

**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](#_Toc5041947)

[2. Szyfry blokowe 4](#_Toc5041948)

[3. DES 12](#_Toc5041949)

[4. AES 12](#_Toc5041950)

[5. RC6 18](#_Toc5041951)

[6. Opis zaimplementowanego programu 18](#_Toc5041952)

[7. Przeprowadzone badania 18](#_Toc5041953)

[8. Wnioski 18](#_Toc5041954)

[Literatura 18](#_Toc5041955)

# 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** [12], 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 powiązanie szyfrogramu z wiadomością. Bardziej złożone, ogólne rozważania matematyczne nad strukturą funkcji szyfrujących oraz deszyfrujących można znaleźć w [12].

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].

Równie ważną właściwością klucza jest jego długość. Odpowiednia liczba bajtów zapewnia zarówno dużą różnorodność wartości, co pozwala na częste zmiany, ale również uodparnia na tzw. ataki brute-force. Jest to sposób, w którym wykonuje się przeszukiwanie zupełne przestrzeni kluczy aż do momentu, w którym z szyfrogramu uzyskuje się zrozumiałą wiadomość. Wydawać by się mogło, że taki atak jest trudny w wykonaniu, aczkolwiek jak udowodniono w dziele [14], złamanie 6-znakowego hasła metodą przeszukiwania zupełnego kończy się sukcesem po około sekundzie (przy użyciu zaawansowanego układu GPU zrównoleglającego czynności). Klucze szyfrów używanych w przeszłości nierzadko miało porównywalną długość w skali bajtów (np. klucz szyfru DES ma 7 bajtów), co uwydatnia fakt, iż wraz ze wzrastającą mocą obliczeniową, powinna rosnąć również wielkość klucza.

Liczba operacji wymaganych do wyszukania klucza i zweryfikowania jego poprawności rośnie niemal eksponencjalnie wraz ze wzrostem jego wielkości, zatem w obecnych czasach stosuje się klucze o wielkości 16 bajtów [1], jednak liczba ta jest zależna od implementacji. Należy również wspomnieć, że odpowiednia długość klucza nie zapewnia całkowitego bezpieczeństwa (zwłaszcza przy błędnej implementacji algorytmu lub złych założeniach). Co więcej, bezpieczeństwo obecnie stosowanych szyfrów nie jest absolutne, albowiem nie znaleziono dotąd sposobu na udowodnienie owego [1]. Przyjmuję się zatem dowód heurystyczny, tj. fakt, iż nikomu nie udało się złamać danego systemu, pomimo wielu przeprowadzonych prób, czyni szyfr akceptowalnym do użytku.

Systemami kryptograficznymi, nad którymi będą prowadzone rozważania w niniejszej pracy są szyfry blokowe. Jak już wspomniano wcześniej, jest to rodzaj symetrycznych szyfrów, w którym przetwarzane są bloki danych. Sama wielkość bloku zależy od implementacji, może to być 8 bajtów jak w algorytmie DES czy też 16 jak w przypadku algorytmu AES [10]. Nie powinny być one jednak za duże (ze względu na oszczędność pamięci), ale również zbyt małe, gdyż spowodowało by to podatność na atak tzw. książki kodowej, czyli stworzenia tabel, które przypisywałyby konkretny blok danych danemu szyfrogramowi – przy większych blokach taka operacja wymaga zbyt dużo nakładu obliczeniowo/pamięciowego, zatem zwyczajowo uznaje się 64 bity za minimum [1]. Nie istnieje „złoty środek” w kwestii kreacji szyfrów blokowych, jednak główną ideą jest stworzenie algorytmu, w którym powtarza się określone bloki instrukcji. Jeden blok instrukcji zwany jest **rundą**, która sama w sobie nie zapewnia bezpieczeństwa szyfru, aczkolwiek powtórzona kilka lub kilkanaście razy tworzy szyfrogram przypominający losowy zlepek znaków. W kwestii konstrukcji kroków rundy, wyróżnia się dwie główne techniki: sieci podstawieniowe-permutacyjne (AES) lub sieci Feisela (DES). Szczegóły na temat każdej z technik zostaną zawarte w przyszłych rozdziałach.

Wymóg co do określonego rozmiaru bloku niesie za sobą konsekwencje. Patrząc ze strony praktycznej, rozmiar wiadomości do zaszyfrowania bardzo rzadko jest równy wielokrotności rozmiaru bloku. W rzeczywistości, ostatni blok zawiera mniejszą liczbę danych. W takim wypadu blok należy uzupełnić odpowiednimi danymi. Wyróżnia się dwie wiodące techniki [11]:

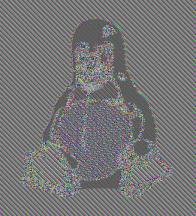
* „kradzież szyfrogramu”, czyli dopełnienie bloku danymi z poprzedniego szyfrogramu,
* padding, technika, w której wypełnia się wiadomość pewnym charakterystycznym ciągiem.

Bardzo popularną techniką paddingu jest technika PKCS#7, w której ciągiem danych jest powtórzona liczba brakujących bajtów (przykładowo, jeśli brakuje 10 bajtów to ciąg uzupełniający stanowi dziesięć liczb 10). Metoda ta ma jedną wadę, mianowicie nawet w przypadku idealnego pokrycia bloków przez dane wejściowe, dodaje się blok dodatkowy (szesnaście razy powtórzona liczba 16), w celu późniejszego usunięcia dopełnienia. W związku z powyższym, rozmiar danych wejściowych może zostać zwiększony o jeden bajt.

Rozmiar wiadomości do zaszyfrowania prawie zawsze przekracza rozmiar jednego bloku, w związku z czym w algorytmie należy zdefiniować schemat przetwarzania kolejnych bloków. Owy schemat nosi nazwę **trybu pracy szyfru blokowego**. Tryb pracy określa zależności (bądź ich brak) pomiędzy kolejnymi blokami tekstu. Istnieje kilka podstawowych trybów pracy, jednak w pracy zostanie zawarty opis dwóch z nich, jako że zachowują one własności szyfru blokowego, podczas gdy pozostałe zmieniają szyfr blokowy w pełnoprawny szyfr strumieniowy. Opis pozostałych szyfrów można znaleźć w [11], zaś wcześniej wspomniane dwa tryby to:

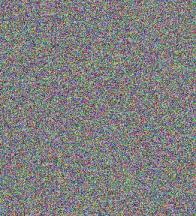
* **ECB** (ang. *electronic code book,* tryb elektronicznej książki kodowej) – w trybie tym każdy blok wiadomości, zarówno podczas szyfrowania jak i deszyfrowania jest przetwarzany zupełnie niezależnie. Ma to swoją zaletę w możliwości całkowitego zrównoleglenia szyfrowania, jednak niesie ze sobą dużo większą wadę w postaci niskiego bezpieczeństwa. Niezależność bloków powoduje, iż ten sam blok znajdujący się w różnych miejscach wiadomości zostanie przetworzony na taki sam szyfrogram. Doskonale jest to widoczne w przypadku szyfrowania obrazów, pomimo zaszyfrowania pikseli, wciąż można zobaczyć zarys tego, co było przedstawione na obrazie. Sławny cytat opisujący tę wadę w przetłumaczeniu na polski brzmi „widać Pingwina” [1] i odnosi się do wyniku szyfrowania logotypu systemu operacyjnego Linux. Przykład ten zaprezentowano na rysunkach 2.1 oraz 2.2.

Rysunek 2.1 Obraz poddany szyfrowaniu.



Rysunek 2.2 Szyfrogram obrazu.

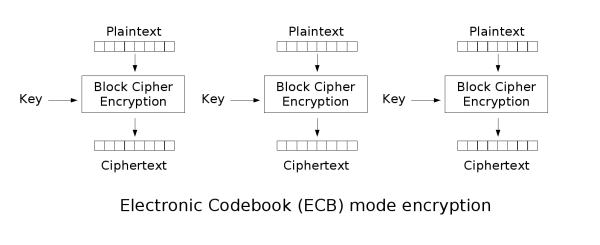
* **CBC** (ang. *cipher block chaining*, wiązanie bloków zaszyfrowanych) – w trybie tym bloki szyfrowane są sekwencyjnie, natomiast przed szyfrowaniem następnej wiadomości, następuje dodanie do bloku (poprzez operację alternatywy wykluczającej) szyfrogramu uzyskanego z poprzedniej wiadomości. Uniemożliwia to zrównoleglenie szyfrowania, albowiem następny blok jest zależny od poprzedniego, aczkolwiek przeprowadzenie deszyfrowania może odbywać się w sposób równoległy (pod warunkiem przechowania wszystkich szyfrogramów, co jest częstym przypadkiem). Co oczywiste, pierwszy blok nie posiada poprzedniego szyfrogramu, zatem przy procesie szyfrowania dodaje się do niego tzw. blok inicjalizacyjny IV (od angielskiego *initialization vector* – wektor inicjalizacyjny). Powinien być on generowany podobnie do klucza, a więc w sposób losowy [11]. Tryb CBC jest również odporny na wady trybu ECB. Dzięki zmianie bloku przed szyfrowaniem, te same bloki wiadomości jawnej uzyskają różny szyfrogram, co z kolei spowoduje niemożliwość szukania schematów, jako że wynik działania szyfru znacznie bardziej przypomina losowy ciąg (szum). Wynik szyfrowania obrazu w trybie CBC zaprezentowano na rysunku 2.3.



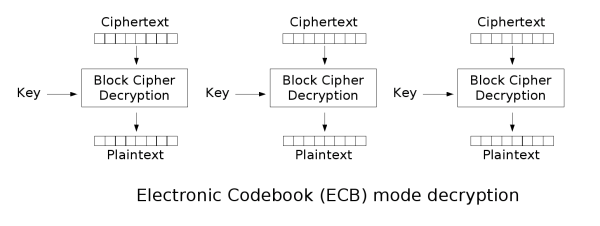
Rysunek 2.3 Wynik szyfrowania obrazu 2.1 w trybie CBC.

Mając na względzie bezpieczeństwo, nie powinno stosować się trybu ECB w praktyce [1]. Ułatwia on kryptoanalizę, co może doprowadzić do złamania wiadomości. Niekoniecznie może to prowadzić do złamania całego szyfru (w szczególności klucza), aczkolwiek narusza poufność danych. W związku z powyższym, rekomendowanym trybem pracy dla szyfrów blokowych (wyłączając tryby zmieniające tryby blokowe na strumieniowe) jest tryb CBC. Istnieje również jego modyfikacja, tryb PCBC, w której poza szyfrogramem dodaje się tekst jawny poprzedniego bloku, ale jest to zmiana w sposobie działania na tyle nieistotna, że szczegółowy opis jest bezzasadny (samo zaś dodanie tekstu jawnego może mieć zastosowanie w przypadku, gdy szyfrogram poszczególnych bloków jest podobny).

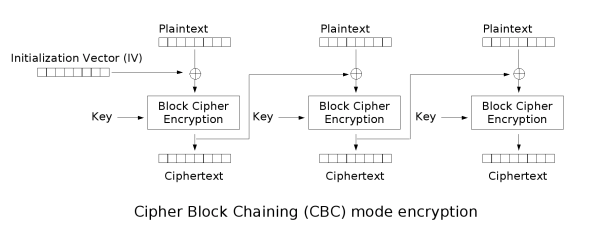
Obrazowo tryby ECB oraz CBC (w procesie szyfrowania i deszyfrowania) zostały przedstawione na rysunkach 2.4-2.7.



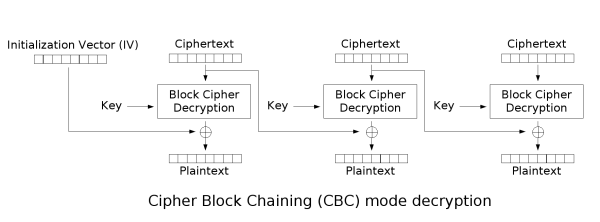
Rysunek 2.4 Schemat szyfrowania w trybie pracy ECB.



Rysunek 2.5 Schemat odszyfrowania w trybie pracy ECB.



Rysunek 2.6 Schemat szyfrowania w trybie pracy CBC.



Rysunek 2.7 Schemat deszyfrowania w trybie pracy CBC.

W latach 70 XX wieku w Stanach Zjednoczonych pojawiła się potrzeba ustandaryzowania szyfrów. Algorytmów do wyboru było wiele, aczkolwiek nie były one satysfakcjonujące, zatem powołano agencję NBS (ang. *National Bureau of Standard*, narodowe biuro standardów przekształcone potem w NIST, instytut standardów i technologii). Biuro przyjęło za standard szyfr opracowany przez firmę IBM i nadało mu nazwę DES (ang *Data Encryption Standard*, standard enkrypcji danych). Od początku był on krytykowany za wielkość zastosowanego klucza, aczkolwiek w tamtych latach moc obliczeniowa nie pozwalała na skuteczne ataki typu brute force. Wraz z upływem lat i postępem technologicznym, obawy o bezpieczeństwo algorytmu DES zaczęły być coraz bardziej uzasadnione. Stan ten sprawił, iż w 1997 NIST ogłosił konkurs na najlepszy algorytm, który miał zostać nowym standardem w kryptografii oraz uzyskać nazwę AES (ang. *Advanced Encryption Standard*, zaawansowany standard enkrypcji). Do konkursu, który zakończył się w 2001 roku, wpłynęło 15 propozycji zaś 5 zostało wybranych do finału. W niniejszej pracy znajdzie się opis dwóch z nich, algorytmu Rijandel, czyli ostatecznego zwycięzcy oraz algorytmu RC6. Opisany i poddany porównaniu zostanie również pierwszy standard, a więc algorytm DES.

# DES

# AES

Algorytmem, który po czterech latach trwania konkursu został wybrany przez NIST oraz otrzymał tytuł *Advanced Encryption Standard* był algorytm Rijndael. Nazwa owego algorytmu pochodzi od połączonych nazwisk jego twórców – Joana Daemena oraz Vincenta Rijmena. Dzięki swojej stosunkowo prostej budowie, można stworzyć jego implementację na wielu platformach i architekturach. Pomimo tej prostoty można go uznać za bezpieczny, albowiem do dzisiaj nie udało się stworzyć skutecznej metody ataku, która pozwoliłaby odtworzyć klucz.

Pod względem wysokopoziomowym, algorytm składa się z 3 kroków. Są to kolejno:

* rozszerzenie klucza – z klucza wejściowego (może być on 128, 192 lub 256 bitowy) podanego do algorytmu, tworzy się ciąg kluczy, inny dla każdej rundy,
* runda wstępna – do bloku wejściowego (16-elementowej macierzy bajtów, zwanej stanem) za pomocą operacji XOR dodawany jest klucz rundy (w tym przypadku, oryginalny klucz),
* runda – ciąg czterech operacji. Liczba rund zależna jest od długości klucza – 10 rund przeprowadza się dla klucza 128-bitowego, 12 dla 192 oraz 14 dla 256. Operacje, które są wykorzystywane w rundzie to:
  + zamiana bajtów,
  + zamiana wierszy,
  + zamiana kolumn,
  + dodanie klucza rundy.

Ostatnia runda odbywa się bez operacji zamiany kolumn. W dalszej części rozdziału znajdzie się opis każdej operacji, a także procesu rozszerzania klucza.

Rozszerzenie klucza jest operacją ważną z punktu widzenia bezpieczeństwa. Pozwala ono na użycie unikalnego klucza w każdej rundzie, w związku z czym każda runda jest inna. Gdyby była identyczna, wynikałaby z tego następująca zależność (4.1):



Gdzie:

 – dwa dane bloki tekstu jawnego – przekształcenie rundy – szyfrogramy odpowiadające .

Z oczywistych względów, zależność taka jest niebezpieczna i wyklucza użycie szyfru na szerszą skalę.

W celu opisania procesu rozszerzania klucza, należy zdefiniować następujące wielkości i transformacje [4]:

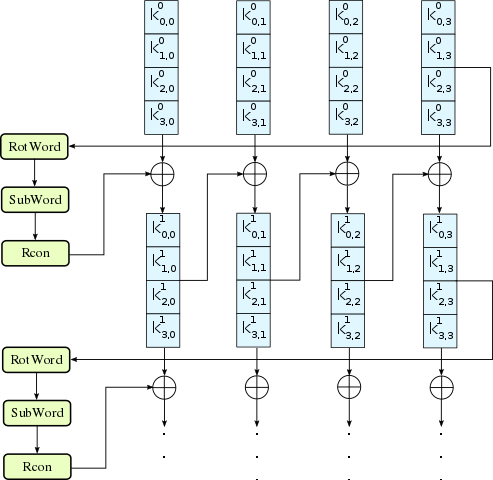
* – długość klucza liczona w 32-bitowych słowach, odpowiednio 4 dla klucza 128, 6 dla 192 i 8 dla klucza 256-bitowego,
* – 32-bitowe słowa oryginalnego klucza,
* – liczba rund, dla których potrzebny jest klucz rundy (11 dla klucz 128, 13 dla 129 oraz 15 dla klucza 256-bitowego),
* – 32-bitowe słowa klucza rozszerzonego,
* Transformacja RotWord przesuwająca bajty w słowie według następującego schematu:
  + , gdzie:  
     to kolejne bajty w słowie
* Transformacja SubWord przypisująca danemu bajtowi określone pole z tzw. tablicy   
  S-box. Szerzej ten proces zostanie opisany przy okazji wyjaśnienia operacji zamiany bajtów w rundzie algorytmu AES.

Przy powyższych założeniach, klucz rozszerzony dany jest zależnością (4.2) [4].



We wzorze (4.2) jest stałą zdefiniowaną z tabeli (4.3). Wartość oznacza indeks, zaś odpowiadającą mu wartość w systemie szesnastkowym.

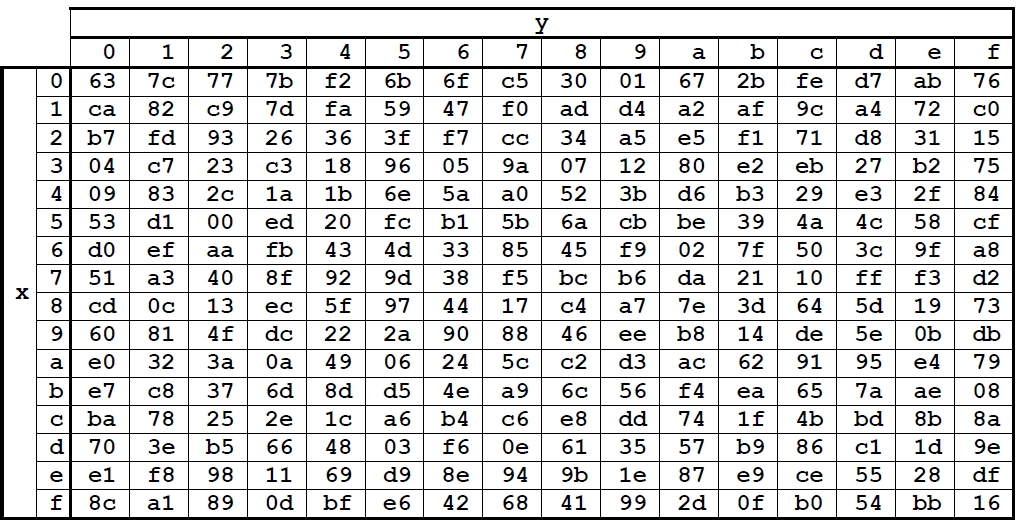


Maksymalny indeks potrzebny w procesie rozszerzania klucza wynosi 10, aczkolwiek można znaleźć wartość dla indeksu większego. Aby to uczynić, należy skorzystać z formuły matematycznej zawartej m.in. w [4]. Graficzna reprezentacja procesu tworzenia kluczy znajduje się na rysunku 4.1.

Rysunek 4.1 Schemat rozszerzania klucza w algorytmie AES.  
Źródło: https://commons.wikimedia.org/wiki/File:AES-Key\_Schedule\_128-bit\_key.svg

Jak już wcześniej wspomniano, dzięki zastosowaniu innego klucza dla każdej rundy, wynik jej działania zależy nie tylko od danych wejściowych, ale także od numeru rundy, w którym są one przetwarzane. We wcześniejszej części rozdziału, etapy rundy zostały wymienione, natomiast poniżej znajdzie się krótki opis każdego z nich.

Pierwszą przeprowadzaną w każdej rundzie operacją jest zamiana bajtów (ang. *sub bytes*). Jest to jedyne nieliniowe przekształcenie w szyfrze, bez niego odwrócenie rundy wymagałoby użycia bardzo podstawowych przekształceń algebraicznych, co wykluczałoby użycie szyfru [1]. Operacja polega na podstawieniu danej (liczby w systemie szesnastkowym) z tabeli w zamian za liczbę wejściową – pierwsza cyfra liczby wejściowej odpowiada numer wiersza, a druga za numer kolumny. Dane w tabeli podstawień (tak zwany s-box) zostały dobrane tak, żeby jak najmniej ze sobą korelować. Rysunek 4.2 przedstawia oryginalną tabelę zawartą w standardzie [4].



Rysunek 4.2 Tablica s-box używana w operacji zamiany bajtów.

Jako że s-box jest bardzo ważnym punktem algorytmu (ze względu na wprowadzenie jedynej nieliniowości), forma tabeli podlega wielu rozważaniom na temat poprawy lub modyfikacji. Ich forma bazuje na wielomianach, zatem przestrzeń poszukiwań jest relatywnie duża. Badania na temat wpływu rzędu wielomianu oraz jego formy na wariancję w danych wypełniających tabelę można znaleźć w [15].

Kolejnym etapem rundy jest operacja zamiany wierszy (ang. *shift rows*). Działa ona bliźniaczo podobno do operacji RotWord używanej w procesie rozszerzania klucza. W obu przypadkach stosuje się cykliczne przesunięcie w lewo, z tą różnicą, iż w rundzie algorytmu przesunięciu ulegają bajty w wierszu, a liczba miejsc, o które następuje przesunięcie zależne jest od numeru wiersza – pierwszy wiersz przesuwany jest w lewo o jedno, drugi o dwa, a trzeci o trzy miejsca. Czwarty wiersz nie jest przesuwany (jest to de facto równe przesunięciu o 4 miejsca, co zachowuje spójność operacji). Dzięki zamianie wierszy, kolumny stają się zależne od siebie, co zwiększa kryptograficzną moc algorytmu.

Przedostatnią operacją w rundzie (ze względu na swoją liniowość i ograniczenie obliczeń, nie występuje w ostatniej rundzie cyklu) jest operacja zamiany kolumn (ang. *mix columns*). W przeciwieństwie do operacji zamiany wierszy, gdzie przekształceniu poddawane były wiersze macierzy stanu, jak sama nazwa wskazuje, zamiana kolumn bazuje na kolumnach. Operacja ta sprowadza się do mnożenia wektora wejściowego z macierzą współczynników zgodnie ze wzorem (4.4)



Operacja mnożenia wykonywana jest w tzw. przestrzeni Galoisa, gdzie operuje się na liczbach maksymalnie 8-bitowych, a operacje zdefiniowane są tak, iż wynik również należy do tej przestrzeni (szczególnie ważne jest to przy operacji mnożenia, gdzie wynik może łatwo wykroczyć poza zakres). Szczegóły implementacji mnożenia w tej przestrzeni można znaleźć w [13]. Dzięki zamianie kolumn, zmiana jakiegokolwiek bajtu w macierzy stanu algorytmu, zmienia wszystkie pozostałe.

Ostatnią operacją rundy jest dodanie klucza rundy za pomocą operacji XOR. Jak już wspomniano przy opisie rozszerzania klucza, jest to kluczowa czynność, albowiem powoduje dywersyfikacje rund względem siebie, jako że każda posiada unikalną daną będącą właśnie kluczem rundy.

Jedna runda algorytmu Rijndael nie jest szczególnie bezpieczna kryptograficznie, aczkolwiek kilkunastokrotne powtórzenie tworzy algorytm, którego do tej pory nie udało się efektywnie złamać [1].

Proces odkodowania szyfrogramu przebiega odwrotnie do procesu szyfrowania przedstawionego powyżej. Odwrotnością operacji dodania klucza jest jego ponowne dodanie (ze względu na własność operacji XOR). Żeby odwrócić zamianę kolumn należy pomnożyć poprzez macierz odwrotną do macierzy z wzoru (4.4). Zamiana wierszy jest trywialnie odwracalna poprzez przesunięcie cykliczne w prawo, zaś operacja s-box posiada odwrotną do tabeli z rysunku 4.2 tablicę przekształceń, którą można znaleźć m.in. w [4]. Operacje szyfrowania czy też deszyfrowania całej wiadomości, a nie jednego bloku są zgodne ze schematami przedstawionymi w rozdziale 2 na rysunkach 2.4-2.7. Algorytm AES można zaimplementować, aby wspierał oba przedstawione tryby pracy szyfru (a także inne niewspomniane w pracy).

Opisana powyżej struktura algorytmu Rijndael jest strukturą oryginalną, zgłoszoną w konkursie NIST. Jak podaje źródło [1], nie jest ono bezpośrednio stosowane. Opracowano rozwiązanie bazujące na specjalnych tablicach oraz instrukcjach XOR, które znacząco usprawnia działanie algorytmu wykonując operacje tożsame pod względem końcowego efektu. Ponadto, stosuje się również instrukcje natywne dla procesora danej architektury, co również przyspiesza proces szyfrowania i deszyfrowania. W projekcie związanym z pracą zostanie zawarta implementacja oryginalnego algorytmu, a uzyskane rezultaty zostaną porównane z wynikami zawartymi w innych źródłach literatury.

# 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. FIPS PUB 197. *The official AES standard.* NIST, 21.10.2001
5. 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
6. 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
7. 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
8. 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
9. 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
10. 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
11. 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).
12. Stinson D. R.: *Kryptografia. W teorii i praktyce.*Warszawa: Wydawnictwo Naukowo-Techniczne, 2005. ISBN 83-204-2982-X
13. Trenholme S. *AES' Galois field*. W: <https://www.samiam.org/galois.html> [dostęp 01.04.19]
14. Vu A., et al., *A homogeneous parallel brute force cracking algorithm on the GPU*.   
    Seoul: ICTC 2011*,* 2011, s. 561-564. doi: 10.1109/ICTC.2011.6082661
15. Wang D., Sun S. *Replacement and Structure of S-Boxes in Rijndael*.   
    Hubei: 2008 International Conference on Computer Science and Software Engineering*,* 2008, s. 782-784. doi: 10.1109/CSSE.2008.296