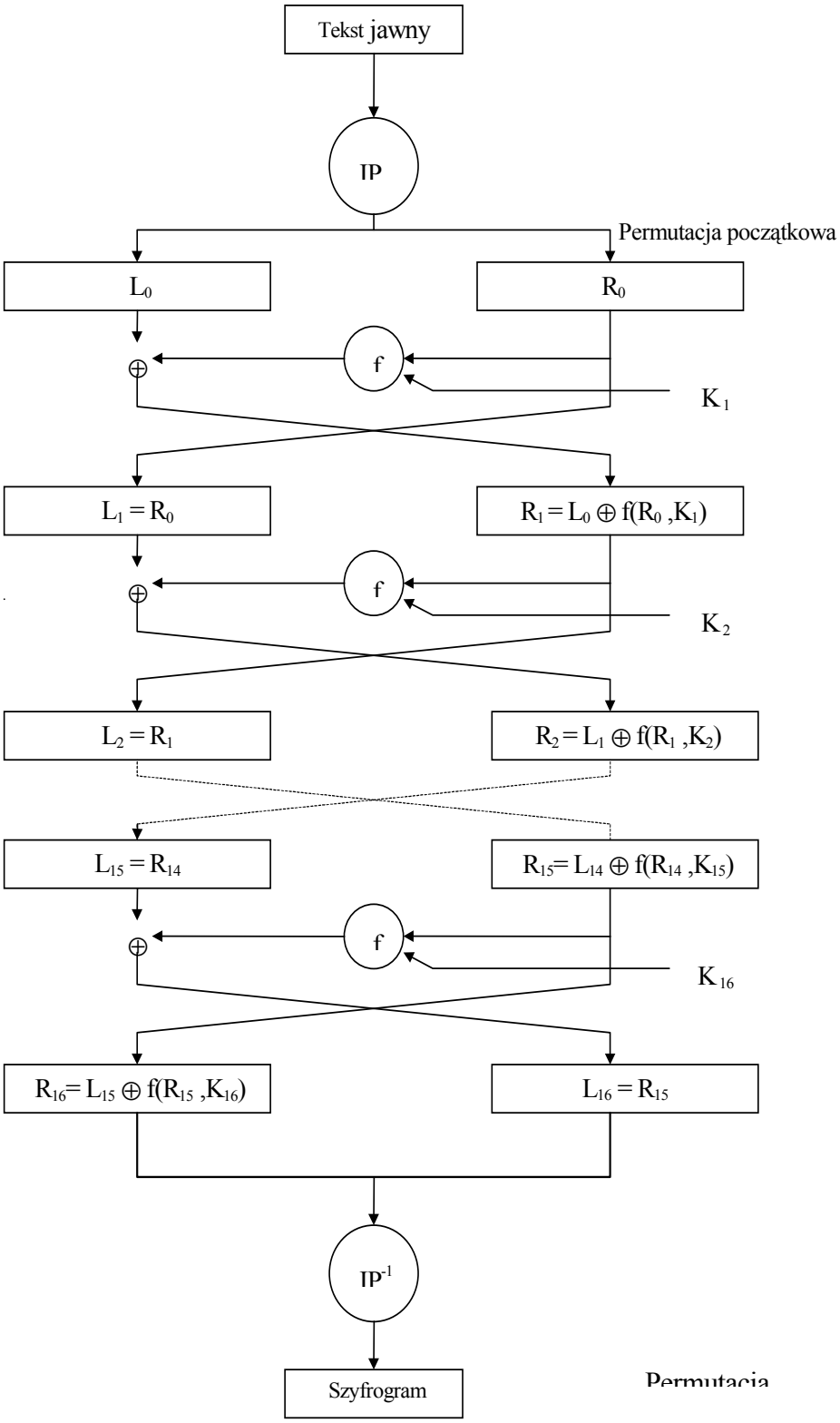
1.1. Standard szyfrowania DES

Powstał w latach siedemdziesiątych i został przyjęty jako standard szyfrowania przez Amerykański Narodowy Instytut Standaryzacji (ang. American National Standards Institute – ANSI) 23 listopada 1976 roku [1, 2, 3, 4, 5, 6, 7, 8, 9, 10].



Rys.14. Schemat blokowy algorytmu DES

DES jest szyfrem blokowym, pracującym na 64-bitowych pakietach danych. Zarówno do szyfrowania, jak i deszyfrowania stosuje się ten sam algorytm. Klucz jest 64-bitowy, przy czym informacja użyteczna zajmuje 56 bitów (co ósmy bit w ciągu klucza jest bitem parzystości). Całe bezpieczeństwo spoczywa właśnie na nim.

Algorytm DES to kombinacja dwu podstawowych technik: mieszania i rozpraszania.

1.1.1. Opis algorytmu

Tekst jawny (64-bitowy blok) poddawany jest permutacji wstępnej (tabela 3, blok oznaczony IP). Potem dzielony jest na dwa podciągi 32-bitowe (rys. 14). Następnie wykonywanych jest 16 cykli jednakowych operacji, nazywanych funkcjami *f*. Po szesnastym cyklu lewa i prawa strona są łączone i poddawane permutacji końcowej (tabela 4).

Tabela 3. Permutacja początkowa IP

58	50	42	34	26	18	10	2	60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6	64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1	59	51	43	35	27	19	11	3
61	53	5	37	29	21	13	5	63	55	47	39	31	23	15	7

Tabela 4. Permutacja końcowa IP-1

40	8	48	16	56	24	64	32	39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30	37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28	35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26	33	1	41	9	49	17	57	25

1.1.2. Jak powstaje klucz?

Ponieważ klucz jest 64-bitowy, redukowany jest do klucza 56 bitów przez pominięcie co ósmego bitu parzystości. Tak przygotowany ciąg bitów poddawany jest permutacji wejściowej (tabela 5), po czym dzielony jest na dwa podciągi 28-bitowe. Następnie połowy te przesuwane są w lewo o jeden lub dwa bity, zależnie od numeru cyklu (tabela 6).

Po połączeniu nowo powstałych ciągów wybiera się 48 z 56 bitów (tabela 7, permutacja z kompresją). Tak otrzymujemy klucz dla i-cyklu (gdzie i jest numerem cyklu), i = 1, ...,16.

Tabela 5. Permutacja klucza

57	49	41	33	25	17	9	1	58	50	42	34	26	18
10	2	59	51	43	35	27	19	11	3	60	52	44	36
63	55	47	39	31	23	15	7	62	54	46	38	30	22
14	6	61	53	45	37	29	21	13	5	28	20	12	4

Tabela 6. Tablica przesunięć połówek klucza

NR ITERACJI I	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Liczb. Przes.	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

Tabela 7. Tablica permutacji kompresji

14	17	11	24	1	5	3	28	15	6	21	10
23	19	12	4	26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40	51	45	33	48
44	49	39	56	34	53	46	42	50	36	29	32

1.1.3. Realizacja funkcji *f*

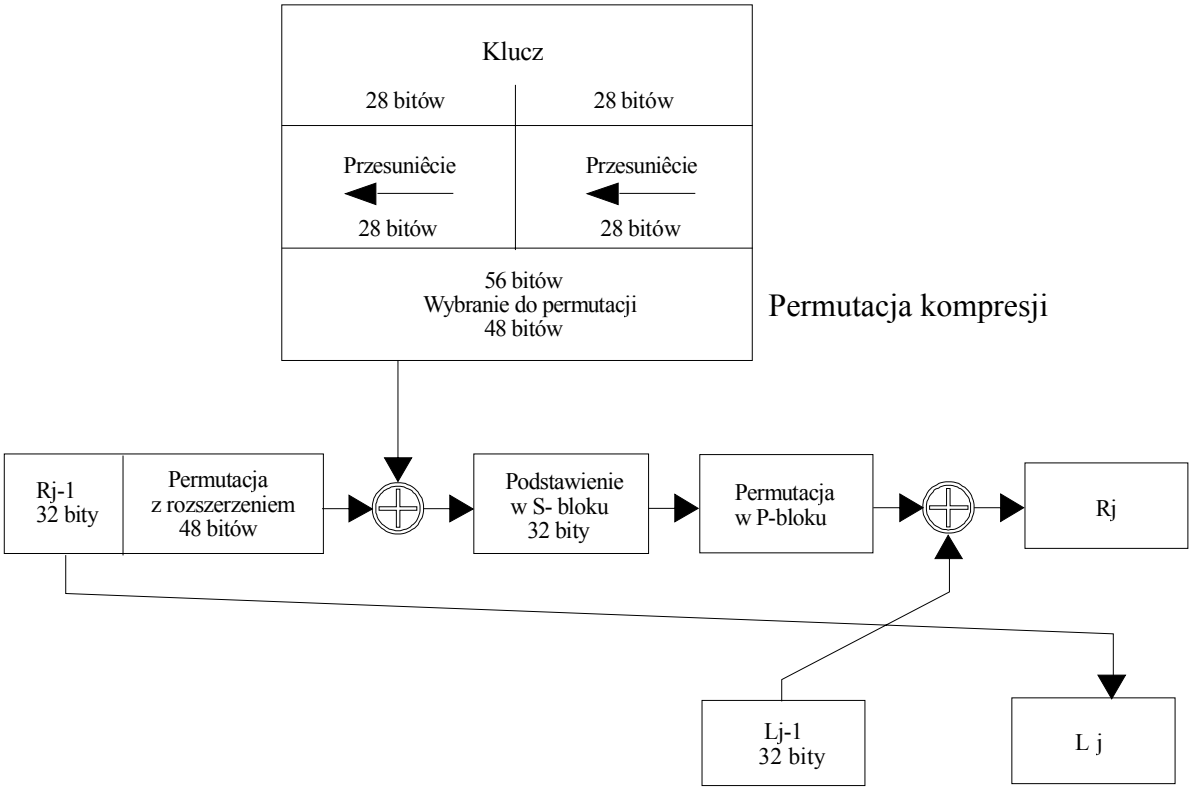
W funkcji *f* (rys. 15) prawa połowa bloku danych jest poddawana permutacji z rozszerzeniem (tabela 8, E), czyli z 32 do 48 bitów. Następnie, nowo powstały podciąg bitów, łączony jest za pomocą poelementowej sumy modulo 2 z 48 bitami przesuniętego i spermutowanego klucza. Po tej operacji otrzymany ciąg dzielony jest na 8 części i wprowadzany do skrzynek S-bloków (tabela 10), gdzie z 6-bitowych podciągów na wyjściu otrzymujemy 4-bitowe podciągi, które łączymy ze sobą. Nowo powstały ciąg jest na wyjściu poddany permutacji (tabela 9, P) i otrzymujemy zaszyfrowany ciąg 32-bitowy.

Tabela 8. Tabela permutacji rozszerzenia

32	1	2	3	4	5	4	5	6	7	8	9
8	9	10	11	12	12	12	13	14	15	16	17
16	17	18	19	20	21	20	21	22	23	24	25
24	25	26	27	28	29	28	29	30	31	32	1

Tabela 9. Tabela permutacji P-bloku

16	7	20	21	29	12	28	17	1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9	19	13	30	6	22	11	4	25



Rys. 15. Metoda wyznaczania wartości funkcji f dla DES

Przekształcenie 6-bitowego bloku na 4-bitowy w skrzynce odbywa się w ten sposób, że liczba b1b6 określa wiersz tablicy, a bity b2b3b4b5 określają kolumnę.

1.1.4. Tryby pracy DES

DES pracuje w czterech trybach pracy:

1. tryb elektronicznej książki kodowej *(Electronic Codebook – ECB)*,
2. tryb wiązania bloków zaszyfrowanych *(Cipher Block Chaining – CBC),*
3. tryb sprzężenie zwrotne wyjścia *(Output Feedback – OFB),*
4. tryb sprzężenie zwrotne szyfrogramu *(Cipher Feedback – CFB).*

Bankowe standardy ANSI specyfikują [6, 7, 8, 9, 10]:

- ECB i CBC do szyfrowania,
- CBC i CFB do uwierzytelniania.

Najczęściej oferowanym, gotowym komercyjnym oprogramowaniem jest elektroniczna książka kodowa, mimo że jest najbardziej podatna na ataki.

Tabela 10. Tablica S-bloków

	0	***1***	***2***	***3***	***4***	***5***	***6***	***7***	***8***	***9***	***10***	***11***	***12***	***13***	***14***	***15***	
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7	***S1***
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8	

2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0	
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13	
0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10	***S2***
1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5	
2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15	
3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9	
0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8	***S3***
1	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1	
2	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7	
3	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12	
0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15	***S4***
1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9	
2	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4	
3	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14	
0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9	***S5***
1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6	
2	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14	
3	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3	
0	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11	***S6***
1	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8	
2	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6	
3	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13	
0	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1	***S7***
1	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6	
2	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2	
3	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12	
0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7	***S8***
1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2	
2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8	
3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11	

1.1.5. Sprzętowe i programowe implementacje DES

DES jest algorytmem, który powstał z myślą o implementacjach sprzętowych. Układ skonstruowany przez Digital Equipment Corporation, zbudowany z 50 tysięcy tranzystorów na podłożu z GaAs, zawiera zespół bramek realizujących tryby ECB i CBC. Dane mogą być szyfrowane i deszyfrowane z szybkością 1 Gbit/s, co jest równoważne 15,6 milionom bloków na sekundę. Jest to imponująca liczba [1, 2, 3, 11, 12, 13, 14, 15].

Implementacje programowe są znacznie wolniejsze i przegrywają w konkurencji z rozwiązaniami sprzętowymi. Tabela 11 przedstawia szybkości realizacji algorytmu DES przez różne mikroprocesory.

Tabela 11. Szybkość realizacji algorytmu DES przez różne mikroprocesory

Procesor	Częstotliwość zegara	Szerokość szyny	Szybkość szyfrowania

	procesora (w Mhz)	(w bitach)	(bloki DES na sekundę)
8088	4,7	8	370
68000	7,6	16	900
80286	6,0	16	1100
68020	16,0	32	3500
68030	16,0	32	3900
80386	25,0	16	5000
68030	50,0	32	9600
68040	25,0	32	23200
80486	33,0	32	40600

1.1.6. Bezpieczeństwo algorytmu DES

Okazuje się, że z powodu sposobu, w jaki jest modyfikowany klucz dla kolejnych cykli algorytmu, niektóre z nich są *kluczami słabymi* (tabela 12), tzn.że klucz użyty w jednym cyklu algorytmu będzie taki sam we wszystkich pozostałych, a co za tym idzie tekst jawny nie zostanie zaszyfrowany.

Istnieją również pary kluczy, które szyfrują tekst jawny do jednakowych szyfrogramów. Innymi słowy, jeden klucz z pary może służyć do deszyfrowania wiadomości zaszyfrowanej drugim kluczem z tej pary. Zamiast generować 16 różnych podkluczy, generowane są dwa. Każdy z nich jest wykorzystywany 8 razy w algorytmie. Klucze takie nazywamy *kluczami półsłabymi* (tabela 13) [1, 2, 3, 16].

Tabela12. Klucze słabe algorytmu DES (zapis szesnastkowy)

Pierwotny ciąg słabego klucza	Faktyczny ciąg klucza
0101 0101 0101 0101	0000000 0000000
FEFE FEFE FEFE FEFE	FFFFFFF FFFFFFF
1F1F 1F1F 1F1F 1F1F	0000000 FFFFFFF
E0E0 E0E0 F1F1 F1F1	FFFFFFF 0000000

Tabela 13. Klucze półsłabe algorytmu DES

01FE	01FE	01FE	01FE
1FE0	1FE0	0EF1	0EF1
01E0	01E0	01F1	01F1
1FFE	1FFE	0EFE	0EFE
011F	011F	010E	010E
E0FE	E0FE	F1FE	F1FE
FE01	FE01	FE01	FE01
E01F	E01F	F10E	F10E
E001	E001	F101	F101
FE1F	FE1F	FE0E	FE0E
1F01	1F01	0E01	0E01
FEE0	FEE0	FEF1	FEF1

W 1990 roku *Eli Biham* i *Adi Shamir* opublikowali metodę kryptoanalizy różnicowej [17]. Atak przy wykorzystaniu tej metody okazał się bardzie skuteczny od dotąd stosowanego ataku brutalnego. Metoda ta przy znanym tekście jawnym działa przeciw DES w dowolnym trybie pracy – ECB, CBC, CFB oraz OFB. DES może być ulepszony przez zwiększenie liczby cykli. Okazuje się, że już przy 19 cyklach metoda wyczerpującego przeszukiwania jest efektywniejsza niż analizy różnicowej (tabela 14).

Tabela 14. Złożoność ataku na DES metodą kryptoanalizy różnicowej

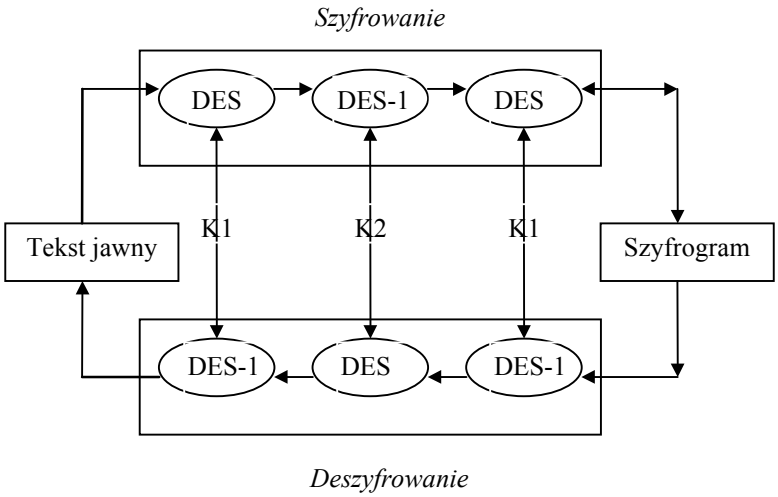
Liczba cykli	**Wybrane teksty jawne**	**Znane teksty jawne**	**Analizowane teksty jawne**	**Złożoność analizy**
8	2^{14}	2^{38}	4	2^{9}
9	2^{24}	2^{44}	2	2^{32}
10	2^{24}	2^{43}	2^{14}	2^{15}
11	2^{31}	2^{47}	2	2^{32}
12	2^{31}	2^{47}	2^{21}	2^{21}
13	2^{39}	2^{52}	2	2^{32}
14	2^{39}	2^{51}	2^{29}	2^{29}
15	2^{47}	2^{56}	2^{7}	2^{37}
16	2^{47}	2^{55}	2^{36}	2^{37}

1.1.7. Modyfikacje algorytmu DES

Ponieważ za sprawą *Eli Biham* i *Adi Shamir* znaleziono dość skuteczną metodę łamania szyfru DES, a postęp techniki zrządził, że nawet w przypadku łamania brutalnego, czas potrzebny na sprawdzenie wszystkich kombinacji klucza nie rozciąga się w nieskończoność, postanowiono zmodyfikować algorytm DES.

Wielokrotny DES

Ponieważ DES nie tworzy grup, można go wykorzystać wielokrotnie. W komercyjnych rozwiązaniach wykorzystuje się trzykrotny DES (rys. 16). Uzyskany szyfrogram jest dużo trudniejszy do złamania metodą wyczerpującego przeszukiwania: 2^{112} prób zamiast 2^{56}. Co ważne potrójne DES opiera się kryptografii różnicowej [1, 2, 3].



Rys. 16. Trzykrotny DES

Uogólniony DES

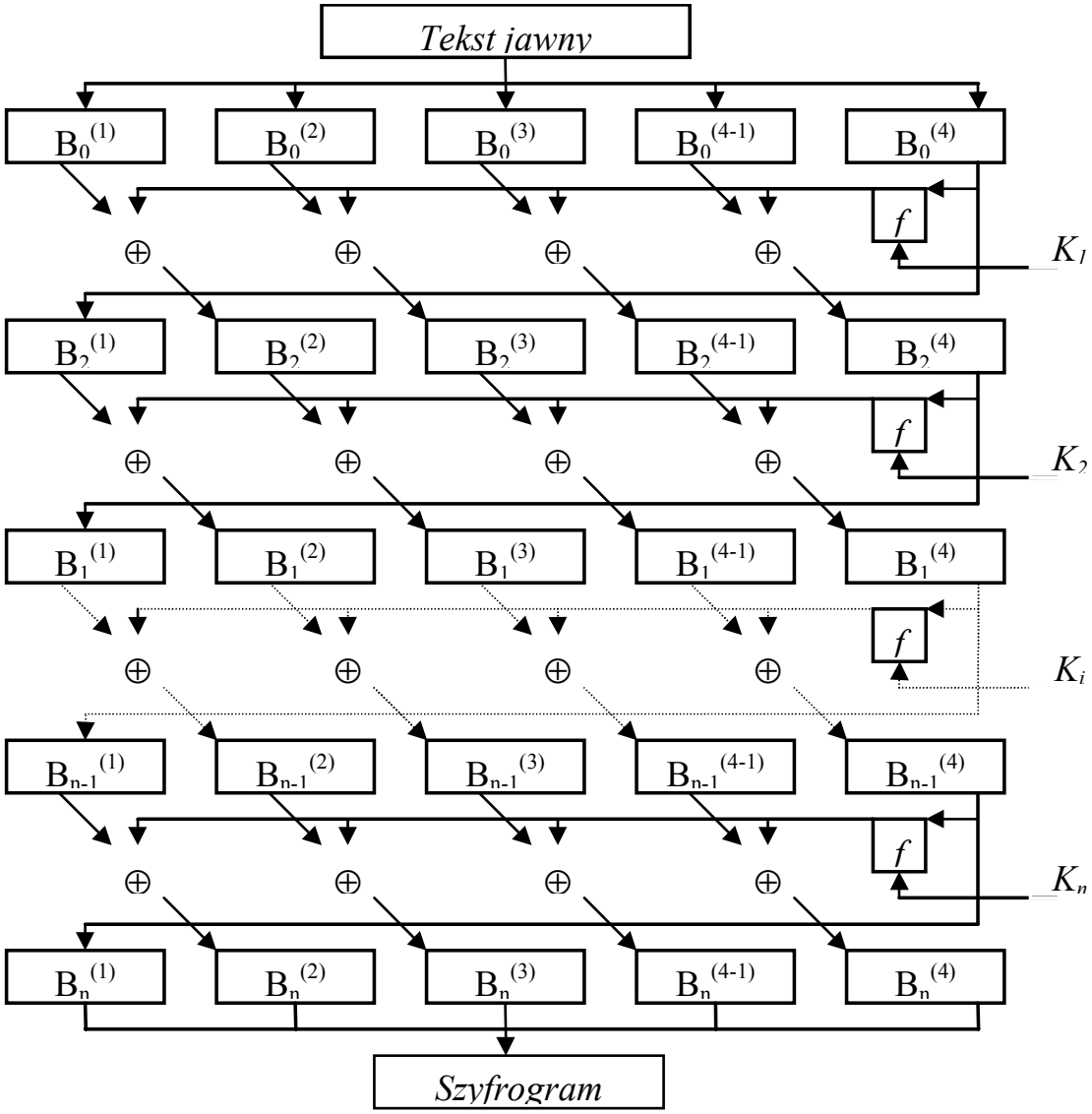
Uogólniony DES *(Generalized DES – GDES),* charakteryzuje się wzrostem długości bloku i niezmienioną funkcją *f* (rys. 17).

Szyfrowane bloki są dzielone na *q* 32-bitowych podbloków. Zazwyczaj liczba *q* jest równa długości bloku podzielonego przez 32. Jak widać ze schematu, funkcja *f* liczona jest tylko raz na cykl, dla podbloku leżącego najbardziej na prawo[1, 2].

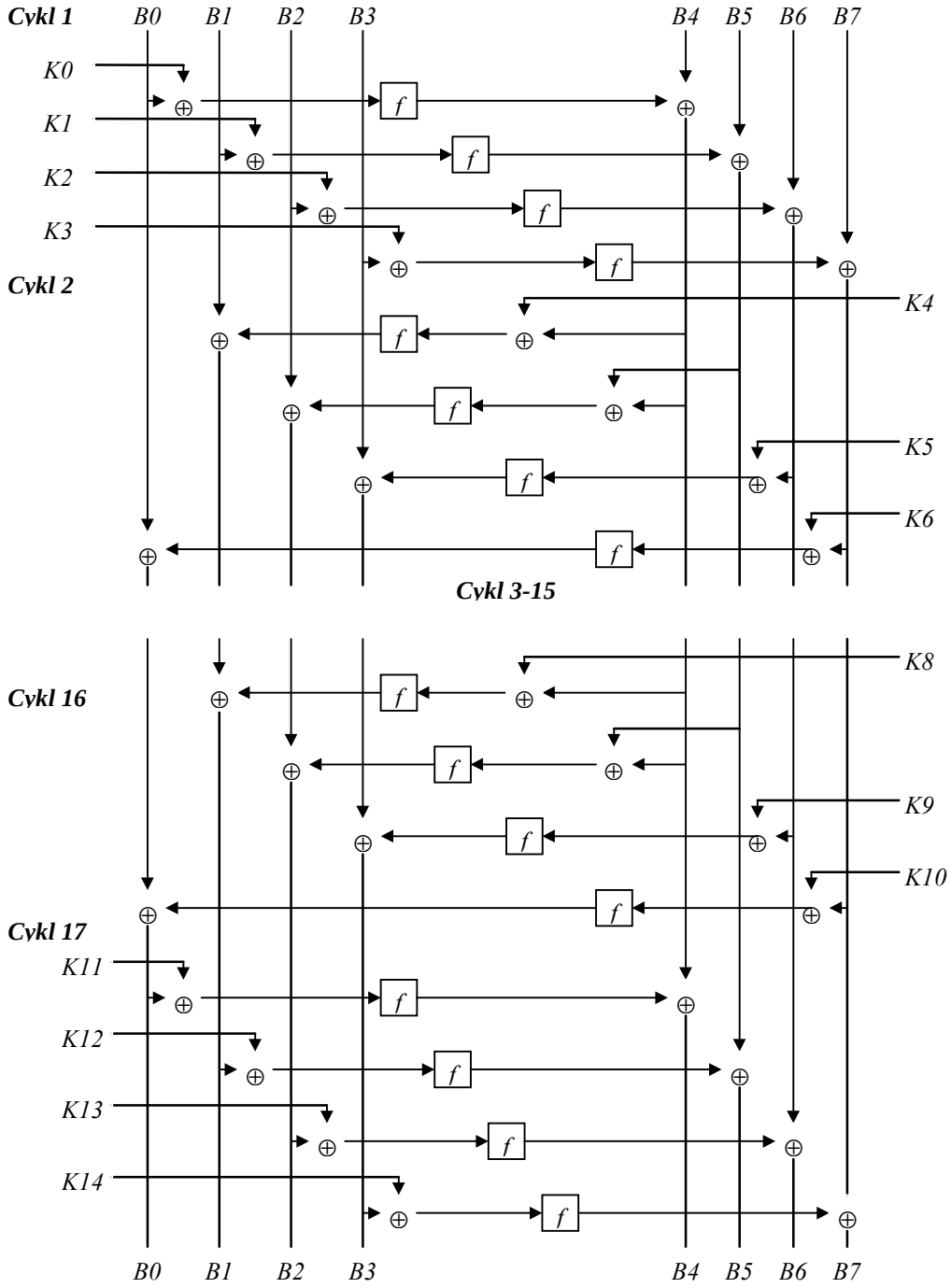
1.1.8. NewDES

NewDES (rys. 18) został zaprojektowany przez Roberta Scotta, w roku 1985, jako następca DES. Blok tekstu jawnego nadal ma 64 bity, zmieniła się natomiast długość klucza, 120 bitów. Scott zrezygnował w swojej wersji algorytmu z permutacji początkowej i końcowej, co w znacznym stopniu uprościło sam algorytm. Wszystkie operacje są wykonywane na całych bajtach, a sam algorytm nigdy nie czyta, nie zapisuje, nie permutuje żadnych pojedynczych bitów.

Funkcja *f* została zaprojektowana na podstawie tekstu Deklaracji Niepodległości. Szczegóły można znaleźć w [18].



Rys. 17. Schemat blokowy algorytmu GDES



Rys. 18. Schemat algorytmu NewDES