

**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](#_Toc3819483)

[2. Szyfry blokowe 4](#_Toc3819484)

[3. DES 4](#_Toc3819485)

[4. AES 4](#_Toc3819486)

[5. RC6 4](#_Toc3819487)

[6. Opis zaimplementowanego programu 4](#_Toc3819488)

[7. Przeprowadzone badania 4](#_Toc3819489)

[8. Wnioski 5](#_Toc3819490)

[Literatura 5](#_Toc3819491)

# Wstęp

Utajnianie informacji nie jest czymś, co zostało wynalezione w ostatnich latach, a nawet biorąc pod uwagę okres stuletni 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** [11], 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 [1]:

* 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

Poprzedni rozdział zawierał intuicyjną, aczkolwiek nieformalną definicję szyfru oraz związanym z nim pojęć. W niniejszym rozdziale zostanie zawarta formalizacja pewnych podstawowych pojęć związanych z kryptografią, a także przedstawiony zostanie zarys działania szyfrów blokowym, będący wstępem do opisu poszczególnych rodzajów implementacji danego systemu.

Każdy system kryptograficzny związany jest z następującą piątką elementów [3]:

* przestrzenią wiadomości jawnych M,
* przestrzenią szyfrogramów C,
* przestrzenią kluczy K,
* rodziną funkcji szyfrujących takich, że: ,
* rodziną funkcji deszyfrujących takich, że: .

Szyfrem potocznie nazywa się konkretnego przedstawiciela rodziny . Zachodzi również bardzo istotna własność między odpowiadającymi sobie funkcjami z rodziny oraz . Stanowi ona następująco (2.1):



Warunek (2.1) mówi, iż jeżeli do zaszyfrowania wiadomości użyto funkcji , to zastosowanie funkcji do odszyfrowania kryptogramu spowoduje uzyskanie pierwotnego tekstu jawnego.

Oczywistym jest również fakt, iż funkcje z rodzin i muszą być różnowartościowe, w przeciwnym razie niemożliwym byłoby jednoznaczne. Bardziej złożone, ogólne rozważania matematyczne nad strukturą funkcji szyfrujących oraz deszyfrujących można znaleźć w [11].

Zgodnie z zasadą Kerckhoffsa, największą „zaporą” stojącą na drodze przechwycenia oryginalnej wiadomości jest klucz szyfrowania. Pierwszym, oczywistym zagrożeniem z tego wynikającym jest fakt, iż zarówno nadawca, jak i odbiorca muszą posiadać tę samą wartość klucza, zatem konieczne jest przekazanie jego wartości. Jednym z rozwiązań jest zaszyfrowanie klucza innym algorytmem i przesłanie go w postaci szyfrogramu. Jest to rozwiązanie prowadzące do nieskończonej rekurencji, albowiem kolejny algorytm również korzysta z kluczy, który należy przekazać, najlepiej poprzez następny szyfrowany kanał. Efektem tego jest konieczność jawnego przekazania klucza, która odbywa się poprzez tzw. kanał bezpieczny [1].

Kolejnym aspektem dotyczącym klucza jest jego postać. Funkcje szyfrujące dążą do tego, ażeby szyfrogramy miały postać całkowicie losową, a korelacja poszczególnych znaków była jak najmniejsza. W związku z tym, wartość klucza powinna być inicjalizowana losowo. Bardzo poważnym błędem w formowaniu klucza jest użycie wbudowanego generatora liczb losowych bez upewnienia się, że jest on przystosowany do zastosowań kryptograficznych. Wyróżniamy generatory RNG (ang. *Random Number Generator,* generator liczb losowych), który korzystając z danych wejściowych (pomiar temperatury, częstotliwość kliknięć myszką itp.) generuje losowe liczby. Jest on przystosowany kryptograficznie, jako że trudno przewidzieć liczbę przezeń wygenerowaną, aczkolwiek jest to proces stosunkowo wolny oraz podatny na manipulację (poprzez wymuszanie pewnych zachowań czujników). Drugim rodzajem generatorów są generatory PRNG (ang. *Pseudo Random Number Generator*, generator liczb pseudolosowych). Szczególnie ten typ generatorów może być podatny na atak poprzez nieprzystosowanie do zadań kryptograficznych, albowiem korzysta on z tzw. ziarna. Znając wartość ziarna (w generatorach niekryptograficznych) możliwym jest przewidzenie ciągu wygenerowanych liczb, co ewidentnie pozbawia algorytm szyfrujący jakiegokolwiek bezpieczeństwa. Należy więc się upewnić, że używa się właściwego generatora [1].

# DES

# AES

# RC6

# Opis zaimplementowanego programu

# Przeprowadzone badania

# Wnioski

# Literatura

1. Aumasson J. P.: *Nowoczesna kryptografia. Praktyczne wprowadzenie do szyfrowania.*Warszawa: Wydawnictwo Naukowe PWN SA, 2018, s. 1-59. ISBN 978-83-01-19900-5.
2. Bhat B., Ali A. W., Gupta A.: *DES and AES performance evaluation.*  
   Noida: International Conference on Computing, Communication & Automation, 2015, s. 887-890.  
   doi: 10.1109/CCAA.2015.7148500
3. Cheng H., Ding Q.: *Overview of the Block Cipher*.   
   Harbin: 2012 Second International Conference on Instrumentation, Measurement, Computer, Communication and Control, 2012, s. 1628-1631. *doi: 10.1109/IMCCC.2012.379*
4. Floissac N., L'Hyver Y.: *From AES-128 to AES-192 and AES-256, How to Adapt Differential Fault Analysis Attacks on Key Expansion   
   Nara:* 2011 Workshop on Fault Diagnosis and Tolerance in Cryptography, 2011, s. 43-53.  
   doi: 10.1109/FDTC.2011.15
5. Kalaiselvi K., Kumar A.: *Enhanced AES cryptosystem by using genetic algorithm and neural network in S‑box*.  
   Banglore: 2016 IEEE International Conference on Current Trends in Advanced Computing (ICCTAC), 2006, s. 1-6. doi: 10.1109/ICCTAC.2016.7567340
6. Liu N., et al.: *Cryptographic performance for Rijndael and RC6 block ciphers*.   
   Xiamen: 2017 11th IEEE International Conference on Anti-counterfeiting, Security, and Identification (ASID)*,* 2017, s. 36-39. doi: 10.1109/ICASID.2017.8285739
7. Mohamed A. B., Zaibi G., Kachouri A.: *Implementation of RC5 and RC6 block ciphers on digital images.*Sousse: Eighth International Multi-Conference on Systems, Signals & Devices*,* 2011,   
   s. 1-6.  
   doi: 10.1109/SSD.2011.5767447
8. Noura M. et al.: *S-DES: An efficient & secure DES variant.*   
   Jounieh: 2018 IEEE Middle East and North Africa Communications Conference (MENACOMM)*,* 2018, s. 1-6. doi: 10.1109/MENACOMM.2018.8371019
9. Sanchez-Avila C., Sanchez-Reillol R.: *The Rijndael block cipher (AES proposal): a comparison with DES.*Londyn: Proceedings IEEE 35th Annual 2001 International Carnahan Conference on Security Technology (Cat. No.01CH37186), 2001, s. 229-234. doi: 10.1109/CCST.2001.962837
10. Schneier B.: *Kryptografia dla praktyków: protokoły, algorytmy i programy źródłowe w języku C*. Warszawa: Wydawnictwa Naukowo-Techniczne, 2002 [ISBN 83-204-2678-2](https://pl.wikipedia.org/wiki/Specjalna:Ksi%C4%85%C5%BCki/8320426782).
11. Stinson D. R.: *Kryptografia. W teorii i praktyce.*Warszawa: Wydawnictwo Naukowo-Techniczne, 2005. ISBN 83-204-2982-X