Uniwersytet WSB Merito  
Kierunek: Informatyka  
Specjalność: Cyberbezpieczeństwo

Rok akademicki: 2024/2025  
semestr letni

**Analiza działania szyfru asymetrycznego RSA z wykorzystaniem narzędzia CrypTool**

Wykonał: Maciej Niemiec

Numer albumu: 107162



# **Wprowadzenie**

Kryptografia jest podstawowym mechanizmem ochrony informacji, **realizującym trzy kluczowe cele: poufność, integralność i autentyczność danych.** Podczas wykładu prowadzący wyróżnił pięć grup technik kryptograficznych, z których każda odpowiada za inny aspekt bezpieczeństwa:

* Szyfrowanie symetryczne - ten sam tajny klucz jest używany do szyfrowania i deszyfrowania wiadomości, gwarantując poufność.
* Szyfrowanie asymetryczne - para kluczy (publiczny i prywatny) pozwala na rozdzielenie funkcji szyfrowania i deszyfrowania; przykładem jest algorytm RSA, którego działanie jest analizowane w tym raporcie.
* Kody uwierzytelniania wiadomości (MAC) - skrót dołączony do przesyłanych danych wraz z tajnym kluczem pozwala jednocześnie potwierdzić ich integralność i pochodzenie.
* Jednokierunkowe funkcje skrótu - obliczają skróty o stałej długości, które są łatwe do określenia, a jednocześnie odporne na rekonstrukcję danych wejściowych i kolizje; typowe rodziny to SHA-1, SHA-2 i SHA-3.
* Podpis cyfrowy - wykorzystujący szyfrowanie asymetryczne i właściwości skrótów, zapewnia integralność, autentyczność i niezaprzeczalność komunikacji.

**W kontekście sprawozdania kluczowy jest drugi punkt: szyfrowanie asymetryczne.** RSA, opierając się na trudności faktoryzacji dużych liczb pierwszych, umożliwia publiczne udostępnienie klucza szyfrowania, przy jednoczesnym zachowaniu klucza deszyfrowania w tajemnicy. Sprawia to, że algorytm ten jest szeroko stosowany nie tylko do samego szyfrowania, ale także do rzeczywistego szyfrowania.

# **Część Laboratoryjna**

## **Zadanie 1. Proszę zapoznać sią z demonstracją algorytmu RSA**

Obraz zawierający tekst, zrzut ekranu, Czcionka, numer

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.

Rysunek 1 - Aplikacja demonstracyjna algorytmu RSA z wyborem liczb p i q, obliczonymi parametrami klucza (N, φ(N), e, d) oraz przykładowym procesem szyfrowania wiadomości.

## **Zadanie 2. Proszę wygenerować klucze kryptograficzne (512 / 1024 / 2048)**

Obraz zawierający tekst, zrzut ekranu, wyświetlacz, numer

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.

Rysunek 2 - Okno aplikacji wyświetlające dostępne pary kluczy asymetrycznych – trzy klucze RSA (512, 1024, 2048 bity) wraz z metadanymi i opcjami zarządzania.

## **Zadanie 3. Dla różnych długości klucza (512, 1024, 2048) zmierzyć i porównać czas szyfrowania i deszyfrowania plików o różnych rozmiarach (np. 1MB, 2MB, 5MB)**

Tabela 1 - Porównanie czasu szyfrowania

|  |  |  |  |
| --- | --- | --- | --- |
| Algorytm | Czas szyfrowania 1MB w sekundach | Czas szyfrowania 2MB w sekundach | Czas szyfrowania 5MB w sekundach |
| RSA (512bit) | 0.171 | 0.355 | 0.872 |
| RSA (1024bit) | 0.330 | 0.650 | 1.621 |
| RSA (2048bit) | 0.562 | 1.180 | 2.956 |

Tabela 2 - Porównanie czasu deszyfrowania

|  |  |  |  |
| --- | --- | --- | --- |
| Algorytm | Czas deszyfrowania 1MB w sekundach | Czas deszyfrowania 2MB w sekundach | Czas deszyfrowania 5MB w sekundach |
| RSA (512bit) | 2.513 | 4.746 | 11.849 |
| RSA (1024bit) | 7.437 | 14.619 | 36.801 |
| RSA (2048bit) | 25.478 | 49.515 | 125.427 |

Obraz zawierający tekst, zrzut ekranu, numer, oprogramowanie

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.

Rysunek 3 - Wynik szyfrowania pliku 5 MB algorytmem RSA w CrypTool – podgląd heksadecymalny danych oraz komunikat z czasem szyfrowania

Obraz zawierający tekst, oprogramowanie, numer, Oprogramowanie multimedialne

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.

Rysunek 4 - Wynik szyfrowania pliku 5 MB algorytmem RSA w CrypTool – podgląd heksadecymalny danych oraz komunikat z czasem szyfrowania

Obraz zawierający tekst, zrzut ekranu, oprogramowanie, numer

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.

Rysunek 5 - Wynik szyfrowania pliku 5 MB algorytmem RSA w CrypTool – podgląd heksadecymalny danych oraz komunikat z czasem szyfrowania

Obraz zawierający tekst, elektronika, zrzut ekranu, oprogramowanie

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.

Rysunek 6 - Wynik deszyfrowania pliku 5 MB algorytmem RSA w CrypTool – podgląd heksadecymalny danych oraz komunikat z czasem deszyfrowania

Obraz zawierający tekst, elektronika, zrzut ekranu, oprogramowanie

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.

Rysunek 7 - Wynik deszyfrowania pliku 5 MB algorytmem RSA w CrypTool – podgląd heksadecymalny danych oraz komunikat z czasem deszyfrowania

Obraz zawierający tekst, elektronika, zrzut ekranu, oprogramowanie

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.

Rysunek 8 - Wynik deszyfrowania pliku 5 MB algorytmem RSA w CrypTool – podgląd heksadecymalny danych oraz komunikat z czasem deszyfrowania

Obraz zawierający tekst, zrzut ekranu, oprogramowanie, numer

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.

Rysunek 9 - Wynik szyfrowania pliku 2 MB algorytmem RSA w CrypTool – podgląd heksadecymalny danych oraz komunikat z czasem szyfrowania

Obraz zawierający tekst, oprogramowanie, numer, Oprogramowanie multimedialne

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.

Rysunek 10 - Wynik szyfrowania pliku 2 MB algorytmem RSA w CrypTool – podgląd heksadecymalny danych oraz komunikat z czasem szyfrowania

Obraz zawierający tekst, zrzut ekranu, numer, oprogramowanie

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.

Rysunek 11 - Wynik szyfrowania pliku 2 MB algorytmem RSA w CrypTool – podgląd heksadecymalny danych oraz komunikat z czasem szyfrowania

Obraz zawierający tekst, zrzut ekranu, oprogramowanie, numer

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.

Rysunek 12 – Wynik deszyfrowania pliku 2 MB algorytmem RSA w CrypTool – podgląd heksadecymalny danych oraz komunikat z czasem deszyfrowania

Obraz zawierający tekst, zrzut ekranu, oprogramowanie, wyświetlacz

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.

Rysunek 13 – Wynik deszyfrowania pliku 2 MB algorytmem RSA w CrypTool – podgląd heksadecymalny danych oraz komunikat z czasem deszyfrowania

Obraz zawierający tekst, elektronika, zrzut ekranu, wyświetlacz

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.

Rysunek 14 – Wynik deszyfrowania pliku 2 MB algorytmem RSA w CrypTool – podgląd heksadecymalny danych oraz komunikat z czasem deszyfrowania

Obraz zawierający tekst, numer, oprogramowanie, zrzut ekranu

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.

Rysunek 15 – Wynik szyfrowania pliku 1 MB algorytmem RSA w CrypTool – podgląd heksadecymalny danych oraz komunikat z czasem szyfrowania

Obraz zawierający tekst, zrzut ekranu, oprogramowanie, numer

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.

Rysunek 16 – Wynik szyfrowania pliku 1 MB algorytmem RSA w CrypTool – podgląd heksadecymalny danych oraz komunikat z czasem szyfrowania

Obraz zawierający tekst, numer, oprogramowanie, Czcionka

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.

Rysunek 17 – Wynik szyfrowania pliku 1 MB algorytmem RSA w CrypTool – podgląd heksadecymalny danych oraz komunikat z czasem szyfrowania

Obraz zawierający tekst, zrzut ekranu, oprogramowanie, wyświetlacz

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.

Rysunek 18 – Wynik deszyfrowania pliku 1 MB algorytmem RSA w CrypTool – podgląd heksadecymalny danych oraz komunikat z czasem deszyfrowania

Obraz zawierający tekst, zrzut ekranu, oprogramowanie, wyświetlacz

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.

Rysunek 19 – Wynik deszyfrowania pliku 1 MB algorytmem RSA w CrypTool – podgląd heksadecymalny danych oraz komunikat z czasem deszyfrowania

Obraz zawierający tekst, zrzut ekranu, wyświetlacz, oprogramowanie

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.

Rysunek 20 – Wynik deszyfrowania pliku 1 MB algorytmem RSA w CrypTool – podgląd heksadecymalny danych oraz komunikat z czasem deszyfrowania

## **Zadanie 4. Porównać działanie algorytmów asymetrycznych z algorytmem symetrycznym**

Obraz zawierający tekst, zrzut ekranu, Czcionka

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.

Rysunek 21 - Poniższa infografika zestawia kluczowe różnice między algorytmami AES (symetryczny) i RSA (asymetryczny) w oparciu o artykuł [GeeksforGeeks](https://www.geeksforgeeks.org/difference-between-aes-and-rsa-encryption/).

**Najważniejsze punkty:**

* **Rodzaj szyfrowania:** AES używa jednego klucza (symetryczny), RSA pary kluczy publiczny/prywatny (asymetryczny)
* **Długości kluczy:** AES 128/192/256 bitów kontra RSA 1024/2048/4096 bitów
* **Wydajność:** AES jest znacznie szybszy i nadaje się do szyfrowania dużych zbiorów danych, RSA jest wolniejszy
* **Zastosowania:** AES – szyfrowanie plików i kanałów, RSA – wymiana kluczy, podpisy cyfrowe
* **Dystrybucja kluczy:** AES wymaga bezpiecznego przekazania tajnego klucza, RSA udostępnia jedynie klucz publiczny

## **Zadanie 5. Do kryptogramów utworzonych w zadaniu 3 dla różnych kluczy wprowadzić następujące zmiany:**

### **Zmienić wartość 1 bajtu,**

### **Usunąć 1 bajt,**

### **Usunąć kilka bajtów**

### **Usunąć fragment długości (512, 1024, 2048)**

# **Analiza Wyników**

## **Pytanie 1. Jak zmieniają się obserwowane parametry?**

## **Pytanie 2. W jaki sposób można wykorzystać narzędzia analizy tekstu dostępne w CrypTool do określenia algorytmu szyfrowania dla danego zaszyfrowanego tekstu?**

## **Pytanie 3. W jaki sposób można wykorzystać narzędzia analizy tekstu dostępne w programie CryptTool do ustalenia hasła używanego do szyfrowania?**

# **Podsumowanie**