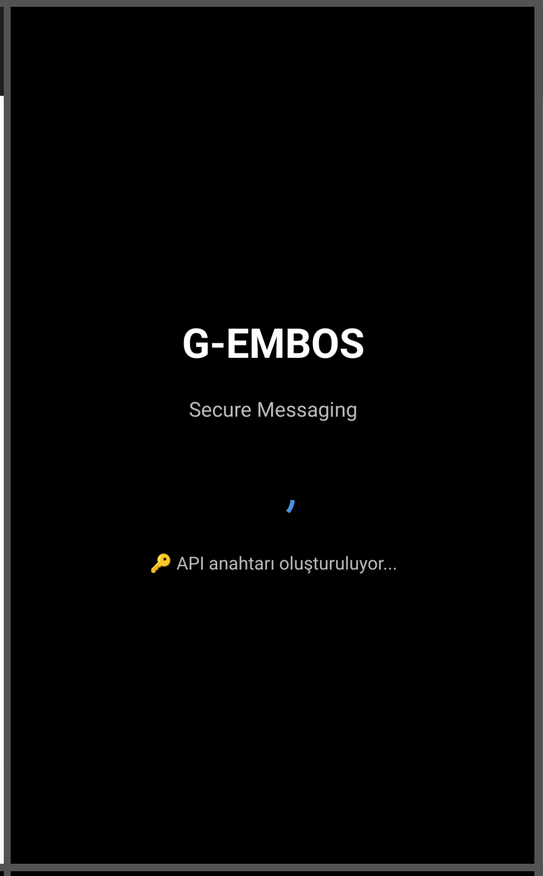
Implementation

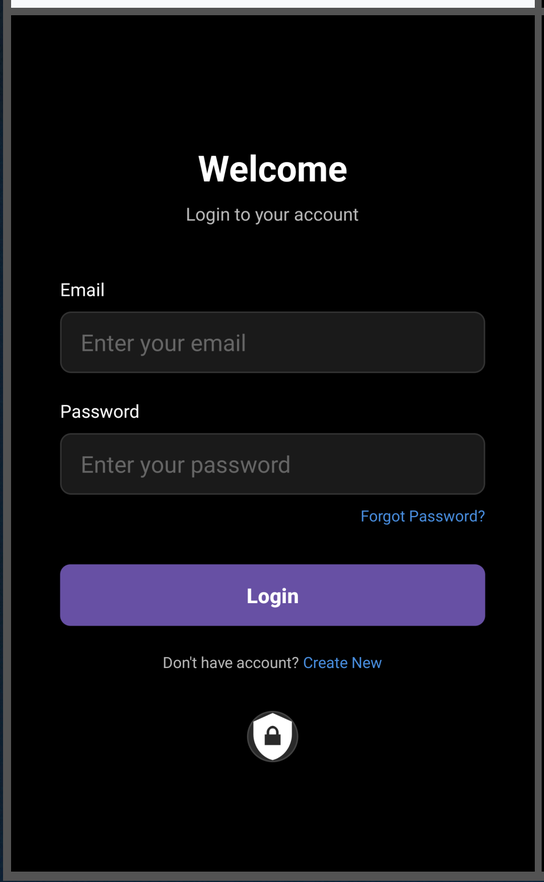
GEMBOS utilizes advanced cryptographic protocols including **Diffie-Hellman Key Exchange** and **Elliptic Curve Cryptography** to enable secure communication without requiring an internet connection. Our backend API is developed using **Spring Boot**, while the **Android application** provides a user-friendly interface that seamlessly interacts with the API for secure messaging.

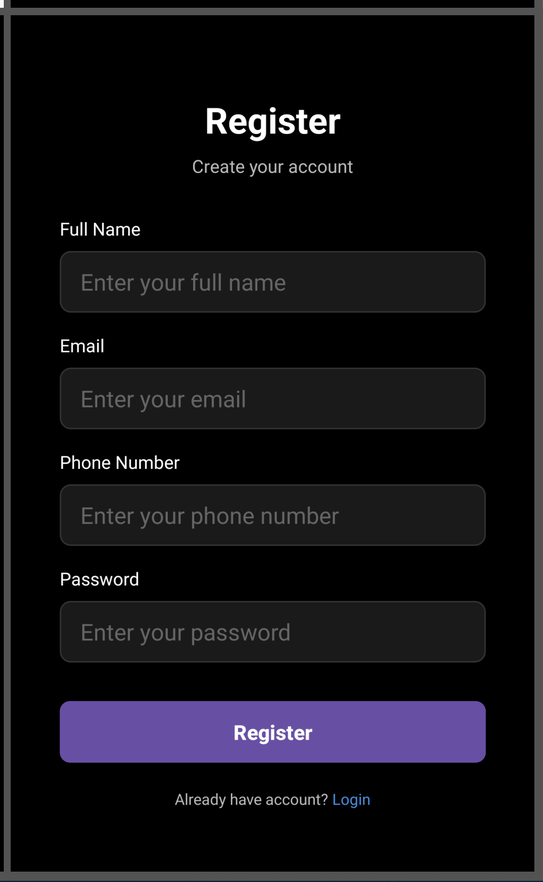
Diffie-Hellman Key Exchange



User Interface







Objectives

- **Advanced Cryptography:** Powered by Diffie-Hellman (DHKE) and Elliptic Curve Cryptography (ECC).
- **Mutual Authentication:** ISO/IEC 9798-3 compliant for verified, secure sessions.
- **Legal Compliance:** Master key system & encrypted message storage meet regulatory standards.
- **User-Friendly Design:** Intuitive interface with uncompromised security.

Conclusion

GEMBOS delivers a secure and user-friendly messaging platform by using advanced cryptographic techniques and standards. By addressing vulnerabilities in traditional SMS systems and ensuring compliance with legal requirements, GEMBOS provides a robust solution for safe communication.

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.