Bezpieczeństwo Systemów Komputerowych
Praca domowa 2

Paweł Bogdan, Igor Podolak

Termin oddania: 6 listopada 2016, godzina 23:55:00

1 Treść zadania

Zadanie polega na "łamaniu" funkcji mieszającej MD5. Na stronie wykładu na platformie `pegaz.uj.edu.pl` jest katalog z plikami o nazwie

`imie_nazwisko.zip`

W każdym takim archiwum są pliki:

1.in - znajdują się w nim hasze słów języka polskiego niezawierające polskich znaków. Słowa zawierają tylko małe litery.

2.in - znajdują się w nim hasze słów języka polskiego. Słowa zawierają tylko małe litery.

3.in - znajdują się w nim hasze słów języka polskiego. Słowa zawierają zarówno małe jak i wielkie litery (nie więcej niż 3 wielkie litery)

4.in – znajdują się w nim hashe haseł złożonych z wielu słów z języka polskiego z dodatkowymi znakami specjalnymi i cyframi.

We wszystkich plikach każdy hash jest w osobnej linijce. Wszystkie słowa wykorzystywane w zadaniach zostały zaczerpnięte ze słownika z odmianami, który można znaleźć na stronie `www.sjp.pl` – zostały wybrane tylko słowa w podstawowej wersji (pierwsze z wiersza)
Do stworzenia hasha posłużyło nam poleceni:

```
hashlib.md5(w.encode('utf-8')).hexdigest()
```

2 Zasady oceniania

Za zadanie można uzyskać 100%. W skład 100% będą wchodziły następujące składniki:

20% – Złamanie wszystkich haszy z pliku 1.in

30% – Złamanie wszystkich haszy z pliku 2.in

50% – Złamanie wszystkich haszy z pliku 3.in

Za złamanie każdego z haszy z pliku 4.in można dostać dodatkowy 1% który uzupełni braki z pozostałych prac domowych. Jeżeli ktoś będzie miał maksymalną ilość punktów z prac domowych to dodatkowe punkty zostaną proporcjonalnie doliczone do puli punktów dających zaliczenie.

3 Wskazówki do wysyłania rozwiązań

Aby zadanie zostało sprawdzone, jako rozwiązanie przez platformę pegaz należy przysłać archiwum ZIP o nazwie pasującej do wzorca:

`imie_nazwisko.zip`

oczywiście bez polskich znaków narodowych. Gdyby rozwiązanie wysyłał Paweł Bogdan, to jego paczka musiałaby się nazywać:

`pawel_bogdan.zip`

Wewnątrz paczki mają się znajdować pliki:

1.out

2.out

3.out

4.out

kod.zip – archiwum z kodami, których Państwo użyliście do rozwiązania pracy domowej

Każdy z plików ma mieć strukturę podobną do pliku wejściowego. W kolejnych linijkach plików mają się znajdować dwa ciągi znaków oddzielone pojedynczą spacją: oryginalny hash i słowo, które ten hash daje. Pliki mają mieć kodowanie UTF-8.
Zachęcam do podejrzenia pliku pawel_bogdan.zip, który jest rozwiązaniem zadania z paczki pawel_bogdan.zip w katalogu Dane wejściowe