<table>
<tr><td colspan="2"> 
POLITECHNIKA POZNAŃSKA</td><td colspan="2"> 
WYDZIAŁ INFORMATYKI
I TELEKOMUNIKACJI</td></tr>
<tr><td>Wykonujący:
Mateusz Irski
Paweł Szczeszek
Bartosz Gabruk</td><td>Kierunek
Teleinformatyka</td><td colspan="2">Systemy szyfrowania i certyfikacji</td></tr>
<tr><td colspan="4">Temat ćwiczenia laboratoryjnego:
Tryb CTR</td></tr>
<tr><td>Numer ćwiczenia
4</td><td>Data wykonania ćwiczenia
08.04.2026</td><td>Grupa
LAB2</td><td>Prowadzący
mgr inż. Paweł Kubczak</td></tr>
</table>

Założenia: 100 podciągów po 1 000 000 bitów. Poziom istotności α = 0.01. Test uznano za spełniony, gdy **P-value >= 0.01** oraz **R >= 96/100**.

1. Wyniki testów statystycznych przeprowadzonych na ciągu zer

Test	P-value	R	Spełniony
Frequency	0.000000	0/100	NIE
Block Frequency	0.000000	0/100	NIE
Cumulative Sums (śr.)	0.000000	0/100	NIE
Runs	0.000000	0/100	NIE
Longest Run	0.000000	0/100	NIE
Rank	0.000000	0/100	NIE
FFT	0.000000	0/100	NIE
NonOverlapping Template (śr.)	0.000000	0/100	NIE
Overlapping Template	0.000000	0/100	NIE
Universal	0.000000	0/100	NIE
Approximate Entropy	0.000000	0/100	NIE
Serial (śr.)	0.000000	0/100	NIE
Linear Complexity	0.000000	0/100	NIE

2. Wyniki testów statystycznych dla ciągu zaszyfrowanego 3DES w trybie ECB i CTR

2.1 3DES ECB

Test	P-value	R	Spełniony
Frequency	0.000000	0/100	NIE
Block Frequency	0.000000	0/100	NIE
Cumulative Sums (śr.)	0.000000	0/100	NIE
Runs	0.000000	0/100	NIE
Longest Run	0.000000	0/100	NIE
Rank	0.000000	0/100	NIE
FFT	0.000000	0/100	NIE
NonOverlapping Template (śr.)	0.000000	0/100	NIE
Overlapping Template	0.000000	0/100	NIE
Universal	0.000000	0/100	NIE
Approximate Entropy	0.000000	0/100	NIE
Serial (śr.)	0.000000	0/100	NIE
Linear Complexity	0.000000	0/100	NIE

2.2 3DES CTR

Test	P-value	R	Spełniony
Frequency	0.534146	100/100	TAK
Block Frequency	0.236810	100/100	TAK
Cumulative Sums (śr.)	0.328473	100/100	TAK
Runs	0.040108	98/100	TAK
Longest Run	0.401199	99/100	TAK
Rank	0.983453	100/100	TAK
FFT	0.137282	100/100	TAK
NonOverlapping Template (śr.)	0.508072	99/100	TAK
Overlapping Template	0.534146	100/100	TAK
Universal	0.350485	97/100	TAK
Approximate Entropy	0.616305	98/100	TAK
Serial (śr.)	0.158185	100/100	TAK
Linear Complexity	0.699313	100/100	TAK

3. Wyniki testów statystycznych dla ciągu zaszyfrowanego AES w trybie ECB i CTR

3.1 AES ECB

Test	P-value	R	Spełniony
Frequency	0.000000	0/100	NIE
Block Frequency	0.000000	100/100	NIE
Cumulative Sums (śr.)	0.000000	0/100	NIE
Runs	0.000000	0/100	NIE
Longest Run	0.000000	0/100	NIE
Rank	0.000000	0/100	NIE
FFT	0.000000	0/100	NIE
NonOverlapping Template (śr.)	0.000000	0/100	NIE
Overlapping Template	0.000000	0/100	NIE
Universal	0.000000	0/100	NIE
Approximate Entropy	0.000000	0/100	NIE
Serial (śr.)	0.000000	0/100	NIE
Linear Complexity	0.000000	0/100	NIE

3.2 AES CTR

Test	P-value	R	Spełniony
Frequency	0.554420	99/100	TAK
Block Frequency	0.419021	100/100	TAK
Cumulative Sums (śr.)	0.288477	98/100	TAK
Runs	0.494392	99/100	TAK
Longest Run	0.867692	99/100	TAK
Rank	0.011791	99/100	TAK
FFT	0.102526	99/100	TAK
NonOverlapping Template (śr.)	0.487074	99/100	TAK
Overlapping Template	0.037566	98/100	TAK
Universal	0.534146	100/100	TAK
Approximate Entropy	0.350485	100/100	TAK
Serial (śr.)	0.881217	100/100	TAK

4. Zwięzły opis działania trybu CTR dla szyfrów blokowych

W trybie CTR szyfr blokowy nie szyfruje bezpośrednio kolejnych bloków danych wejściowych. Najpierw szyfrowana jest wartość licznika, zwykle złożona z nonce i inkrementowanego numeru bloku. Otrzymany blok wyjściowy tworzy strumień klucza, który jest następnie łączony z danymi operacją XOR. Dzięki temu identyczne bloki danych nie prowadzą do identycznych bloków szyfrogramu, o ile licznik ma różne wartości. Tryb CTR działa więc podobnie do szyfru strumieniowego i zwykle daje wyniki o znacznie lepszych własnościach statystycznych niż ECB.

5. Podsumowanie i wnioski

- Ciąg złożony z samych zer nie spełnia testów NIST - uzyskane P-value są równe 0.000000, a proporcja R wynosi 0/100.
- Szyfrowanie w trybie ECB nie maskuje powtarzalnej struktury danych wejściowych. Dla 3DES ECB oraz AES ECB wyniki pozostają nielosowe i praktycznie wszystkie testy są niespełnione. W AES ECB test Block Frequency ma R = 100/100, ale nadal nie jest spełniony, ponieważ P-value = 0.000000.
- Szyfrowanie w trybie CTR istotnie poprawia własności statystyczne szyfrogramu. Zarówno dla 3DES CTR, jak i AES CTR wszystkie zestawione testy spełniają kryteria P-value i proporcji R.
- Wniosek praktyczny jest taki, że o jakości statystycznej wyniku decyduje nie tylko sam algorytm blokowy, ale również tryb pracy. Dla danych silnie regularnych tryb CTR eliminuje widoczne wzorce znacznie skuteczniej niż ECB.