

POLITECHNIKA ŚWIĘTOKRZYSKA

Wydział Elektrotechniki, Automatyki i Informatyki

Maksymilian Sowula

Paweł Marek

Jakub Szczur

Daniel Cieślak

Numer grupy dziekańskiej: 1ID21A

Kryptografia

Złożone Struktury Danych

1. Wprowadzenie do kryptografii

1.1. Historia i rozwój

1.2. Podstawowe pojęcia

1.3. Podstawowe cele

1.4. Klasyfikacja algorytmów kryptograficznych

1.4.1. Kryptografia klasyczna

1.4.2. Kryptografia symetryczna

1.4.3. Kryptografia asymetryczna

1.5. Zastosowania

2. Klasyczne metody szyfrowania

2.1. Szyfr Cezara

2.2. Szyfr Vigenère'a

3. Kryptografia symetryczna

3.1. Algorytm DES

3.2. Algorytm AES

4. Kryptografia asymetryczna

4.1. Algorytm RSA

5. Implementacja i pomiary wydajności

5.1. Środowisko testowe

Macbook Pro M3 Pro – 18 GB RAM, 12 rdzeni CPU (5 wydajnościowych + 6 efektywnych)

5.2. Najważniejsze fragmenty kodu

5.3. Wyniki pomiarów

6. Wnioski