

**Správce hesel s dvoufaktorovou autentizací**

**Autor:** Michal Žernovič (230923), David Zeman(231304), Oliver Bielik (231229), Vojtěch Vaculík (230338)

**Obor:** BPC-IBE  
**Predmet:** BPC-AKR

Obsah

[Úvod 3](#_Toc85912173)

[Ciele projektu 4](#_Toc85912174)

[Teoretická časť 5](#_Toc85912175)

[Dvojfázové overenie 5](#_Toc85912176)

[Hash 5](#_Toc85912177)

[AES 5](#_Toc85912178)

[RSA 5](#_Toc85912179)

[Stav riešenia 6](#_Toc85912180)

[Autori 7](#_Toc85912181)

[Záver 8](#_Toc85912182)

[Prílohy 9](#_Toc85912183)

# Úvod

V dobe kedy je potrebný účet pre každú službu ktorú používame sa viac a viac rozširujú tzv. Password Managers. Ide o programy, v ktorých si môžeme uložiť heslá a dostať sa k nim pomocou jedného „master“ hesla. Vďaka takýmto programom môžeme zredukovať rôzne risky – môžeme používať komplexné heslá a nemusíme si ich pamätať, stačí nám master heslo. Tieto programy ponúkajú aj možnosť vygenerovať dlhé a bezpečné heslá a automaticky ich uložiť, takže užívateľ nemá dôvod používať to isté heslo na viac službách zo strachu, že by viac hesiel zabudol.

Prirodzene takýto software musí byť aj dostatočne chránený rôznymi kryptografickými funkciami a algoritmami. V tomto projekte vytvoríme jednoduchú aplikáciu na ukladanie hesiel s patričnými bezpečnostnými opatreniami.

# Ciele projektu

# Teoretická časť

## Dvojfázové overenie

Dvojfázové overenie je v dnešnej dobe veľmi rozšírený spôsob overenia, či je daný užívateľ oprávnený prihlásiť sa do služby. Typicky to býva SMS kód, alebo e-mail ktorý príde vlastníkovi účtu na iné zariadenie ako to z ktorého sa prihlasuje. Dvojfázovosť tohto overenia rozumieme v tom, že sú jednotlivé kroky od seba nezávislé.

Národný úrad štandardov a technológií (NIST) v smernici v roku 2016 zavrhoval SMS kódy ako validný spôsob overenia, avšak rok na to boli vo finalizovanej smernici považované za bezpečné. [1]

## Hash

Jeden z krokov pri ukladaní hesla v kryptografii je použitie hashovacej funkcie. Hashovacia funkcia musí spĺňať určité vlastnosti – Musí byť odolná voči získaniu pôvodnej správy, odolná voči získaniu inej predlohy a

## AES

## 

## RSA

# Stav riešenia

# Autori

# Záver

# Prílohy

Zdroje

[1] NIST Softens Guidance on SMS Authentication [online] 2021 [cit. 23-10-2021] https://www.onespan.com/blog/nist-softens-guidance-sms-authentication

[2] Cryptographic hash function [online] 2021 [cit. 23-10-2021]

https://en.wikipedia.org/wiki/Cryptographic\_hash\_function