DOI: https://doi.org/10.53052/9788367652124.07

Gracjan HANKUS[1], Olga VESELSKA[2]

Opiekun naukowy: Ruslana ZIUBINA[3]

# APLIKACJA GENERUJĄCA SILNE I ŁATWE DO ZAPAMIĘTANIA HASŁA

**Streszczenie:** W artykule opisano autorską aplikację, opracowaną w celu poprawy bezpieczeństwa użytkowników w sieci poprzez umożliwienie tworzenia silnych i jednocześnie łatwych do zapamiętania haseł. Wygenerowane hasła mają postać tzw. passphrase, co stanowi kompromis między wygodą użytkowania a bezpieczeństwem. Porównano hasła pochodzące z dwóch źródeł – własnej aplikacji oraz gotowych rozwiązań komercyjnych.

**Słowa kluczowe:** cyberbezpieczeństwo, hasło wyrazowe, generator haseł, menedżer haseł, aplikacja

# SOFTWARE GENERATING STRONG AND EASILY MEMORABLE PASSWORDS

**Summary:** The paper presents own software designed to enhance users' online security by creating strong and easily memorable passwords. Generated passwords take the form of passphrases, striking a balance between user convenience and security. The study compares passwords from two sources: own software and commercial ones.

**Keywords:** cybersecurity, passphrase, password generator, password manager, software

## 1. Wstęp

Wzrost cyfryzacji i dynamiczny rozwój technologii przyczyniły się do rewolucji sposobu prowadzenia życia codziennego. Obecnie Internet stał się nieodzownym narzędziem, które przenika niemal każdy aspekt życia. W obliczu rosnącej liczby usług online, pojawia się coraz więcej zagrożeń, na które narażeni są użytkownicy sieci. Cyberprzestępcy wykorzystują rosnącą popularność usług internetowych do

[1] Uniwersytet Bielsko-Bialski, Wydział Budowy Maszyn i Informatyki, specjalność: Techniki tworzenia oprogramowania, s52837@student.ubb.edu.pl
[2] Uniwersytet Bielsko-Bialski, Wydział Budowy Maszyn i Informatyki, specjalność: Techniki tworzenia oprogramowania, oveselska@ubb.edu.pl
[3] dr inż., Uniwersytet Bielsko-Bialski, Wydział Budowy Maszyn i Informatyki, rziubina@ubb.edu.pl

przeprowadzania różnorodnych ataków. W związku z tym, konieczne jest podjęcie środków mających na celu zapewnienie właściwej ochrony danych w świecie cyfrowym. Jednym z nich jest wybór odpowiedniego hasła, gdyż stanowi ono pierwszą linię obrony przed niepowołanym dostępem do konta i kradzieżą danych. Zaleca się, aby korzystać z różnych haseł do różnych kont, jednak to rozwiązanie staje się uciążliwe – współczesne standardy bezpieczeństwa wymagają, aby hasła były złożone z kombinacji liter, cyfr i znaków specjalnych. Hasła w postaci losowych ciągów znaków są praktycznie niemożliwe do zapamiętania, dlatego w odpowiedzi na ten problem opracowano aplikację, która generuje hasła w postaci tzw. passphrase, czyli haseł wyrazowych, opartych na pewnej frazie, powiedzeniu czy przysłowiu.

## 2. Polityka tworzenia silnych haseł

Silne i trudne do odgadnięcia hasła są kluczowym czynnikiem wpływającym na bezpieczeństwo użytkowników. Aby zapewnić skuteczną ochronę, hasło powinno zawierać: minimum 12 znaków, wielkie i małe litery, cyfry oraz znaki specjalne. Mimo że hasła składające się z losowych znaków są trudne do złamania, często stają się praktycznie niemożliwe do zapamiętania. Najlepszym rozwiązaniem jest stosowanie tzw. passphrase – hasła opartego na pewnej frazie, np. wyrażenie „Ala ma dwa białe koty i trzy czerwone papugi" może zostać zapisane jako „Ama2BKi3CPap". Takiej postaci hasło, choć może wydawać się skomplikowane, jest łatwe do zapamiętania dla osoby, która zna sposób jego powstania. Hasła frazowe stanowią kompromis między bezpieczeństwem a wygodą. Zaleca się, aby tworzyć hasło na podstawie kilku wyrazów lub zdania. Aby zwiększyć jego złożoność, warto wprowadzić zmianę kapitalizacji tekstu oraz zamienić niektóre litery na znaki specjalne, np. „S" na „$" czy „B" na „8". Tworząc hasło, nie trzeba używać całych wyrazów – można je skrócić, np. do dwóch pierwszych liter. Dodatkowo, dobrą praktyką jest wstawienie cyfr lub znaków specjalnych do hasła [1, 2, 3].

## 3. Analiza istniejących programów generujących hasła

Na rynku dostępnych jest wiele rozwiązań służących do generowania i zarządzania hasłami, co daje użytkownikom bardzo szeroki wybór. Aplikacje różnią się m.in. oferowanymi funkcjami, ceną, interfejsem użytkownika czy sposobem przechowywania i zabezpieczania haseł. Komercyjne rozwiązania można podzielić na trzy kategorie – generatory haseł, menedżer haseł oraz internetowe generatory haseł.

Generatory dają możliwość konfiguracji hasła – użytkownik może dostosować jego długość oraz wybrać rodzaj użytych znaków. Zapamiętanie wygenerowanych haseł okazuje się niewygodne, gdyż mają postać losowych ciągów znaków. Ich utrwalenie staje się praktycznie niemożliwe, zwłaszcza jeśli użytkownik używa wielu haseł tej postaci. W takim przypadku warto skorzystać z menedżera haseł, który umożliwi ich bezpieczne przechowywanie.

Dostęp do menedżera możliwy jest po wprowadzeniu hasła głównego, które jest wymagane przy każdym uruchomieniu aplikacji. W ten sposób zapewniony zostaje dodatkowy poziom bezpieczeństwa dla użytkowników i ochrona prywatnych danych.

Hasło główne zwykle zostaje ustawione podczas konfiguracji aplikacji i może być zmienione w dowolnym momencie. Menedżer często oferuje rozszerzenia do popularnych przeglądarek oraz aplikacje mobilne na systemy Android i iOS. Pozwalają także na synchronizację danych w chmurze, dzięki czemu użytkownicy mogą mieć do nich dostęp z różnych urządzeń bez konieczności zapamiętywania ich. Wszystkie dane są szyfrowane, co zapewnia bezpieczeństwo i ochronę przed nieautoryzowanym dostępem. Oprócz funkcji przechowywania haseł, menedżer również posiada wbudowane generator.
Na rynku istnieją także generatory dostępne na stronach internetowych. Są to narzędzia, które nie wymagają instalacji oprogramowania na urządzeniu. Ich zasada działania jest taka sama jak w przypadku zwykłych generatorów.

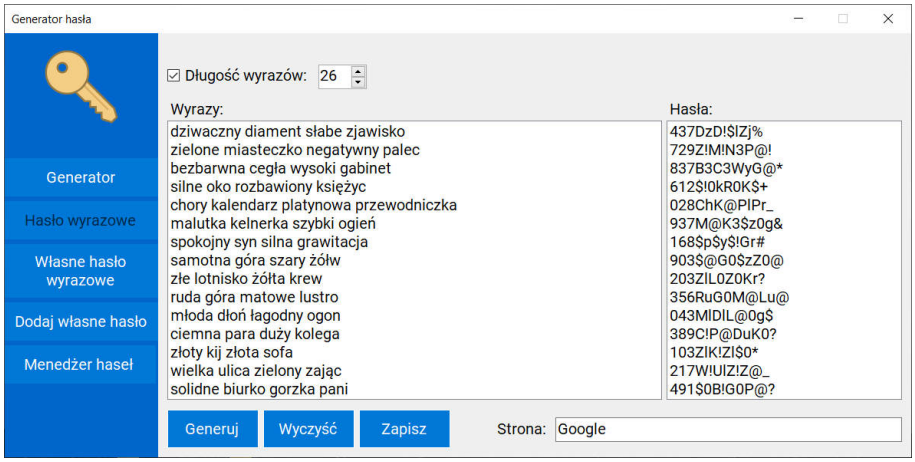
## 4. Opis programu generującego silne i łatwe do zapamiętania hasła

### 4.1. Przeznaczenie programu

Program skierowany jest dla osób używających wielu różnych haseł do kont internetowych, których zapamiętanie staje się uciążliwe. Aplikacja pozwala użytkownikowi wygenerować unikalne i silne hasła, które są łatwe do zapamiętania, a także bezpiecznie przechowywać je w jednym miejscu. Dzięki temu nie musi on zapisywać haseł w zeszycie, na telefonie lub innych niebezpiecznych miejscach, aby je zapamiętać.

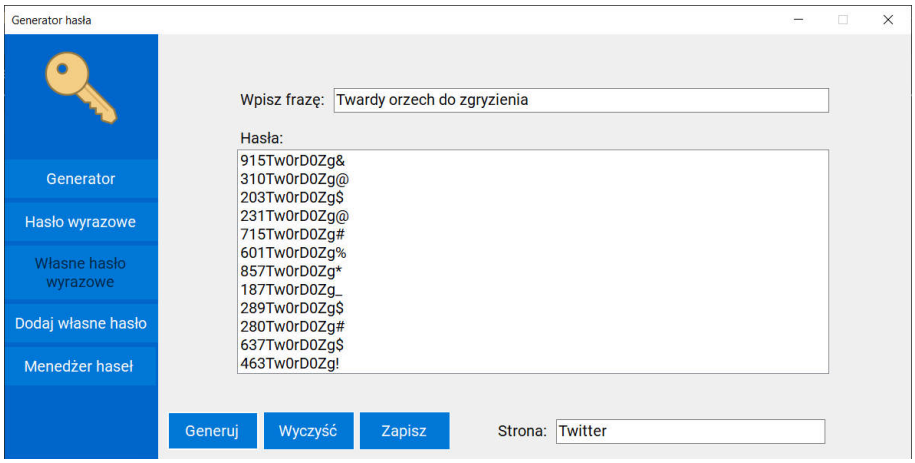
### 4.2. Budowa programu

Program zbudowany jest z okien, między którymi użytkownik może się przełączać. Pozwalają one na wybór sposobu generowania haseł oraz ich zapis do bazy wraz z wyświetleniem. Użytkownik może opcjonalnie podać nazwę strony, do której hasło ma zostać użyte.
Pierwsze okno to generator haseł w postaci losowych ciągów znaków. Pomimo że hasła tej postaci są trudne do zapamiętania, znajdują się w programie na wypadek, gdyby użytkownik mimo wszystko chciał ich używać. Użytkownik może w pełni skonfigurować hasła, wybierając odpowiednie parametry.
Drugie okno oferuje generowanie haseł na podstawie abstrakcyjnych połączeń wyrazów tworzonych według schematu: przymiotnik + rzeczownik. Program losuje po dwa przymiotniki i rzeczowniki z bazy oraz łączy je ze sobą. W ten sposób powstają zbitki wyrazowe, które łatwo zapamiętać. Im bardziej fikcyjne tym trudniej będzie złamać hasło.




*Rysunek 1. Widok okna generatora haseł tworzonych na podstawie zbitek wyrazowych*

Trzecie okno to generator, który tworzy hasła wykorzystując dane wprowadzone przez użytkownika. Zaleca się, aby był to tekst, który bardzo dobrze zapada w pamięć – znane powiedzenie, przysłowie, cytat, fragment tekstu piosenki czy łacińska sentencja. Dzięki temu użytkownik bez problemu zapamięta silne hasło.




*Rysunek 2. Widok okna generatora haseł tworzonych na podstawie wpisanej frazy*

W przypadku gdy hasła wygenerowane przez poprzednie generatory nie spełniają oczekiwań użytkownika, może on wprowadzić do bazy swoje własne. Przed zapisem następuje sprawdzenie, czy wpisana fraza widnieje na liście najpopularniejszych haseł – jeśli nie, program pomyślnie zapisuje ją do bazy.

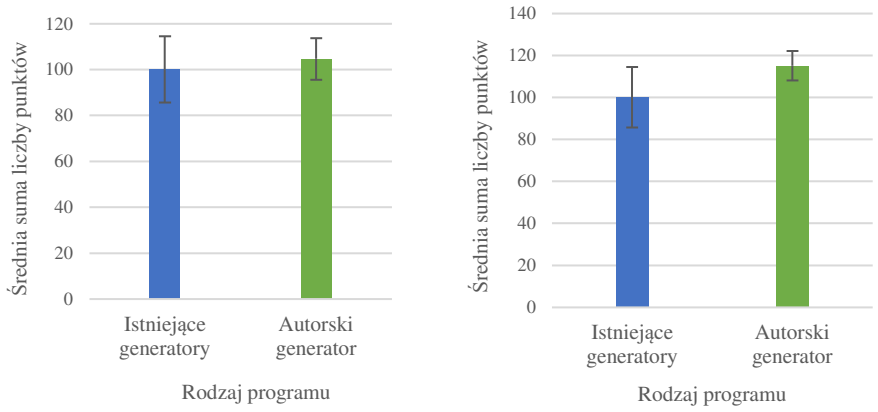
Ostatnim oknem aplikacji jest menedżer haseł, do którego dostęp możliwy jest po wpisaniu przez użytkownika hasła. Po pomyślnym zalogowaniu, użytkownik uzyskuje dostęp do swoich haseł. Aby zapobiec przechwyceniu haseł przez osoby niepożądane, podczas ich zapisu zastosowano szyfrowanie RSA.

### 4.3. Opis algorytmu generowania haseł w postaci passphrase

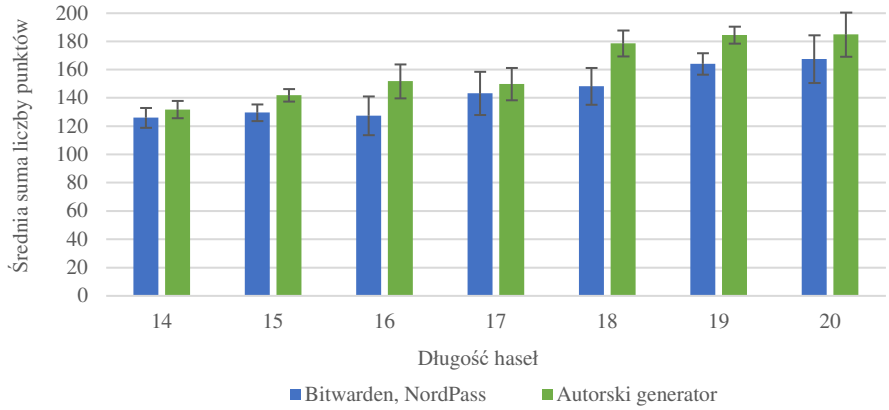
Na początku utworzonych haseł znajdują się trzy losowe cyfry. Następnie hasła zawierają dwie początkowe litery każdego wyrazu zbitki, a pierwszej z nich zostaje zmieniona wielkość. Polskie znaki diakrytyczne zostają zmienione na podstawowe, a niektóre litery na inne znaki, tak aby zwiększyć złożoność haseł. Hasło zakończone jest losowym znakiem specjalnym.
W oknie, w którym użytkownik wprowadza własne hasło wyrazowe, idea tworzenia haseł zmienia się w przypadku, gdy wpisana fraza jest krótka (zawiera do 15 znaków). Na początku również znajdują się trzy losowe cyfry, następnie jednak program łączy je ze wszystkimi znakami występującymi we frazie, uwzględniając zmianę znaków oraz wielkości liter. Wyrazy oddzielone są myślnikiem.

## 5. Ocena skuteczności wygenerowanych haseł

Aby porównać wygenerowane hasła, wykorzystano wybrane funkcje narzędzia opracowanego przez Uniwersytet Illinois w Chicago, które ocenia siłę hasła przyznając punkty dla poszczególnych kryteriów [4]. Punkty są obliczane na podstawie wzorów i przyjmują wartości dodatnie lub ujemne, w zależności od kryterium. Kryteria uwzględnione w ocenie to: liczba znaków, wielkie litery, małe litery, cyfry, znaki specjalne, sekwencje wielkich liter, sekwencje małych liter, sekwencje cyfr, sekwencje kolejnych liter, sekwencje kolejnych cyfr, sekwencje kolejnych znaków specjalnych. Na poniższym rysunku przedstawiono porównanie siły haseł pochodzących z autorskiej aplikacji oraz z komercyjnych rozwiązań.




*Rysunek 3. Wykresy przedstawiające porównanie siły haseł. Po lewej – hasła w postaci losowych ciągów znaków. Po prawej – hasła w postaci losowych ciągów znaków (kolor niebieski) oraz hasła wyrazowe (kolor zielony).*




*Rysunek 4. Wykres przedstawiający porównanie siły haseł dla haseł wyrazowych*

## 6. Wnioski

W artykule omówiony został temat haseł. Opisano zalecany sposób generowania silnych haseł, istniejące rozwiązania komercyjne oraz własną aplikację wraz z oceną skuteczności. Zaprojektowana aplikacja łączy w sobie funkcje programów dostępnych na rynku, które pozwalają wygenerować i bezpiecznie przechowywać silne hasła. To, co odróżnia autorski projekt od gotowych rozwiązań, to możliwość tworzenia trudnych do złamania haseł, jednocześnie łatwych do zapamiętania. Proponowaną metodą jest generowanie haseł w postaci passphrase. Ich siłę określono na podstawie obliczonych punktów – im więcej punktów zdobyło hasło, tym mniejsza jest jego podatność na złamanie. Autorski program uzyskał wyższe wyniki niż istniejące na rynku aplikacje. Warto dodać, że słupki błędów dla aplikacji własnego autorstwa były zawsze niższe niż dla istniejących programów – świadczy to o mniejszym rozrzucie punktów.

## LITERATURA

1. STAMP M.: Information Security: Principles and Practice, 2nd Edition, John Wiley & Sons, Hoboken, 2011, s. 231-234
2. Serwis internetowy firmy Microsoft: Tworzenie i używanie silnych haseł, h*ttps://support.microsoft.com/pl-pl/windows/tworzenie-i-u%C5%BCywanie-silnych-hase%C5%82-c5cebb49-8c53-4f5e-2bc4-fe357ca048eb*, 07.10.2023
3. Serwis internetowy Uniwersytetu w Buffalo: How to Create a Secure Passphrase, *https://www.buffalo.edu/content/www/ubit/service-guides/safe-computing/_jcr_content/rightcol/download_1820535914/file.res/how-to-create-a-secure-passphrase-2017-08-10_HQP.pdf*, 07.10.2023
4. Serwis internetowy Uniwersytetu Illinois w Chicago: *https://www.uic.edu/apps/strong-password/*, 07.10.2023