

**WYDZIAŁ ELEKTROTECHNIKI, AUTOMATYKI,  
INFORMATYKI I INŻYNIERII BIOMEDYCZNEJ**

KATEDRA AUTOMATYKI I ROBOTYKI

Praca dyplomowa magisterska

*Porównanie i implementacja zaawansowanych szyfrów blokowych*

*Comparison and implementation of advanced block ciphers*

Autor: *Jarosław Jałocha*

Kierunek studiów: Automatyka i Robotyka

Opiekun pracy: Prof. *dr. Inż. Marek Ogiela*

Kraków, 2019

*Uprzedzony o odpowiedzialności karnej na podstawie art. 115 ust. 1 i 2 ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (t.j. Dz.U. z 2006 r. Nr 90, poz. 631   
z późn. zm.): „ Kto przywłaszcza sobie autorstwo albo wprowadza w błąd co do autorstwa całości lub części cudzego utworu albo artystycznego wykonania, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 3. Tej samej karze podlega, kto rozpowszechnia bez podania nazwiska lub pseudonimu twórcy cudzy utwór w wersji oryginalnej albo w postaci opracowania, artystyczne wykonanie albo publicznie zniekształca taki utwór, artystyczne wykonanie, fonogram, wideogram lub nadanie.”, a także uprzedzony o odpowiedzialności dyscyplinarnej na podstawie art. 211 ust. 1 ustawy z dnia 27 lipca 2005 r. Prawo o szkolnictwie wyższym (t.j. Dz. U. z 2012 r. poz. 572, z późn. zm.) „Za naruszenie przepisów obowiązujących w uczelni oraz za czyny uchybiające godności studenta student ponosi odpowiedzialność dyscyplinarną przed komisją dyscyplinarną albo przed sądem koleżeńskim samorządu studenckiego, zwanym dalej „sądem koleżeńskim”, oświadczam, że niniejszą pracę dyplomową wykonałem osobiście i samodzielnie i że nie korzystałem ze źródeł innych niż wymienione w pracy.*

*<podpis dyplomanta>*

Spis treści

[1. Wstęp 2](#_Toc3065907)

[2. Szyfry blokowe 4](#_Toc3065908)

[3. DES 4](#_Toc3065909)

[4. AES 4](#_Toc3065910)

[5. RC6 4](#_Toc3065911)

[6. Opis zaimplementowanego programu 4](#_Toc3065912)

[7. Przeprowadzone badania 4](#_Toc3065913)

[8. Wnioski 4](#_Toc3065914)

[Bibliografia 4](#_Toc3065915)

# Wstęp

Utajnianie informacji nie jest niczym nowym. Od zarania dziejów dbano, żeby wiadomości nie trafiały w niepowołane ręce, gdyż mogło by się to skończyć katastrofą. W tym celu zaczęto stosować szyfry zmieniające początkowy tekst wiadomości na postać całkowicie niezrozumiałą dla niepowołanej osoby. Oczywiście, przekształcenie było znane dla docelowego adresata, zatem mógł odwrócić transformację i odczytać ukryty sens przekazu. Działania te dały początek dziedzinie nauki zwanej **kryptologią** [Bruce Schneier]. Wyróżnia się w niej dwie odrębne gałęzie:

* kryptografię (gałąź badająca sposoby utajniania wiadomości),
* kryptoanalizę (gałąź przełamywania szyfru nie posiadając o nim pełnej wiedzy, np. nie znając klucza tudzież szczegółów implementacji).

Jak już wspomniano, szyfrowanie używane już było w czasach starożytnych. Ze względu na oczywiste ograniczenia technologiczne stosowano proste szyfry: przestawieniowe (sztandarowym przypadkiem jest tutaj szyfr Cezara), podstawieniowe lub permutacyjne. Składały się one zazwyczaj z jednej operacji i były dość proste do złamania, nawet w owych, zamierzchłych czasach.

Rozwój techniki zwiększył możliwości algorytmów kryptograficznych. Zaczęto tworzyć maszyny szyfrujące o skomplikowanych strukturach, w wyniku działania których powstawał szyfrogram w ogóle nieprzypominający początkowej wiadomości, a zlepek losowych znaków (co jest jednym z aksjomatów skutecznego szyfrowania). Kluczową własnością takich urządzeń był ukryty algorytm szyfrujący, zatem głównym celem kryptoanalityków było poznanie sposobu tworzenia szyfru i odwrócenie go, żeby uzyskać pierwotną wiadomość. Przykładem takiej maszyny jest niemiecka Enigma stosowana szeroko w czasie II Wojny Światowej. Jak pokazała historia tworzenie skomplikowanych algorytmów jest z punktu widzenia bezpieczeństwa nieefektywne, gdyż przechwycenie maszyny prędzej czy później zakończy się złamaniem algorytmu.

Wraz z pojawieniem się komputerów oraz niedoskonałością rozwiązań mechanicznych zdecydowano się zmienić podejście. Stwierdzono, że szyfrowanie powinno odbywać się w zgodzie z tzw. **Zasadą Kerckhoffsa** [Stinson], która mówi, że dobry system kryptograficzny powinien pozostać bezpieczny nawet wtedy, kiedy szczegóły jego działania (w szczególności przeprowadzone operacje szyfrujące) są znane. Jedyną nieznaną, z punktu widzenia atakującego, informacją powinien być tzw. **klucz**, czyli sekretna wartość niezależna od treści wiadomości, która zostaje użyta w procesie szyfrowania oraz deszyfrowania. Ze względu na sposób użycia klucza wyróżnia się szyfry [Aumasson]:

* symetryczne – klucz używany do szyfrowania i deszyfrowania jest jednakowy (tajny),
* asymetryczne – klucz używany do szyfrowania jest znany (tzw. klucz publiczny), jest on różny od klucza używanego do odszyfrowania wiadomości (tzw. klucz prywatny, który pozostaje tajny).

Szyfry dzielą się również ze względu na sposób kodowania informacji. Do podziału tego włączają się m.in.:

* szyfry blokowe – w jednej iteracji utajniona zostaje z góry określona grupa bitów zwana blokiem,
* szyfry strumieniowe – utajniony zostaje każdy bit z osobna.

W pracy oraz programie komputerowym z nią związanym znajdzie się studium nad szyframi należącymi do grupy **symetrycznych szyfrów blokowych**. Przyszłe rozdziały dotyczyć będą krótkiego, ogólnego wprowadzenia do szyfrów blokowych, następnie przybliżone zostaną szczegóły implementacyjne każdego z zaimplementowanych szyfrów. Kolejny rozdział będzie dotyczył opisu stworzonego programu komputerowego, który pozwoli użyć każdego z opisanych algorytmów do zaszyfrowania określonego pliku oraz umożliwi przeprowadzenie badań na temat szybkości algorytmów. Ich opis zostanie zawarty w rozdziale 7., dzięki którym wysnute zostaną wnioski opisane w kolejnym rozdziale.

# Szyfry blokowe

# DES

# AES

# RC6

# Opis zaimplementowanego programu

# Przeprowadzone badania

# Wnioski

# Bibliografia

Bruce Schneier: *Kryptografia dla praktyków: protokoły, algorytmy i programy źródłowe w języku C*. Warszawa: Wydawnictwa Naukowo-Techniczne, 2002, s. 27–28. [ISBN 83-204-2678-2](https://pl.wikipedia.org/wiki/Specjalna:Ksi%C4%85%C5%BCki/8320426782).

Stinson

Aumasson