## **Bezpieczeństwo komputerowe**

Laboratorium – lista nr 2 (grupa A), 4 XI

1. Zebrane dane

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Id | Numer roweru | Kod cyfrowy | Kod fizyczny | Zamknięcie |
| 1 | 57650 | 7528 | 7538 | kat. I |
| 2 | 57100 | 1322 | 1111 | kat. I |
| 3 | 57258 | 1442 | 1450 | kat. II |
| 4 | 57476 | 3247 | 3347 | kat. II |
| 5 | 57514 | 8807 | 1151 | kat. II |
| 6 | 57162 | 6842 | 6843 | kat. I |
| 7 | 57147 | 9925 | 9936 | kat. I |
| 8 | 57792 | 5552 | 5510 | kat. I |
| 9 | 57772 | 4351 | 4120 | kat. I |
| 10 | 57301 | 9268 | 2210 | kat. II |
| 11 | 57162 | 6842 | 6962 | kat. II |
| 12 | 57100 | 1322 | 1211 | kat. I |
| 13 | 63749 | 4420 | 4978 | kat. II |
| 14 | 57163 | 2483 | 3583 | kat. I |
| 15 | 57612 | 8142 | 8142 | kat. I |
| 16 | 57732 | 5117 | 5117 | kat. I |
| 17 | 57127 | 9339 | 9339 | kat. I |
| 18 | 57428 | 1086 | 3206 | kat. II |
| 19 | 57324 | 1995 | 5991 | kat. II |
| 20 | 57797 | 3956 | 4068 | kat. II |
| 21 | 57824 | 4393 | 4293 | kat. II |
| 22 | 57231 | 9063 | 9064 | kat. II |
| 23 | 57688 | 7055 | 7077 | kat. II |
| 24 | 57663 | 7282 | 6948 | kat. II |
| 25 | 57293 | 4824 | 1593 | kat. II |
| 26 | 57955 | 8221 | 8886 | kat. II |
| 27 | 57540 | 5664 | 5665 | kat. II |
| 28 | 57200 | 5329 | 5089 | kat. I |
| 29 | 63730 | 7236 | 7237 | kat. II |
| 30 | 57115 | 9448 | 9560 | kat. II |

Legenda skrótów:

* kat. I – dany rower zamknięty jest za pomocą zamka elektronicznego
* kat. II – dany rower zamknięty jest wyłącznie za pomocą zamka fizycznego

1. Analiza danych

Link do *Cracking Android pattern lock in five attempts*.

<https://www.lancaster.ac.uk/staff/wangz3/publications/ndss_17.pdf>

Tak jak na obrazku można 4-cyfrowy kod podzielić na różne osobne pozycje. Taki rozkład tego kodu będzie najlepszy ponieważ pozycje są niezależne od siebie, a najważniejsze są przesunięcia pojedynczych pozycji w górę lub w dół, aby uzyskać kod dostępu do zapiętego roweru.



**Ważne spostrzeżenie!**

Po przeanalizowaniu wszelkich danych widzimy, że kody cyfrowe od kodów fizycznych bardzo się nie różnią, a niektórych przypadkach nawet nie są zmienione. Te nie zmienione kody występują tylko przy rowerach **kat. I**. Zakładam, że taka sytuacja się zdarza, gdy osoba wypożyczająca rower odpina rower tylko za pomocą zamka fizycznego (gdzie nie zapina bezpiecznie zamka), a następnie po podróży oddaje rower do bazy, czyli zamka elektrycznego. Po oględzinach wszelkich wyników łatwo zauważyć, że cyfra z pierwszej pozycji jest bardzo często nie przestawiona, aż w 70% przypadków pierwsza pozycja była taka sama jak na kodzie cyfrowym. Czyli można uznać, że łamanie kodu w 80% dotyczy tylko 3 pozycji niezależnych od siebie.

**RAZ ZEBRANE – SZUKAJ I KRADNIJ**

Dobrze zauważyć, że raz już wypożyczony rower ma zawsze (przynajmniej przez cały sezon) taki sam kod odblokowania. Raz poznany kod umożliwia nam zdobycie roweru bez zgadywania. Czyli tak jak zleca zadanie, jeżeli każdy z osoby zbierze 30 kodów odblokowujących rower to mamy, bardzo dużo kodów, co pozwala nam na złamanie szyfru znając wszelkie kody!