Üniversite : İstanbul Kültür Üniversitesi
Enstitü : Lisansüstü Eğitim Enstitüsü
Anabilim Dalı : Bilgisayar Mühendisliği
Programı : Bilgisayar Mühendisliği
Tez Danışmanı : Dr. Öğr. Üyesi Öznur ŞENGEL
Tez Türü ve Tarihi : Yüksek lisans – Haziran 2025

ÖZET

Günümüzde kullanıcılar, uygulama platformlarında oluşturdukları hesaplarının güvenliğini arttırmak için her uygulama için ayrı ayrı uzun ve karmaşık şifreler üretmek zorunda kalmaktadır. Güçlü şifreler oluşturmak ve bunları akılda tutmak zor olduğundan kullanıcılar ya her platform için aynı şifreyi kullanmayı tercih etmektedir ya da düz metin dosyasına kaydetme, kağıda yazma, tarayıcı aracılığıyla şifre saklama gibi güvenli olmayan saklama yöntemlerini kullanmaktadırlar. Bu teknikler kullanıcı şifrelerini siber saldırılara karşı açık hale getirmektedir.

Zayıf ve tekrarlanan parola kullanımı ile güvensiz saklama alışkanlıklarının getirdiği zayıflığın yanı sıra, mevcut şifre oluşturma yöntemleri çoğunlukla ASCII tabanlı karakterler kullanmakta ve kaba kuvvet ve sözlük saldırılarına karşı daha savunmasız şifreler üretmektedir. Bu tez, dijital platformlarda hesap güvenliğini artırmak amacıyla emoji tabanlı yenilikçi bir şifre yönetim sistemi sunmaktadır. Veri katmanı, iş mantığı katmanı ve sunum katmanından oluşan şifre yönetim sistemi Windows 11 üzerinde Python ve SQLite kullanılarak geliştirilmiştir. Kullanıcı arayüzü Tkinter ile inşa edilerek sanal emoji klavye, mesaj ve onay ekranları ile zenginleştirilmiştir.

Mevcut şifre yönetim sistemlerinin temel özellikleri, avantajları, dezavantajları ile popüler uygulamaların şifre oluşturma kısıtları göz önünde bulundurulmuş ve emoji tabanlı şifre oluşturma algoritması geliştirilmiştir. Geliştirilen şifre oluşturma

algoritması 8, 10, 12 ve 16 birim uzunluğunda, sadece emoji veya emoji ile birlikte kullanıcının belirlediği ASCII karakter kombinasyonlarına göre şifreler oluşturuyor.

Sistemde kaydedilen verilerin güvenliği için 128 bit anahtar uzunluğu ile Gelişmiş Şifreleme Standardı algoritması sayaç modu kullanılmıştır. Algoritmanın ihtiyacı olan 128 bit uzunluğundaki anahtar için bilgisayarın donanım bilgileri ve emoji matrisleri kullanılarak bir anahtar üretim algoritması geliştirilmiştir. Donanım değişimlerinde kurtarma için QR kod entegrasyonu sağlanmıştır.

Uygulama kullanılabilirlik, işlevsellik, güvenlik, birim testleri ve NIST SP 800-22 kriterleriyle değerlendirilmiştir. Sonuçlar, emoji kullanımının şifre çeşitliliğini ve entropisini arttırdığını, böylece kullanıcı deneyimini ve güvenliğini başarıyla korurken kaba kuvvet ve sözlük saldırılarına karşı direnci arttırdığını göstermektedir.

Anahtar Kelimeler: Anahtar üretimi, Emoji tabanlı şifre, Gelişmiş Şifreleme Standardı, Parola yöneticisi

University : T.C. İstanbul Kültür University
Institute : Institute of Graduate Studies
Department : Computer Engineering
Program : Computer Engineering
Supervisor : Assis. Prof. Dr. Öznur ŞENGEL
Degree Awarded and Date : MSc – June 2025

ABSTRACT

Today, users are compelled to come up with complex and long passwords for each program to secure their digital platform account better. Since it is hard to generate tough passwords and recall them, users reuse the same password for multiple platforms or resort to unsafe storage methods such as saving in plain text files, written on paper, or password storage through the browser. The techniques leave user passwords exposed to cyber-attacks.

Aside from the weakness brought by weak and habituated password usage and insecure storage habits, current methods of password creation mostly employ ASCII-based characters and generate more defenseless passwords to brute-force and dictionary attacks. This thesis presents a new system based on emoji for password management to improve account security on online platforms. The system, composed of a data layer, business logic layer, and presentation layer, is executed with Python and SQLite on Windows 11. Tkinter is employed to develop the user interface and enhance with a virtual emoji keyboard, message screens, and confirmation screens.

The basic traits, advantages, and disadvantages of existing password management systems, and password generation restrictions of popular applications were explored to design a new emoji-based password generation algorithm. This algorithm generates

8, 10, 12, and 16 units long passwords based on only emojis or combinations of emojis with user-defined custom ASCII characters.

To protect stored data, the Advanced Encryption Standard counter mode algorithm with a 128-bit key was employed. A specially designed key generation algorithm utilizing the computer's hardware specifications and emoji matrices for generating the encryption key was implemented. QR code integration during recovery in case of hardware alteration was incorporated.

The application was also tested for usability, functionality, security, unit tests, and on the foundation of NIST SP 800-22. The results indicate that emoji usage increases password diversity and entropy, thereby enhancing resistance to brute-force and dictionary attacks while successfully maintaining user experience and security.

Keywords: Key generation, Emoji-based password, Advanced Encryption Standard, Password manager