**RAPORT Z PODPISU CYFROWEGO NA PRZEDMIOT „BEZPIECZEŃSTWO SYSTEMÓW TELEINFORMATYCZNYCH”**

1. **Imię i nazwisko:**

* Michał Kuniczuk – 151972

1. **Link do repozytorium:**

* <https://github.com/goudzior/TRNG>

1. **Opis działania:**

* Kod wykorzystuje czas podróży pakietu HTTP GET. Pakiety są timestampowane w procesorze. Wysyłamy go więc do losowego serwera i oczekujemy na odpowiedź. Na tej podstawie obliczany jest czas podróży w nanosekundach. To źródło entropii jest następnie XORowane z generatorem liczb pseudolosowych i w ten sposób otrzymujemy nasze liczby losowe. Te wygenerowane liczby są następnie wykorzystywane to znalezienia współczynników p i q w algorytmie RSA. Pierwszy test koduje i rozkodowuje hash wiadomości, aby sprawdzić poprawność programu, drugi testuje niezbywalność klucza przez generacje drugiej pary i próbę rozszyfrowania hashu. Trzeci test natomiast bada integralność wiadomości poprzez porównanie skrótów dwóch różnych wiadomości po ich rozszyfrowaniu.