Generator Liczb Losowych

Laboratorium Bezpieczeństwa Systemów Teleinformatycznych (cz. 2)

Wykonali:

Waldemar Wagner, Krystian Tworzewski

Data oddania:

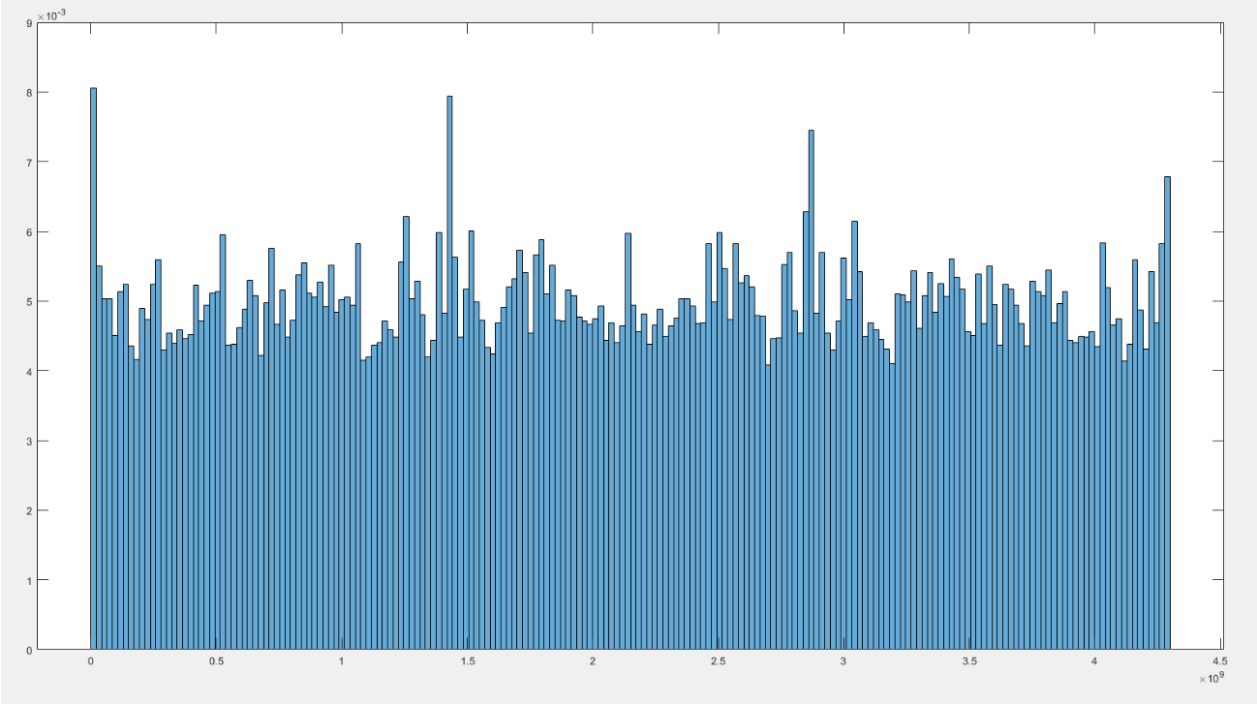
27.05.2021 r.

Podstawa opracowania:

H. Zhu , C. Zhao , X. Zhang , L. Yang, „A novel iris and chaos-based random number generator”, Computers & Security, vol. 36, pp. 40-48, July 2013.

Zakres danych testowych:

Na potrzeby realizowanego pakietu testów wygenerowano 20 000 000 liczb 32- bitowych, o empirycznym rozkładzie bliskim równomiernemu, przedstawionym poniżej:

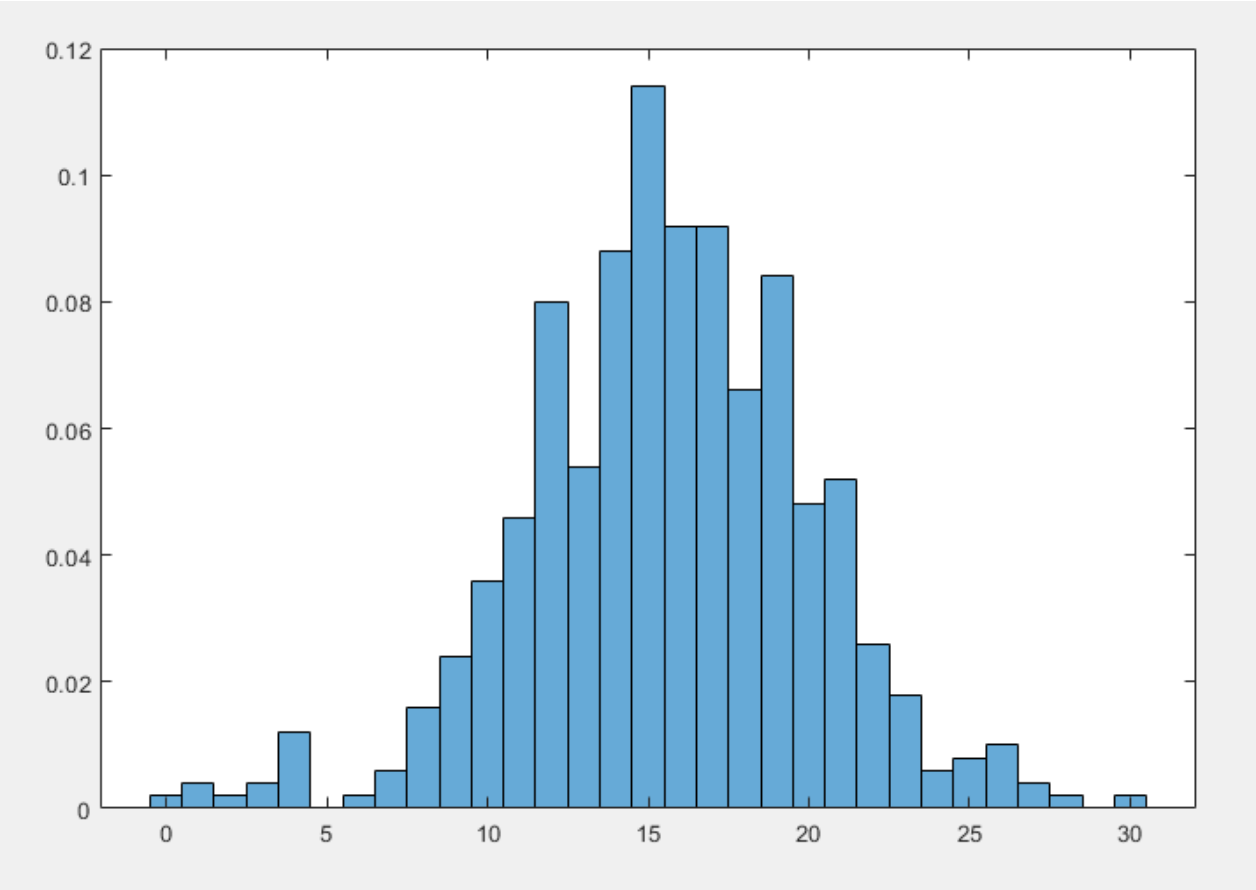


Entropia wyliczona zgodnie ze wzorem: $e = -\sum i\ pi\ log2\ (pi\ )$, dla powyższego rozkładu wynosi 21.4161 bita.

Test nr 1 - Birthday Spacings Test

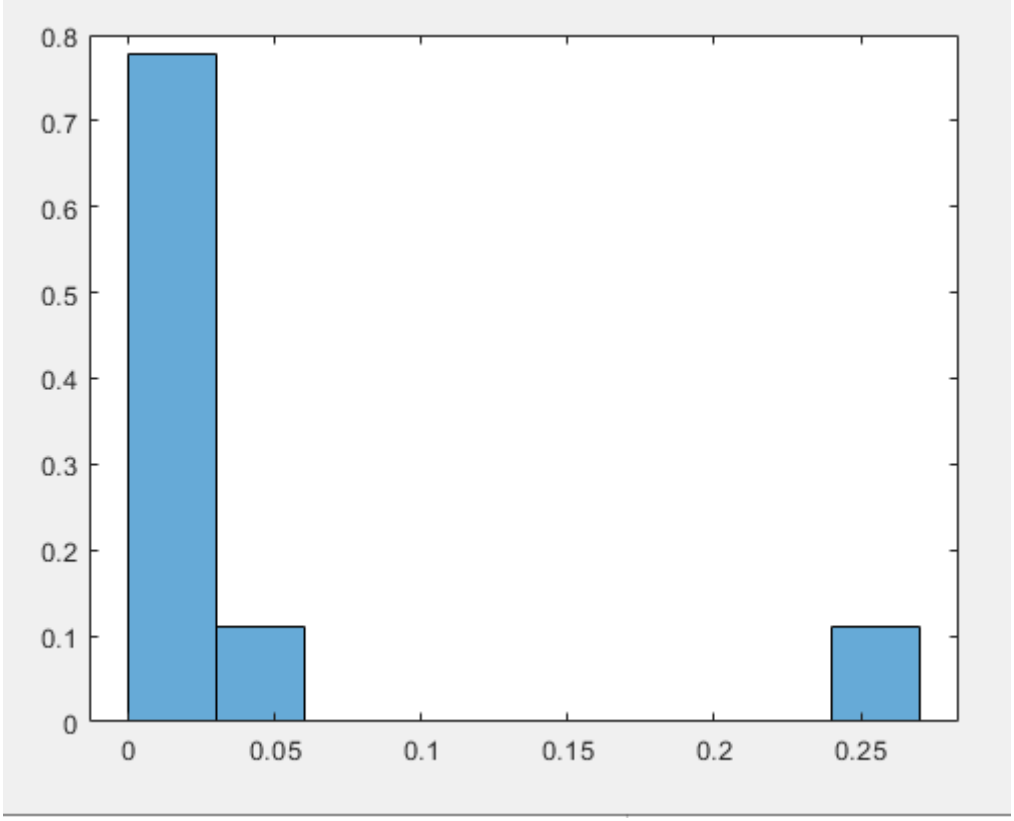
Na potrzeby przeprowadzenia Birthday Spacings Test wykorzystane zostało 512 000 liczb 32-bitowych podzielone na podciągi zawierające 1024 liczb. Dany podciąg reprezentuje sekwencję „urodzin". Na posortowanych liczbach zostały zdefiniowane odstępy, które były różnicą kolejnych liczb. Każda próbka liczby równych odstępów jest zmienną o rozkładzie Poissona z wartością oczekiwaną $n^3/4k$. Pojedyńczy test na 1024 liczbach 32-bitowych wykonano 500 razy, w którym z każdym z tych testów uzyskany został empiryczny rozkład zliczeń urodzin, które powtórzyły się wiecej niz raz.

Przykładowy rozkład jednego z 500 testów został przedstawiony poniżej:



Dla wygenerowanych 9 rozkładów empirycznych wykonano test dopasowania Kołmogorowa-Smirnowa w odniesieniu do rozkładu równomiernego, z każdego porównania uzyskując wartość p.

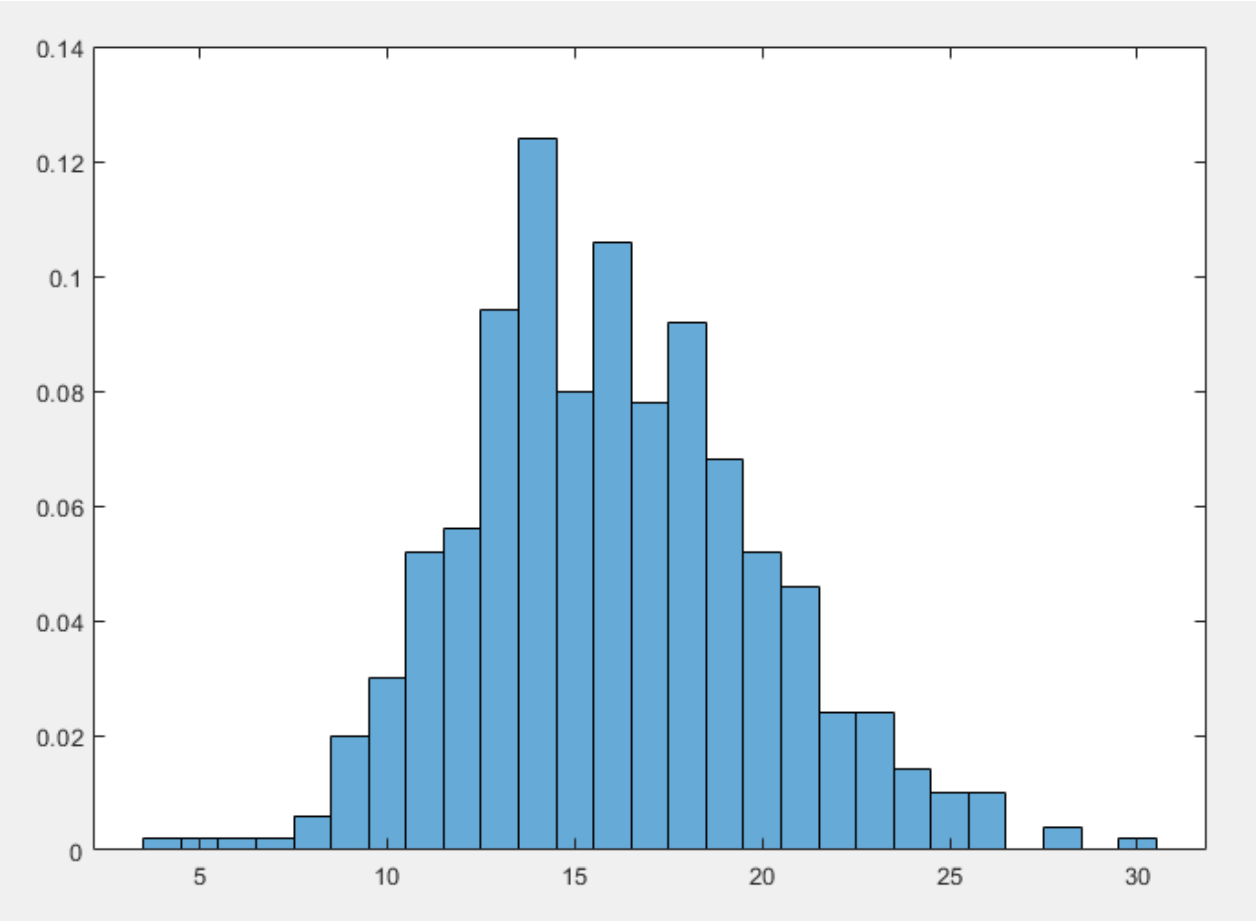
Dla 9 wartości p uzyskano rozkład empiryczny przedstawiony poniżej:



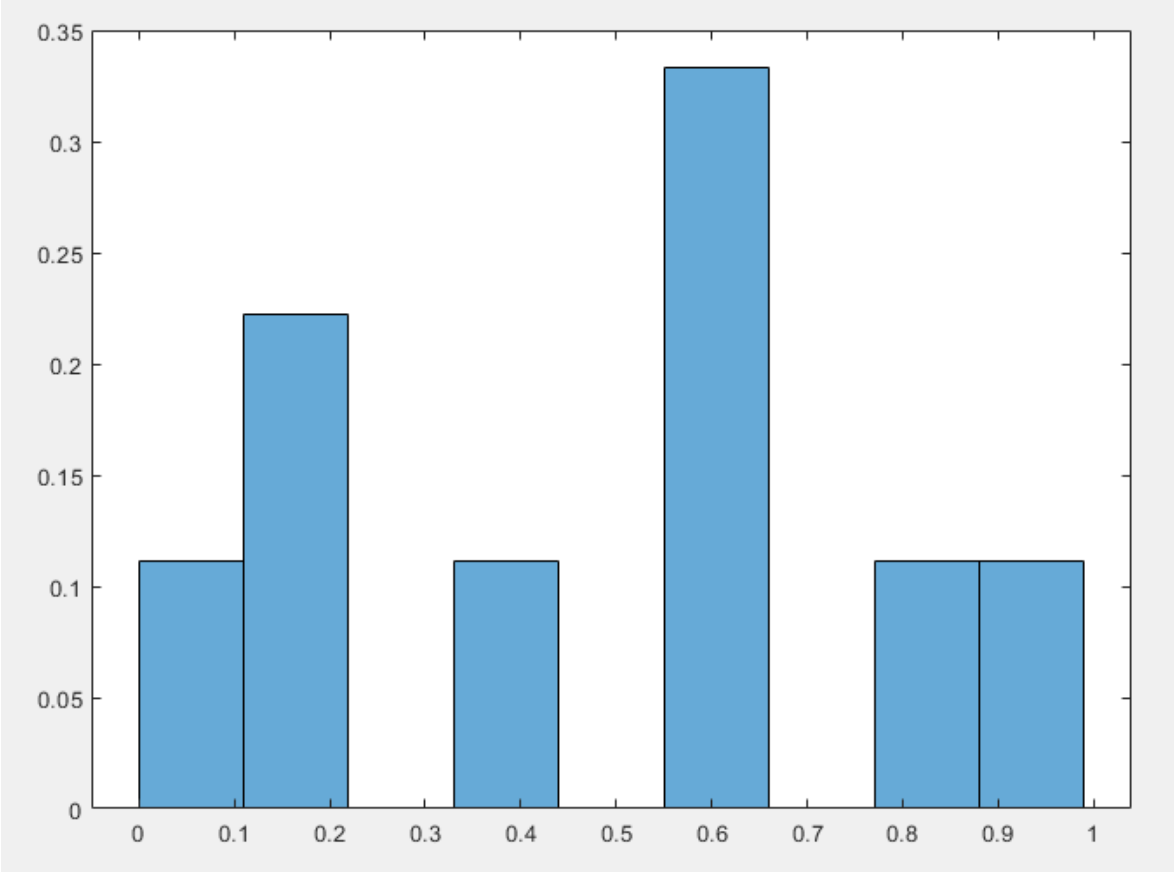
Weryfikacja zgodności dopasowania za pomocą testu Kołmogorowa-Smirnowa wykazała $p =$ 1.5706e-07, co niestety dla liczb wygenerowanych z implementowanego generatora, hipoteza zerowa nie jest spełniona.

Aby sprawdzić, czy implementacja testu urodzinowego jest poprawna wykorzystany został generator systemowy.

Przykładowy rozkład jednego z 500 testów dla generatora systemowego został przedstawiony poniżej:



Dla wygenerowanych 9 rozkładów empirycznych wykonano test dopasowania Kołmogorowa-Smirnowa w odniesieniu do rozkładu równomiernego, z każdego porównania uzyskując wartość p. Dla 9 wartości p uzyskano rozkład empiryczny został przedstawiony poniżej:

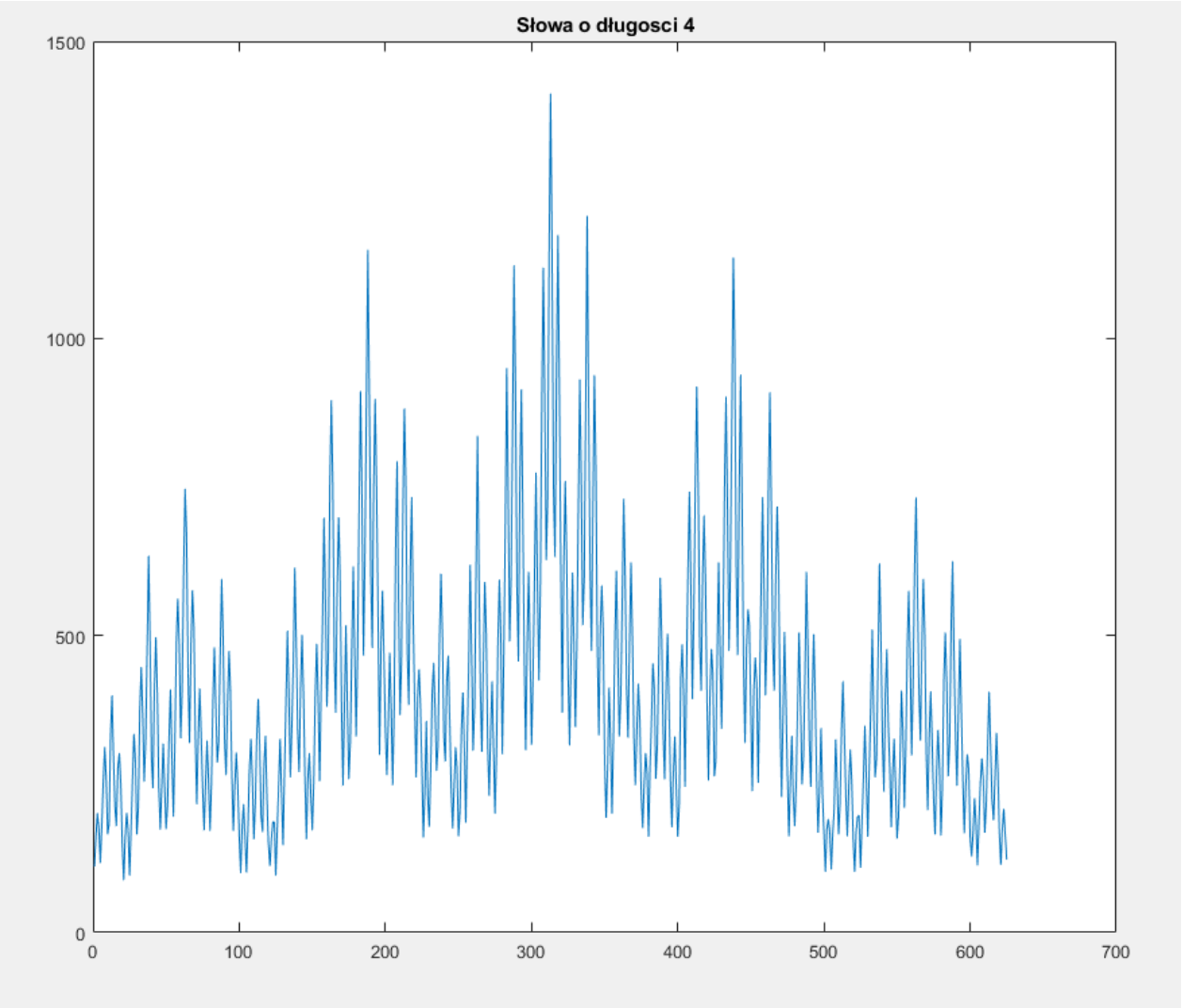


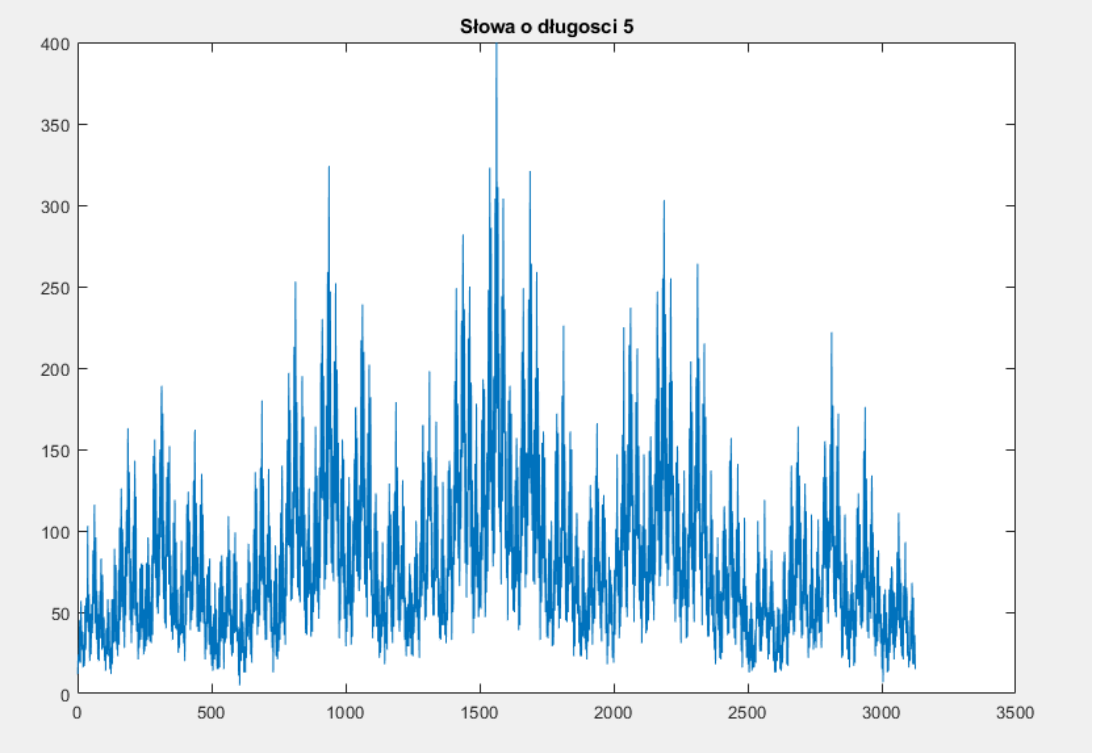
Weryfikacja zgodności dopasowania do rozkładu równomiernego za pomocą testu Kołmogorowa-Smirnowa wykazała $p =$ 0.7133, a więc wartość prawdopodobną mieszczącą się w zakresie $p < 0{,}025$ lub $p > 0{,}975$.

Test nr 2 - Count-the-Ones Tests

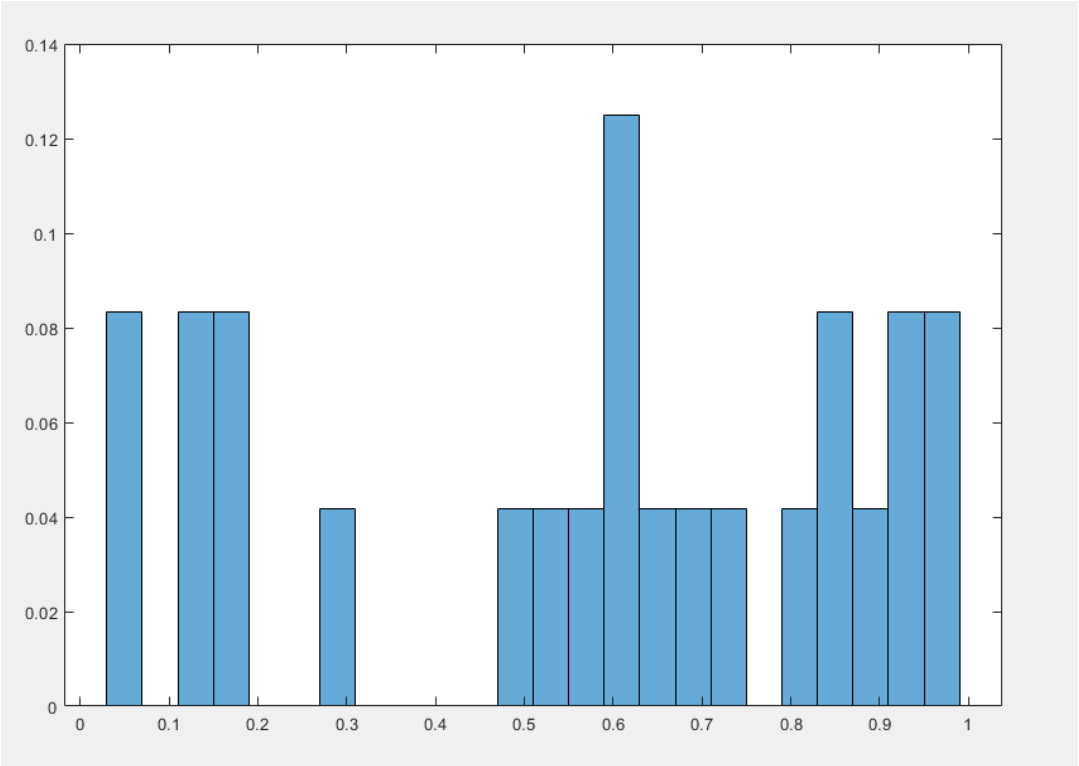
Na potrzeby przeprowadzenia Birthday Spacings Test wykorzystane zostało 6 144 000 liczb 8-bitowych podzielone na podciągi zawierające 256 000 liczb. Dla każdego strumienia bajtów liczby ilość występujących „jedynek". Każdy bajt został zamieniony na literę odpowiednio ze wcześniej policzoną ilością „jedynek". Ciąg stworzony z liter został podzielony na pięcio i czteroliterowe nakładające się słowa. Częstość występowania każdego słowa została poddana do testu chi-kwadrat jako różnica sum Pearsona Q5-Q4.

Poniżej przedstawiony jest przykładowy wykres wystąpień słów 5 i 4-literowych. Jest to wartość obserwowana wykorzystywana do wzoru na chi-square.





Dla wygenerowanych 24 rozkładów empirycznych wykonano test dopasowania Kołmogorowa-Smirnowa w odniesieniu do rozkładu równomiernego, z każdego porównania uzyskując wartość p. Dla 24 wartości p uzyskano rozkład empiryczny został przedstawiony poniżej:

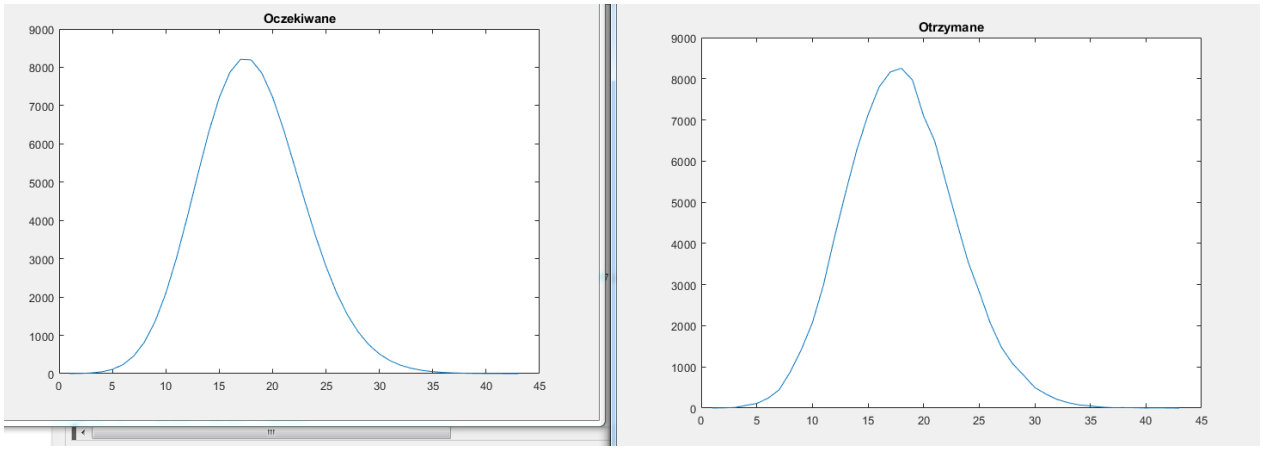


Weryfikacja zgodności dopasowania do rozkładu równomiernego za pomocą testu Kołmogorowa-Smirnowa wykazała $p =$ 0.2189, a więc wartość prawdopodobną mieszczącą się w zakresie $p < 0{,}025$ lub $p > 0{,}975$.

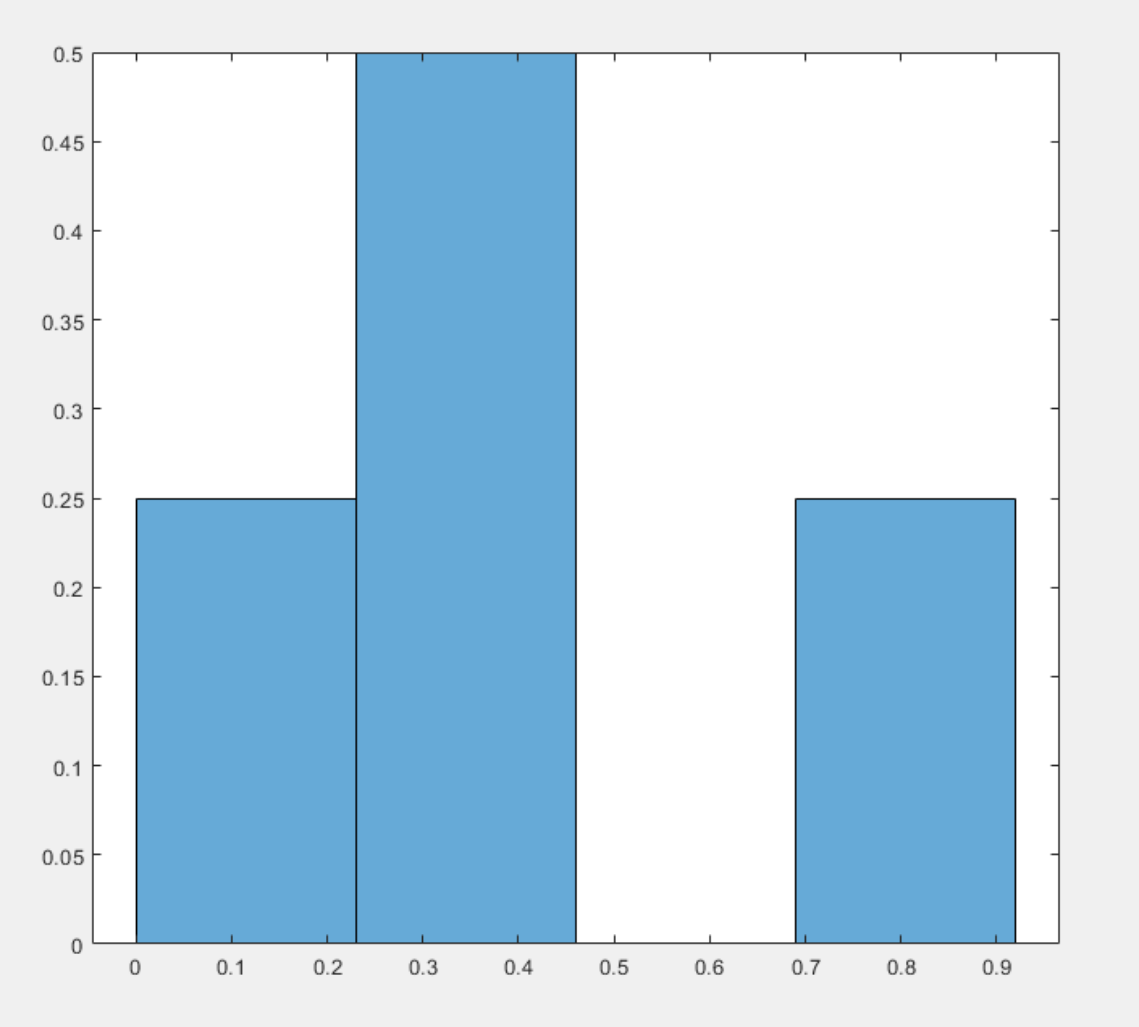
Test nr 3 - Squeeze Test

Na potrzeby przeprowadzenia Squeeze Test wykorzystane zostało 20 000 000 liczb 32-bitowych. Każda z liczb jest dzielona przez 2^{32} w celu uzyskania liczb z przedzialu [0,1). Wykonane zostało 4 iteracje po 5 000 000 liczb i z każdego została uzyskana p-wartość. Pojedyńczy test polega na na zmniejszaniu początkowej wartości k = 2147483647 przy zastosowaniu formuly $\lceil kf \rceil$, gdzie f jest to kolejna wygenerowana liczba, do momentu gdy uzyskana zostanie wartość k = 1. Dla 100 000 powtórzeń zostaje zliczona liczba iteracji j. Wektor ten wykorzystany został do policzenia p-wartości w teście chi-kwadrat.

Przykładowy rozkład przedstawiono poniżej:



Dla wygenerowanych 4 rozkładów empirycznych (tylko 4 ze względu na dużą ilość potrzebnych danych) wykonano test dopasowania Kołmogorowa-Smirnowa w odniesieniu do rozkładu równomiernego, z każdego porównania uzyskując wartość p. Dla 4 wartości p uzyskano rozkład empiryczny został przedstawiony poniżej:



Weryfikacja zgodności dopasowania do rozkładu równomiernego za pomocą testu Kołmogorowa-Smirnowa wykazała $p =$ 0.4924, a więc wartość prawdopodobną mieszczącą się w zakresie $p < 0{,}025$ lub $p > 0{,}975$.

Uwagi:

1. Powtarzając kolejne iteracje w testach Count the Ones Test oraz Squeeze Test, aby uzyskać kilka bądź kilkanaście p-wartości potrzebujemy dużej ilości wygenerowanych danych co łączy się z długim czasem oczekiwania zarówno na wczytanie danych jak i dalsze wykonanywane operacje na nich.
2. Kod programu i potrzebne pliki dostępne są pod linkiem: https://github.com/skrb7/Bezpieczenstwo-Systemow-Teleinformatycznych/Diehard_tests