Bezpieczeństwo komputerowe

Badanie poziomu zabezpieczeń wykorzystywanych w systemie wypożyczalni Wrocławskiego Roweru Miejskiego

Lista 2

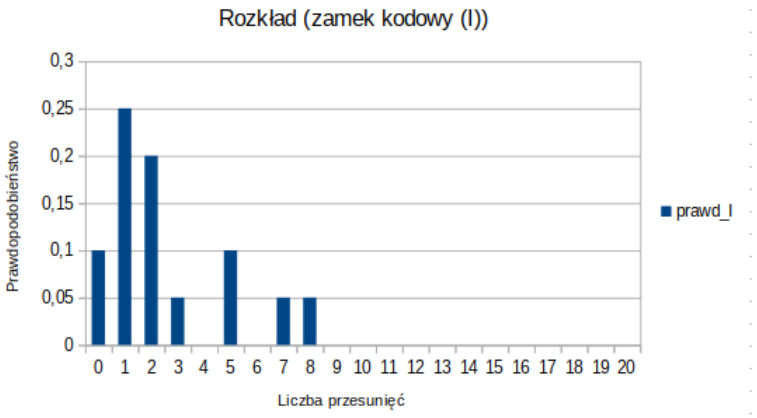
Jakub Gogola
236412

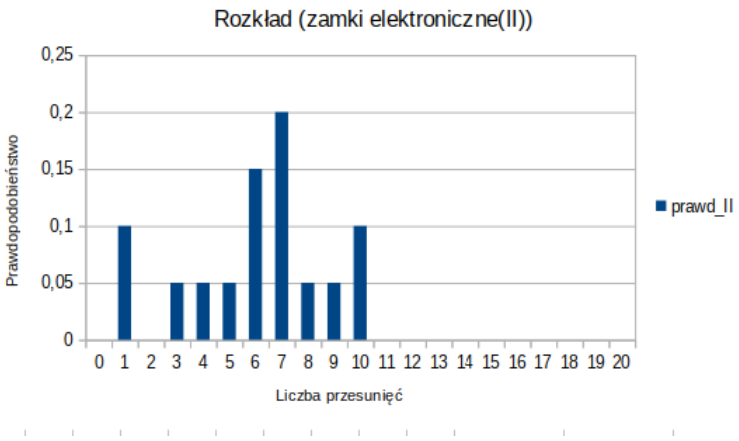
31 października 2018

Wrocławski Rower Miejski to system umożliwiający mieszkańcom Wrocławia wypożyczanie rowerów w specjalnych stacjach (wypożyczalniach) za pomocą aplikacji mobilnej. Rowery są w nich zabezpieczone za pomocą specjalnych zamków elektornicznych, które można odblokować wypożyczając dany jednoślad za pomocą wspomnianej aplikacji. W wypadku, gdy wszystkie stojaki wyposażone w zamki są zajęte, rower może zostać zabezpieczony za pomocą zamka kodowego, do którego kod również jest dostępny za pośrednictwem aplikacji. Wspomniany kod zostaje ujawniony użytkownikowi systemu WRM w momencie wypożyczenia danego pojazdu.

1 Problem

Celem zadania było zbadanie poziomu zabezpieczeń rowerów w systemie wypożyczalni Wrocławskiego Roweru Miejskiego. Należało wypożyczyć przynajmniej po 15 rowerów zabezpieczonych za pomocą zamków elektronicznych i 15 rowerów zabezpieczonych zamkami kodowymi. Przy każdym wypożyczeniu należało notować rodzaj zabezpieczenia, kod służący do odblokowania zamka kodowego oraz rzeczywisty kod pozostawiony przez poprzedniego użytkownika. Następnie należało policzyć rozkład zmiennej losowej X, która określała ile przestawień na danym zamku należy zrobić, aby odblokować rower. Zabrane dane znajdują się w pliku `rowery.csv`. Oto wyniki:





Oprócz tego została policzona entropia według wzoru:

$$H(X) = -\sum_{i=1}^{n} \mathbb{P}[X = i] \cdot \log_2 \mathbb{P}[X = i]$$

Dla rowerów zapiętych na zamek elektroniczny entropia wyniosła $2,61979810080172$, a dla pozostałych $2,27706045218805$.

Ponadto, złodziej potrzebowałby średnio 2 przesunięć, aby odpiąć rower zamknięty na zamek kodowy.

2 Podsumowanie

Zwiększenie długości PINu lub dodanie do niego również liter nie zwiększyłoby zapewne bezpieczeństwa systemu, ponieważ użytkownicy i tak zmienialiby kod najczęściej na jednej pozycji.

Biorąc pod uwagę fakt, że zamki nie zapewne zmieniane z dnia na dzień, dosyć łatwo (w krótkim okresie czasu od zebrania danych) można by zweryfikować czy użytkownik zebrał prawdziwe dane czy też je wygenerował porównując dane dla danego roweru.