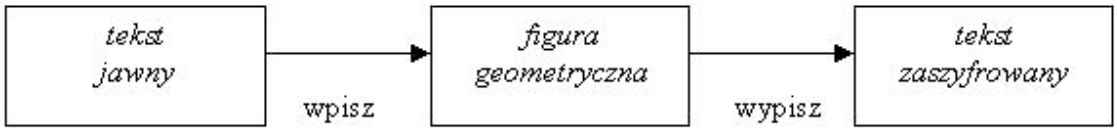
3. Zasada działania szyfrów

3.1 Szyfry przestawieniowe

Szyfry przestawieniowe swoją zasadę działania opierają na przestawianiu znaków w tekście. Zaszyfrowany tekst jest niczym innym jak permutacją tekstu jawnego, tj. zawiera wszystkie znaki tekstu jawnego, ale ustawione w innej kolejności. Wykorzystywane jest zazwyczaj w tym celu przekształcenie zwane *transpozycją*. Zasadę jej działania przedstawia poniższy rysunek .



Rys. 3.1. Działanie szyfrów przestawieniowych

Funkcję figury geometrycznej mógł spełniać np. walec, na który nawijano taśmę z tekstem jawnym a następnie odczytywano szyfrogram z góry do dołu.

3.1.1 Szyfr kolumnowy (klucz – permutacja kolumn)

W szyfrach kolumnowych, jak sama nazwa wskazuje funkcję figury geometrycznej pełni tablica dwuwymiarowa. Tekst jawny jest wpisywany do niej wierszami, a kryptogram otrzymujemy odczytując kolumny w określonej kolejności. Klucz *k* stanowią:

- parametry tablicy (wysokość × szerokość),
- permutacja *p* kolumn.

Przykład 3.1.1
Dany jest tekst jawny:

BRYLANTY PRZECHOWYWANE SĄ W SEJFIE BANKU OBOK STACJI

Tekst ten wpisujemy do tablicy o wymiarach 5 × 9, pomijając znaki spacji.

B	R	Y	L	A
N	T	Y	P	R
Z	E	C	H	O
W	Y	W	A	N
E	S	Ą	W	S
E	J	F	I	E
O	B	O	K	S
T	A	C	J	I

Tekst zaszyfrowany otrzymujemy odczytując kolumny w porządku (3 5 1 2 4) i ma on postać:

YYCWĄFOCARONSESIBNZWEEOTRTEYSJBALPHAWIKJ

Kluczem dla podanego przykładu jest k = (9 × 5, (3 5 1 2 4)).

Jeśli chodzi o tą metodę, to:

- odczytywanie może odbywać się np. skosem, nie tylko kolumnami,
- tablica to nie jedyna figura geometryczna, jaką możemy zastosować,
- można używać siatek - tekst jawny wpisywany jest w określone miejsca, a siatka obracana o 90°.

Kryptoanaliza tego typu szyfru jest nieskomplikowana. Jeśli domyślamy się, że określone słowo znajduje się w tekście jawnym, to możemy już przeprowadzić atak. Metoda ta jednak da pożądane rezultaty, gdy słowo to będzie dłuższe niż szerokość tablicy użytej do zaszyfrowania tekstu.

Przykład 3.1.2

Dany jest tekst zaszyfrowany tablicą z przykładu 3.1.1:

YYCWĄFOCARONSESIBNZWEEOTRTEYSJBALPHAWIKJ

Przypuszczalnie wiadomość zawiera słowo BRYLANTY. Można założyć, że osoba szyfrująca użyła tabeli o szerokości 3, wtedy w szyfrogramie powinny istnieć ciągi ‘BL’, ‘RA’, ‘YN’. Gdy nie natkniemy się w szyfrogramie na takie ciągi, zwiększamy szerokość tabeli o 1 i ponawiamy szukanie. Gdy jako prawdopodobną szerokość tabeli weźmiemy 5, zauważamy że w szyfrogramie istnieją następujące ciągi ‘BN’, ‘RT’, ‘YY’ (litery w tych ciągach leżą jeden pod drugim w tabeli). To spostrzeżenie sugeruje nam rzeczywistą szerokość tablicy, czyli 5. Drugim etapem ataku jest znalezienie odpowiedniego porządku

kolumn tablicy, a do przetestowania jest $n!$ możliwości, gdzie n to szerokość tablicy. Gdy znajdziemy właściwą kolejność wypełniania kolumn, szyfr zostanie całkowicie złamany (otrzymujemy nie tylko tekst jawny, ale dysponujemy też kluczem, umożliwiającym łamanie dalszych wiadomości).

Język ma określoną strukturę, stąd następujące po sobie litery zależą od siebie w pewien określony sposób. Gdy szyfrogram jest dostatecznie długi i otrzymany został z użyciem identycznych transpozycji grup znaków o jednakowej długości, wtedy łatwo jest go przetestować pod kątem występowania „sprzyjających" sobie par znaków. Metoda jest następująca :

1. Długość grupy znaków wyznaczamy przez zbadanie indeksu koincydencji (patrz szyfry podstawieniowe), otrzymujemy wartość n.
2. Tworzymy $n(n-1)/2$ par pozycji i oraz j w grupach (i, j = 1,2,3,...,n). Dla każdej takiej pary oceniamy ogólne rozmieszczenie tych samych i tak samo rozmieszczonych par liter w tekście.
3. Jeśli mamy do czynienia z tekstem jawnym napisanym w języku naturalnym, wtedy pary następujących po sobie liter mają rozkład typowy dla tego języka. Pary znaków, które nie leżą bezpośrednio obok siebie, nie są powiązane tak silnymi zależnościami (odpowiada im inny rozkład).
4. Powyższą analizę stosujemy do par z punktu 2. W wypadku niektórych z nich zaobserwujemy typowe rozkłady bigramów tekstu jawnego. Takie pary liczb z przedziału 1, 2, ... , n określamy mianem par wyróżnionych.
5. Wśród wyróżnionych par próbujemy odszukać łańcuchy następującej postaci:

   $$(n_1, n_2), (n_3, n_4), (n_5, n_6), ...$$

   Tego typu łańcuch długości n_i, w którym wszystkie n_i są różne, może być już szukaną transpozycją.
6. Jeśli nie znajdziemy żadnego odpowiedniego łańcucha lub po wykorzystaniu otrzymanego nie uzyskamy sensownego tekstu, musimy próbować inaczej łączyć ogniwa łańcucha, ewentualnie odgadując brakujące z nich. Pomocne mogą być tu digramy, które w praktyce nigdy nie występują.

3.1.2 Szyfr kolumnowy (ze słowem-kluczem)

Kluczem w szyfrach kolumnowych niekoniecznie musi być rozmiar tablicy i porządek odczytywania jej kolumn, ale może to być także konkretne słowo-klucz. Wtedy każdej literze słowa-klucza przypisujemy indeks. Zaczynamy od liczby 1, a kończymy na liczbie będącej długością słowa-klucza. Indeks 1 przypisywany jest literze słowa-klucza, która jest najbliżej początku alfabetu, indeks 2 otrzymuje druga w kolejności litera itd. Gdyby w słowie-kluczu pojawiły się dwie takie same litery, wtedy indeksujemy je od lewej. Drugim krokiem jest utworzenie tablicy o szerokości równej długości słowa-klucza i wysokości obliczonej ze wzoru: *suma/długość_klucza*, gdzie *suma* jest wynikiem dodania kolejno do siebie liczb całkowitych z przedziału <1, d*ługość_klucza*>, np. weźmy słowo kluczowe BALON, wtedy suma = 1 + 2 + 3 + 4 + 5, czyli suma = 15, więc tablica będzie mieć wymiary 5 × 3. Kolejną czynnością jest wpisanie tekstu jawnego to tak utworzonej tablicy w taki sposób, że w *i*-tym wierszu umieszczamy tyle znaków, ile wynosi indeks *i*-tej litery słowa-klucza. Kryptogram odczytujemy kolumnami zgodnie z indeksami liter klucza.

Przykład 3.1.3
Dany jest tekst jawny

BRYLANTY_SĄ_W_MOJEJ_SKRYTCE

Klucz: BALATON

B	**A**	**L**	**A**	**T**	**O**	**N**
3	**1**	**4**	**2**	**7**	**6**	**5**
B	R					
Y	L	A	N			
T						
Y	_	S				
Ą	_	W	_	M	O	J
E	J	_	S	K	R	
Y	T	C	E	X		

Aby zachować zasadę wypełnienia każdego wiersza, w ostatnim dodajemy pusty znak ‘X’. Otrzymany kryptogram (wolne pola pomijamy) ma postać:

RL_ _JTN_SEBYTYĄEYASW_CJORMKX

3.1.3 Szyfr przekątnokolumnowy (ze słowem-kluczem)

Podobnie jak w poprzednim szyfrze używane jest słowo-klucz, którego litery są indeksowane na identycznej zasadzie. Tablica szyfrująca ma wymiary $n \times m$, gdzie n to szerokość równa długości klucza, a m to wysokość równa zaokrąglonemu w górę wynikowi z podzielenia długości tekstu jawnego przez długość klucza, np. dla tekstu jawnego o długości 41 znaków i klucza o 8 literach, trzeba już użyć tablicy o 6 wierszach, a ostatni wiersz będzie wypełniony do końca pustymi znakami ‘X’. Różnica polega na tym, że tekst jawny wpisujemy do tablicy wierszami, wypełniając każdy wiersz do końca, niezależnie od indeksów liter klucza. Szyfrogram również jest odczytywany w zgodnie z kluczem od góry do dołu tablicy, jak miało to miejsce w poprzednim szyfrze, ale nie kolumnami a skosem, od prawej do lewej (przyjmując, kolumny skrajne za sąsiednie).

Przykład 3.1.4
Dany jest tekst jawny

BRYLANTY_SĄ_W_MOJEJ_SKRYTCE_W_BANKU

Klucz: MAROKO

M	**A**	**R**	**O**	**K**	**O**
3	**1**	**6**	**4**	**2**	**5**
B	*R*	Y	L	A	N
T	Y	_	S	Ą	_
W	_	M	O	J	*E*
J	_	S	K	*R*	Y
T	C	E	_	W	_
B	A	*N*	K	U	X

Kursywą oznaczona jest pierwsza odczytywana przekątna, a otrzymany szyfrogram ma postać:

RTER_NASM_TXB_JKEAL_ _J_UNĄOSCBYYWYWK

Kryptoanaliza szyfrów: kolumnowego i przekątnokolumnowego ze słowem-kluczem, może być przeprowadzana w podobny sposób, jak dla szyfrów kolumnowych z kluczem będącym permutacją kolumn tablicy szyfrującej. Dla wszystkich wymienionych wyżej szyfrów problemem dosyć istotnym jest konieczność wypełniania wierszy do końca znakami pustymi ‘X’. Ich liczba i pozycja ułatwiają znalezienie informacji o strukturze transpozycji.

3.1.4 Szyfr siatkowy

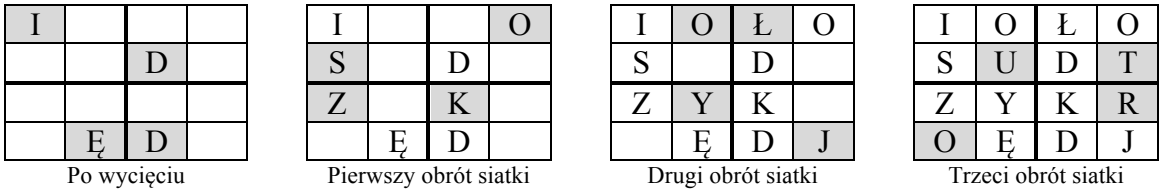
Szyfry siatkowe są bardzo ciekawą odmianą szyfrów przestawieniowych. W szyfrach tych wykorzystuje się tablice kwadratowe o boku długości 2 lub wielokrotności 2 (zazwyczaj stosuje się tablice o boku min 4). Maksymalna długość tekstu jawnego, jaki możemy zaszyfrować równa jest kwadratowi długości boku tablicy. Zasada działania szyfrów siatkowych jest prosta. Wykorzystuje się do szyfrowania specjalne siatki, w których tekst jawny wpisuje się we wskazanych miejscach. Następnie siatkę obraca się 3 razy o 90°, po każdym obrocie wpisując kolejną grupę znaków tekstu jawnego. Tekst wpisywany jest w we wskazane miejsca od lewego, górnego narożnika. Tablica jest podzielona na cztery kwadraty. Siatka ma tyle „dziur” do wpisywania tekstu, ile wynosi *n,* gdzie *n* jest kwadratem długości boku jednego z tych kwadratów. Kwadraty te z kolei podzielone są jeszcze na *n* kwadratów jednostkowych ponumerowanych od 1 do *n*. Numeracja kwadratów jednostkowych nie jest przypadkowa. Przykładowe numerowanie tabeli 6 × 6 pokazuje tabela 3.1:

Tabela 3.1 Wypełnienie tablicy szyfru siatkowego o wymiarach 6 × 6

1	2	3	7	4	1
4	5	6	8	5	2
7	8	9	9	6	3
3	6	9	9	8	7
2	5	8	6	5	4
1	4	7	3	2	1

Przykład 3.1.5
Dany jest tekst jawny:

IDĘ DO SZKOŁY JUTRO



Po wycięciu początkowym | Pierwszy obrót siatki | Drugi obrót siatki | Trzeci obrót siatki

Komórki z ciemniejszym tłem wskazują miejsca, w które wpisywana jest kolejna grupa znaków (w tym przykładzie 4 kolejne znaki, spacje zostają pominięte). Po odczytaniu wierszami tablicy (po trzecim obrocie siatki) otrzymujemy szyfrogram:

IOŁOSUDTZYKROĘDJ

Atak na szyfry siatkowe może odbyć się w sposób brutalny: sprawdzamy wszystkie możliwości umieszczenia „dziur" w siatce; o ile dla tablicy 4 × 4 jest to 256 kombinacji, to dla tablicy 6 × 6 jest to już 16384 !!!. Pomocne okażą się też techniki znane z szyfrów opisanych w rozdziałach 3.1.1 - 3.1.4.

3.1.5 Szyfr permutacyjny

Szyfry permutacyjne działają na tekście jawnym podzielonym na grupy znaków o długości T (permutują znaki tekstu jawnego z pewnym okresem T). Jeśli f będzie permutacją zbioru $\{1, 2, 3, ..., T\}$, szyfrowanie odbywa się w taki sposób, że w każdym z bloków o długości T permutujemy znaki zgodnie z f.

Przykład 3.1.6
Dany jest tekst jawny:

SPOTKAJMY_SIĘ_JUTRO_RANO

Klucz: k = (3 6 1 4 2 5)

m = SPOTKA JMY_SI Ę_JUTR O_RANO

E(m, k) = TSKOPA YJ_IMS ĘRU_TJ OR_NAO

m - wiadomość podzielona na bloki długości 6

E(m, k) - otrzymany z szyfrowania z kluczem f tekst.

Deszyfrowanie wymaga użycia permutacji odwrotnej.

3.2 Szyfry podstawieniowe

W szyfrach podstawieniowych każdy znak tekstu jawnego zostaje zastąpiony innym znakiem. Podstawienie to powoduje, że tekst jawny nie jest zrozumiały dla nikogo oprócz odbiorcy, który odwraca podstawianie i uzyskuje tekst jawny. W kryptografii wyróżnia się cztery podstawowe typy szyfrów podstawieniowych:

- prosty, w którym każdy znak tekstu jawnego jest zastępowany odpowiadającym mu znakiem alfabetu tajnego,
- homofoniczny, podobny do prostego szyfru podstawieniowego z tym, że pojedynczemu znakowi tekstu jawnego jest przyporządkowanych kilka znaków. Na przykład literze „A" może odpowiadać 5,13,25,56, literze „B" - 7,19,42 itd.,
- polialfabetyczne, które są złożeniem wielu prostych szyfrów podstawieniowych. Zmiana alfabetu może na przykład następować wraz z pozycją znaku w szyfrowanym tekście,
- poligramowy (wieloliterowy), to taki, w którym są szyfrowane grupy znaków. Na przykład trójce „ABA" odpowiada „RTQ", a „ABB" opowiada „SSL" itd.

3.2.1 Szyfr Cezara

Szyfr Cezara jest przykładem szyfru prostego (monoalfabetycznego), który przesuwa w swojej uogólnionej postaci litery alfabetu jawnego cyklicznie w prawo o k pozycji. Jeśli ponumerować litery alfabetu zgodnie z tabelą 3.2, to litery te można traktować jako liczby.

Tabela 3.2 Indeksowanie liter i znaków w szyfrze Cezara

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Wtedy szyfr Cezara realizuje przekształcenie E takie, że dla każdego $m \in$ A

$$c = E\,(\mathrm{m}, \mathrm{k}) = (\mathrm{m} + \mathrm{k}) \bmod n$$

n – długość alfabetu

Deszyfrowanie jest realizowane wg wzoru

$$m = E^{-1}\,(\mathrm{c}, \mathrm{k}) = (\mathrm{c} - \mathrm{k}) \bmod n$$

k – przesunięcie (Cezar w swojej pierwotnej wersji miał przesunięcie równe 3)

m – litera tekstu jawnego, c – litera szyfrogramu

Przykład 3.2.1
Dany jest tekst jawny:

PRACA DYPLOMOWA

Użycie szyfru Cezara (z przesunięciem $k = 3$) daje kryptogram:

SUDFDGBSORPRZD

Kryptoanaliza szyfru Cezara jest bardzo prosta. Wystarczy sprawdzić wszystkie możliwe klucze, gdyż każda litera kryptogramu znajduje się w stałej odległości od odpowiadającej jej litery tekstu jawnego. Inną metodą ataku na proste szyfry podstawieniowe jest analiza częstości występowania liter. Dla każdego języka naturalnego (np. angielskiego, polskiego) częstość występowania określonego znaku (litery) jest inna. Przykładowe oczekiwane wartości podaje tabela 3.3.

Tabela 3.3 Częstości występowania liter

Znak(i)	Język naturalny			
	Język polski		Język angielski	
	Literatura	Informatyka	Literatura	Informatyka
a ą	0,080	0,063	0,067	0,058
B	0,013	0,010	0,013	0,010
c, ć	0,038	0,029	0,019	0,023
D	0,030	0,020	0,031	0,025
e ę	0,069	0,055	0,089	0,089
f	0,001	0,007	0,021	0,017
...	...	...	...	...

Aby obliczyć częstość występowania znaków należy zliczyć wystąpienia takich samych liter, a następnie podzielić przez długość tekstu. Przeprowadzenie takiego badania na kryptogramie i porównanie z częstościami oczekiwanymi umożliwia dopasowanie liter kryptogramu do liter tekstu jawnego. Można też sprawdzić częstość występowania digramów (par znaków) i trigramów (trójek znaków). Przykładowo, gdy obliczymy częstość litery *p* w szyfrogramie i otrzymamy wynik 0,036 oraz wiemy, że tekst zaszyfrowany to fragment literatury polskiej, możemy spróbować podstawić za *p* literę *c* (bądź *ć*). W efekcie dalszych podstawień, można otrzymać tekst jawny.

Inną odmianą szyfru Cezara jest bardziej złożone przekształcenie:

$$c = E\,(\mathrm{m}, \mathrm{k}) = m \cdot k \bmod n$$

Przy deszyfrowaniu wiadomości zaszyfrowanej wg powyższej zależności wymagany jest warunek: NWD[1] (m, k) = 1, tzn., aby liczby *m* i *k* były liczbami względnie pierwszymi. Deszyfrowanie oparte jest na przekształceniu:

$$m = E^{-1}\,(\mathrm{c}, \mathrm{k}) = c \cdot k^{-1} \bmod n = c \cdot k^{\varphi(n)-1} \bmod n$$

gdzie $\varphi(n)$ to wartość funkcji Eulera[2]

Przykładowa wartość funkcji Eulera dla $n = 27$ to liczność zbioru {1, 2, 4, 5, 7, 8, 10, 11, 13, 14, 16, 17, 19, 20, 22, 23, 25, 26}. Każdy z elementów tego zbioru jest względnie pierwszy z *n*, a liczność zbioru wynosi 18 i jest to wartość funkcji Eulera.

Przykład 3.2.2

Dany jest tekst jawny: KASA

Klucz: $k = 8$

Indeksując litery tekstu jawnego wg tabeli 3.2.1, otrzymujemy

K	A	S	A
10	0	18	0

A po zastosowaniu przekształcenia $f(\mathrm{m}) = 8 \cdot m \bmod 27$, otrzymujemy kryptogram ZAJA:

Z	A	J	A
26	0	9	0

Przy deszyfrowaniu dla każdej litery szyfrogramu obliczamy k^{-1}. Dla powyższego przykładu $k^{-1} = 8^{\varphi(27)-1} \bmod 27$, a następnie wyznaczyć literę tekstu jawnego stosując przekształcenie $m = c \cdot k^{-1} \bmod 27$.

W przykładzie tym pojawił się problem podniesienia do 18-stej potęgi liczby 8. Rozwiązać to można stosując algorytm potęgowania dyskretnego.

Jeszcze inną odmianą szyfrów monoalfabetycznych jest szyfr wykorzystujący przekształcenie afiniczne postaci:

$$c = f(\mathrm{m}) = (m \cdot r + s) \bmod n$$

---

[1] Najmniejszy wspólny dzielnik liczb *m* i *k*

[2] Funkcja Eulera określa liczbę elementów względnie pierwszych niewiększych niż n. (funkcja Eulera dla liczby całkowitej dodatniej n, określa ilość całkowitych liczb dodatnich mniejszych niż n i względnie pierwszych z n. Mówi się wtedy, ze jest to liczba określająca *wielkość zbioru residuów mod n*. Na przykład zbiór residuów mod 10 to liczby {1,3,7,9}, gdyż nie zawierają one wspólnego dzielnika (różnego od 1) z liczba 10. Zatem φ (n) = 4.

gdzie NWD (r, n) = 1. Kluczem szyfrującym jest w tym przypadku nie pojedyncza liczba, a para liczb $k = (r, s)$.

Szyfry afiniczne są niewiele bardziej skomplikowane jeśli chodzi o próbę ataku na nie. Gdy posiadamy pewien zbiór t zgodności (lub spodziewanych zgodności) pomiędzy elementami tekstu jawnego m_i a elementami krytpogramu c_i dla $1 \leq i \leq t$, to współczynniki r i s klucza można obliczyć z układu równań:

$$m_1 \cdot r + s \bmod n = c_1$$
$$m_2 \cdot r + s \bmod n = c_2$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$
$$m_t \cdot r + s \bmod n = c_t$$

3.2.2 Szyfr AtBash

Szyfr AtBash jest mniej znanym przykładem algorytmów monoalfabetycznych. Litery alfabetu są również indeksowane od 0 do 25. Nie występuje tu natomiast klucz ani przesunięcie, jak w szyfrze Cezara. Szyfrowanie polega na podstawieniu za literę tekstu jawnego odpowiadającej jej litery odwróconego alfabetu, np. literze ‘A’ wiadomości jawnej odpowiada ‘Z’ w szyfrogramie. Można przyjąć alfabet tajny jest odwrotnością alfabetu jawnego, ale indeksowanie odbywa się od lewej do prawej, czyli w tym przypadku od ‘Z’ do ‘A’ (‘Z’ ma indeks 0). Proces szyfrowania jest więc to podstawienie za każdą literę tekstu jawnego litery o tym samym indeksie z alfabetu tajnego.

Przykład 3.2.3
Tablica z alfabetem jawnym:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A

Tekst jawny PROGRAMOWANIE da kryptogram KILTIZNLDZMRV.

Deszyfrowanie odbywa się na identycznej zasadzie jak szyfrowanie: można skorzystać z tej samej tabeli, tyle że dla każdej litery szyfrogramu (trzeci wiersz) szukamy jej odpowiednika (w tej samej kolumnie, wiersz pierwszy).

Kryptoanaliza tego rodzaju szyfru jest banalnie prosta. W przypadku, gdy nie ma pewności, że do zaszyfrowania wiadomości użyto algorytmu Atbash, przydatna może okazać się też analiza częstości występowania znaków.

3.2.3 Szyfr Polibiusza

Szyfr Polibiusza jest przedstawicielem rodziny szyfrów monoalfabetycznych. Zasada jego działania opiera się na specjalnej macierzy o wymiarach 5 × 5. Tablica ta jest wypełniona od góry wierszami najpierw słowem-kluczem, a potem kolejnymi literami alfabetu (poczynając od następnej po ostatniej literze klucza). Żadna litera w tablicy nie może się powtórzyć. Przykładowe wypełnienie pokazuje tabela 3.4:

Tabela 3.4 Przykładowe wypełnienie tablicy 5 × 5 dla szyfru Polibiusza

	1	**2**	**3**	**4**	**5**
1	K	L	U	C	Z
2	A	B	D	E	F
3	G	H	I,J	M	N
4	O	P	Q	R	S
5	T	V	W	X	Y

Jak widać litera ‘J’ jest traktowana jako ‘I’ (jest tylko 25 pól, a 26 liter alfabetu). Szyfrowanie polega na podstawieniu za każdą literę tekstu jawnego dwóch cyfr, będących współrzędnymi kolumny i wiersza, w których przecięciu znajduje się dana litera.

Przykład 3.2.4
Dany jest tekst jawny: SPOTKANIE JEST JUTRO
Szyfrogram otrzymany z użyciem powyższej tablicy ma postać:

54241415111253334233311544 14

Deszyfrowanie przebiega w sposób następujący. Dysponując szyfrogramem i kluczem należy brać kolejne pary cyfr. Każda taka para to współrzędne kolumny i wiersza w tablicy. Na ich przecięciu jest litera tekstu wynikowego.

3.2.4. Szyfr Delastelle'a

Szyfr Delastelle'a należy również do grupy szyfrów monoalfabetycznych. Zasada działania tego algorytmu zbliżona jest do szyfru Polibiusza. Nie jest to przypadek, ponieważ właśnie od tego szyfru się wywodzi. Analogicznie, oparty jest on na tablicy o wymiarach 5 × 5, wypełnionej literami zgodnie z zadanym kluczem. Zachowana zostaje też zasada zamiany litery 'J' na 'I'. O ile w szyfrze Polibiusza kryptogram był dwukrotnie dłuższy od tekstu jawnego i złożony z samych cyfr z przedziału <1, 5> będących indeksami liter z rzeczonej tablicy, o tyle w niniejszym algorytmie taka postać jest jedynie formą przejściową. Sam szyfrogram ma identyczną długość jak tekst jawny i, podobnie jak on, składa się z samych liter. Dokładną zasadę szyfrowania tym sposobem obrazuje następujący przykład.

Niech tabela 5 × 5 ma identyczny wygląd jak tabela 3.4, a słowem szyfrowanym będzie 'LAMPKA'. Pierwszym etapem (po utworzeniu tej tablicy) jest utworzenie tablicy pomocniczej (tabela 3.5) o trzech wierszach i tylu kolumnach, ile liter znajduje się w tekście jawnym. W komórkach pierwszego wiersza znajdują się kolejno wpisywane litery słowa szyfrowanego, w drugim – indeks oznaczający kolumnę w jakiej znajduje się dana litera w tablicy 5 × 5, natomiast w trzecim – indeks odpowiadający wierszowi, w jakim znajduje się litera w tej tablicy.

Tabela 3.5 Tabela pomocnicza w szyfrze Delastelle'a

Tekst:	L	A	M	P	K	A
Kolumna:	2	1	4	2	1	1
Wiersz:	1	2	3	4	1	2

Mając tak przygotowaną tablicę – tworzona zostaje postać pośrednia, na podstawie której dopiero tworzony jest szyfrogram. Postać ta, jak wcześniej wspomniano – to ciąg cyfr o długości dwukrotnie dłuższej od tekstu jawnego, którego składowymi są właśnie cyfry znajdujące się w drugim i trzecim wierszu tabeli 3.5. Wcześniej należy jednak wybrać wariant szyfrowania. Do wyboru są trzy opcje: szyfrowanie poziome, z dołu do góry oraz z góry na

dół. Jako, że odczyt samego kryptogramu odbywa się dla wszystkich opcji identycznie – wybór ten ma wpływ już na wygląd samej postaci pośredniej.

Szyfrowanie poziome jest najprostszym sposobem i sprowadza się jedynie do przepisania wszystkich cyfr do jednego ciągu w takiej kolejności, w jakiej występują litery tekstu jawnego, zważając jednak przy tym na fakt, iż najpierw do ciągu wpisywane są wszystkie litery drugiego wiersza, a dopiero po nich następuje dopisanie do ciągu wszystkich liter z wiersza trzeciego. Tak więc dla tego przykładu postać pośrednia wygląda tak: 214211123412.

Drugi i trzeci sposób są do siebie bardzo zbliżone i zarazem niewiele bardziej skomplikowane od szyfrowania poziomego. Zasada szyfrowania z góry na dół przedstawia się następująco: zaczynając od pierwszej litery słowa szyfrowanego, najpierw do postaci przejściowej wpisywany jest numer kolumny, w jakim znajduje się i-ta litera tekstu jawnego, a następnie numer wiersza, w którym jest litera na pozycji i+1. Przy wyborze szyfrowania z góry na dół ciąg liczb ma postać: 221344211211.

Analogicznie – przy szyfrowaniu z dołu do góry do ciągu cyfry wpisywane się „po skosie", z tą różnicą jednak, że najpierw wpisuje się numer wiersza, w którym położona jest i-ta litera, a następnie numer kolumny, w której jest litera z pozycji i+1. W taki sposób tworzony ciąg cyfr dla słowa 'LAMPKA' przy kluczu 'KLUCZ' wygląda następująco: 112432411122.

Jak już wspomniano powyżej – sam odczytanie szyfrogramu przebiega dla wszystkich wariantów w identyczny sposób. Otóż z postaci przejściowej brane są kolejne pary cyfr i dla każdej z par odczytywana jest litera z tablicy 5 × 5, i następnie wstawiana do szyfrogramu, przy czym pierwsza cyfra w parze oznacza indeks kolumny, a druga – indeks wiersza w jakim dana litera się znajduje. A tak wyglądają kryptogramy, jakie otrzymane zostaną po zaszyfrowaniu algorytmem Delastelle'a każdą z metod:

- szyfrowanie poziome: LEKAQA
- szyfrowanie z góry na dół: BGRLAK
- szyfrowanie z dołu do góry: KPDCKB.

3.2.5 Szyfr homofoniczny

Szyfry homofoniczne odwzorowują każdy znak alfabetu jawnego A w podzbiór znaków alfabetu tajnego B. Wszystkie podzbiory alfabetu tajnego są wzajemnie rozłączne tzn. każdej literze alfabetu A przyporządkowany jest zbiór znaków, z których żaden nie pojawi się w zbiorze odpowiadającym innej literze tego alfabetu. Szyfrowanie polega na tym, że każda litera tekstu jawnego zastępowana jest dowolnym znakiem z odpowiadającego jej zbioru z alfabetu tajnego.

Przykład 3.2.5
Dany jest tekst jawny: ABC, oraz odpowiadające literom ‘A’, ‘B’, ‘C’ zestawy homofonów (resztę liter w tym przykładzie pominięto):

$$f(\mathrm{A}) = \{\%, \&, \mathrm{O}, :, \mathrm{X}, >\}$$
$$f(\mathrm{B}) = \{\mathrm{M}, !\}$$
$$f(\mathrm{C}) = \{\mathrm{V},], -\}$$
$$\ldots$$

Przykładowe kryptogramy mają postać:

&!-
%MV
OM-

Takich trzyliterowych kryptogramów dla powyższego przykładu można otrzymać $6 \cdot 2 \cdot 3 = 36$.

Deszyfrowanie przebiega w sposób jednoznaczny (o ile któryś z homofonów nie występuje w więcej niż jednym podzbiorze alfabetu tajnego). Litery tekstu jawnego otrzymujemy z podstawiania litery alfabetu jawnego, w której uprzednio przypisanym podzbiorze znajduje się aktualnie deszyfrowany znak.

Liczność podzbioru znaków alfabetu tajnego przypisanego określonej literze alfabetu jawnego powinna być uzależniona od częstości występowania tej litery w języku naturalnym. Widać to w powyższym przykładzie. Jeśli stosujemy się do tej zasady przypisując podzbiory do liter, wtedy atak na szyfr poprzez analizę częstości występowania znaków jest prawie że niemożliwy, gdyż rozkład częstości zostaje ukryty. Jednak podstawienia w równie małym stopniu co w prostych szyfrach podstawieniowych ukrywają wewnętrzne regularności języka, w którym napisano wiadomość. Analiza chociażby rozkładu digramów znacznie zwiększa skuteczność ataku.

3.2.6 Szyfr Vigenére'a

Wobec słabości szyfrów monoalfabetycznych próbowano wymyślać bardziej rozbudowane algorytmy. Naturalnym krokiem było wykorzystanie większej ilości alfabetów. Posunięcie to dało początek szyfrom polialfabetycznym. Najbardziej znanym przedstawicielem tej grupy jest właśnie szyfr Vigenére'a. Zasada działania opiera się na szyfrowaniu z użyciem specjalnego hasła (klucza). Każda litera tekstu jawnego szyfrowana jest z pojedynczą literą klucza w sposób identyczny jak w przypadku szyfru Cezara – litery klucza i tekstu jawnego mają przypisane indeksy od 0 do 25 (dodatkowo znak '_' ma indeks 26), które są dodawane a następnie wynik dzielony jest modulo 27, a otrzymana liczba zamieniana jest na literę szyfrogramu. W przypadku, gdy hasło jest krótsze od szyfrowanego tekstu powtarzamy je wielokrotnie.

Przykład 3.2.6
Dany jest tekst jawny: JUTRO POD POMNIKIEM
klucz: MARS

J	U	T	R	O	P	O	D	P	O	M	N	I	K	I	E	M
M	A	R	S	M	A	R	S	M	A	R	S	M	A	R	S	M
V	U	J	I	_	P	E	V	A	O	C	E	U	K	Z	W	Y

Tekst jawny został pozbawiony znaków spacji. Dla pierwszej kolumny obliczenie wygląda następująco: 9 (J) + 12 (M) mod 27 = 21 → V. Otrzymany szyfrogram:

VUJI_PEVAOCEUKZWY

Deszyfrowanie wymaga wpisania w pierwszy wiersz tablicy szyfrogramu, w drugi klucza, w trzecim będzie wpisany otrzymany tekst wynikowy. Przy rozszyfrowywaniu, podobnie jak przy szyfrowaniu, brana jest za każdym razem: jedna litera klucza i jedna litera kryptogramu. Rozróżnić można dwie sytuacje:

- indeks litery szyfrogramu jest większy bądź równy indeksowi litery klucza: wtedy literę tekstu wynikowego można otrzymać z odjęcia indeksów (szyfrogramu od klucza) i podstawienia litery odpowiadającej obliczonej liczbie za literę tekstu wynikowego,
- indeks litery szyfrogramu jest mniejszy od indeksu litery klucza: wtedy indeks litery tekstu wynikowego obliczany jest ze wzoru:

  $$27 - |\text{indeks\_lit\_kryp} - \text{indeks\_lit\_klucza}| \bmod 27,$$

  wynik jest zamieniany na literę tekstu wynikowego.

Oba przypadki rozpatruje szyfr Beauforta, który służy do deszyfrowania tekstu, zaszyfrowanego szyfrem Vigenére'a. Jeśli c traktować jako indeks litery kryptogramu, k_i jako literę klucza a n jako długość alfabetu (czyli w tym przypadku 27), to prawdziwy jest wzór

$$E(m, k_i) = (m - k_i) \bmod n = (m + n - k_i) \bmod n$$

Jeszcze innym algorytmem polialfabetycznym jest szyfr Vernama, przekształcający ciąg zero-jedynkowy w ciąg zero-jedynkowy. Szyfr ten generuje wynikowy ciąg bitów w taki sposób, że tekst jawny jest zamieniany na postać bitową, np. każda litera może być przedstawiona w postaci bitowej powstałej z zamiany wartości decymalnej, odpowiadającej danej literze w tabeli kodów ASCII. Dla przykładu litera 'A' o wartości decymalnej ASCII równej 65 miałaby wtedy postać binarną 1000001. Gdy klucz zostanie przedstawiony również w postaci binarnej, bit tekstu zaszyfrowanego powstaje w wyniku operacji sumowania modulo 2 kolejnych bitów tekstu jawnego i klucza.

Atak na szyfr Vigenére'a i inne polialfabetyczne może być przeprowadzony z użyciem dwóch metod:

- obliczenie indeksu koincydencji,
- wykonanie testu Kasiskiego,

Wykorzystanie obu z nich ma na celu wyznaczenie okresu klucza T, czyli jego długości. Indeks koincydencji określa prawdopodobieństwo wystąpienia w szyfrogramie dwóch jednakowych liter i jest obliczany z zależności [STOK03]:

$$IC = \frac{\sum_{\alpha \in A} F_a (F_a - 1)}{n(n-1)},$$

gdzie F_a jest liczbą wystąpień litery a alfabetu A w tekście o długości n. Obliczona według powyższego wzoru wartość dla konkretnego szyfrogramu może być porównana z wartościami

oczekiwanymi indeksu koincydencji, charakterystycznymi dla konkretnego języka. Język polski ma zupełnie inne wartości indeksu koincydencji niż np. język angielski. Dla tego drugiego wyglądają one następująco [STOK03]:

Tabela 3.6 Wartości oczekiwane indeksu koincydencji dla języka angielskiego

IC	*T*
0,066	1
0,052	2
0,047	3
0,045	4
0,044	5
0,041	10
0,038	b. duże

W lewej kolumnie znajdują się oczekiwane wartości indeksu koincydencji, a w prawej prawdopodobne okresy klucza. Jeśli dla przykładu obliczona z konkretnego szyfrogramu wartość indeksu koincydencji wyniesie 0,051, to spodziewać się można, że długość klucza, jaki użyto do zaszyfrowania, będzie równa 2. Aby jednak wyniki były dokładne konieczna jest duża próba (odpowiednio długi kryptogram).

Inną metodą ułatwiającą wyznaczenie okresu klucza jest test Kasiskiego. Sugeruje on długość klucza na podstawie analizy powtórzeń znaków w szyfrogramie. Kiedy dla losowego tekstu praktycznie nie występują dwa takie same bloki o długości co najmniej trzech znaków, to w tekstach opartych na językach naturalnych zdarza się to bardzo często. Dla przykładu: w języku polskim końcówki –enie, -ówki itp., w języku angielskim słowo ‘the’, końcówki –ally , -tial itp. Test Kasiskiego polega na poszukiwaniu takich właśnie bloków co najmniej trzech znaków i badaniu odstępów pomiędzy nimi w kryptogramie. Jeśli otrzymane dla pewnego bloku odstępy wynoszą: 18, 36, 12, to wtedy okres klucza może wynosić 3 lub 6.

Dysponując prawdopodobną wartością okresu klucza, wyznaczoną jedną z dwóch powyższych metod (lub obydwoma, może wykluczyć błędne obliczenia), należy dobrać grupy wszystkich znaków, które zostały zaszyfrowane tą samą literą klucza. W każdej z tych grup można przeprowadzić atak poprzez analizę częstości występowania znaków, gdyż, grupa taka zaszyfrowana jest z wykorzystaniem zwykłego podstawienia. Sprawdzanie otrzymanych

rezultatów pod względem sensowności treści i kolejne podstawienia powinny dać pożądane rezultaty.

3.2.7 Szyfr Playfaira (podstawowy)

Szyfr Playfaira należy do ostatniej grupy szyfrów podstawieniowych, a mianowicie do szyfrów wieloliterowych, które operują na grupach liter. Ten akurat algorytm działa jednocześnie na parze liter. Szyfrowanie odbywa się z wykorzystaniem tablicy 5 × 5, wypełnionej z zadanym kluczem w identyczny sposób, co w szyfrze Polibiusza. Pokazuje to tabela 3.4. Tekst, który ma być zaszyfrowany, musi najpierw zostać poddany formatowaniu. Operacja ta polega na rozdzieleniu dwóch identycznych znaków w tekście jawnym, leżących koło siebie, znakiem pustym ‘X’. Taki znak jest też wstawiany na koniec tekstu, jeżeli ma on długość nieparzystą. Mając parę znaków wiadomości, która ma być zaszyfrowana, należy postępować wg schematu:

- jeżeli znalezione litery leżą w tym samym wierszu, wtedy za znaki szyfrogramu podstawiane są sąsiednie, leżące na prawo od nich znaki. Przy czym kolumna pierwsza traktowana jest jako leżąca na prawo od piątej,
- jeżeli znalezione litery leżą w tej samej kolumnie, wtedy za znaki szyfrogramu podstawiane są sąsiednie, leżące poniżej znaki. Przy czym wiersz pierwszy jest traktowany jako leżący poniżej piątego,
- jeżeli litery leżą w różnych wierszach i kolumnach, to pierwsza litera szyfrogramu leży w tej samej kolumnie, co odpowiadający jej znak, ale w wierszu o indeksie równym indeksowi wiersza drugiego znaku. Analogicznie wygląda szyfrowaniu drugiego znaku z pary.

Przykład 3.2.7
Dany jest tekst jawny MADONNA

klucz: KAROL

	1	2	3	4	5
1	K	A	R	O	L
2	M	N	P	Q	S
3	T	U	V	W	X
4	Y	Z	B	C	D
5	E	F	G	H	I

Tekst jawny zostaje najpierw poddany formatowaniu: między litery ‘N’ wstawiony został znak pusty ‘X’ – tekst ma teraz postać MADONXNA. Warunek parzystości jest spełniony, więc nie ma konieczności dopisywania znaku pustego na końcu. Szyfrogram otrzymany z użyciem powyższej tablicy wygląda następująco: NKCLSUUN. Podkreślone litery powstały z podstawienia trzeciej pary znaków tekstu jawnego, czyli ‘NX’. Operacja ta jest pokazana za pomocą strzałek na tablicy powyżej.

Deszyfrowanie odbywa się wg podobnego schematu, co szyfrowanie. Jeżeli litery leżą w jednym wierszu to nie ma przesunięcia w prawo, a w lewo; jeżeli leżą w jednej kolumnie to litery tekstu wynikowego powstają z przesunięcia w górę. Natomiast, gdy litery kryptogramu leża w różnych wierszach i kolumnach, to deszyfrowanie byłoby operacją podstawienia odwrotnego do tego, które ukazane jest w powyższej tablicy.

Kryptoanaliza szyfrów wieloliterowych przebiega podobnie jak w przypadku kryptoanalizy prostych szyfrów podstawieniowych – przeprowadza się analizę częstości występowania znaków w tekście. Problem jednak jest taki, że do czynienia ma się w przypadku szyfru Playfaira z digramami, a częstości występowania najpopularniejszych z nich są do siebie bardzo zbliżone. Stąd przydatna jest wiedza na temat wzorców językowych (niektóre digramy niemal nigdy nie występują).

3.2.8 Szyfr Playfaira (II Wojna Światowa)

Szyfr Playfaira w okresie II Wojny Światowej doczekał się ciekawej odmiany. W tej wersji nie ma jednej tablicy 5 × 5, a są dwie. Stąd konieczne jest podanie dwóch (najlepiej

różnych) kluczy. Wypełnienie każdej z nich nie różni się od wypełnienia w podstawowej wersji algorytmu Playfaira. Szyfrowanie jednak wygląda już nieco inaczej. Tekst jawny może zawierać dwie identyczne litery, leżące koło siebie. Natomiast zasada utrzymania parzystości, jeśli chodzi o długość wiadomości, jest przestrzegana. Dlatego przed przystąpieniem do szyfrowania tekstu o nieparzystej liczbie znaków, dodany zostaje do niego na końcu znak pusty ‘X’. Tak sformatowany tekst powinien zostać wpisany do tablicy o dwóch wierszach i długości równej dokładnie połowie długości szyfrowanej wiadomości, w sposób pokazany w tabeli 3.7:

Tabela 3.7 Wypełnianie tabeli pomocniczej tekstem jawnym w szyfrze Playfaira (IIWŚ)

T	E	K	S	T
J	A	W	N	Y

Górny wiersz zawiera litery, z lewej tablicy a w dolnym z prawej. Schemat zaszyfrowania pojedynczej pary liter tekstu jawnego z wykorzystaniem obu tabel głównych i tabeli pomocniczej (powyżej) wygląda następująco:

- wczytanie pary znaków z tabeli pomocniczej (przykładowo TJ),
- jeżeli litery leżą w tych samych wierszach, to litery szyfrogramu powstają z podstawienia sąsiednich, leżących na prawo znaków. Za literę z lewej tablicy podstawiana jest litera z lewej tablicy i analogicznie dla drugiej litery, leżącej w prawej tablicy. Podobne podstawienie stosuje się, gdy litery leża dokładnie w tych samych miejscach w obu tabelach (przecięcie wierszy i kolumn o identycznych indeksach),
- jeżeli litery leża w różnych wierszach, to obie tablice traktować można jako jedną całość tzn. tablicę o wymiarach 10 × 5 i odczytujemy litery szyfrogramu zgodnie z zasadą szyfrowania w podstawowej wersji algorytmu Playfaira.

Należy pamiętać, że odczytane z lewej tablicy (mimo „umownego połączenia”) litery szyfrogramu umieszcza się w górnym wierszu tablicy o identycznych wymiarach, co tabela 3.2.4, a litery z prawej tablicy szyfrującej w dolnym wierszu. Kryptogram powstaje z odczytania wierszami tak powstałej tablicy.

Przykład 3.2.8
Dany jest tekst jawny: WIZYTA GOŚCI JUTRO
klucze: PLAC, KORA

Spacje w tekście jawnym są pomijane, litery ’Ś’ i ‘J’ są zamieniane odpowiednio na ‘S’ i ‘I’. Następnie tekst jawny zostaje wpisany do tabeli pomocniczej:

W	I	Z	Y	T	A	G	O
S	C	I	I	U	T	R	O

Tablice główne wyglądają następująco:

P	L	A	C	D
E	F	G	H	I
K	M	N	O	Q
R	S	T	U	V
W	X	Y	Z	B

K	O	R	A	B
C	D	E	F	G
H	I	L	M	P
Q	R	S	T	U
V	W	X	Y	Z

Otrzymana tablica pomocnicza szyfrogramu ma postać:

R	E	O	N	U	T	A	C
X	D	W	W	P	A	E	I

a kryptogram odczytany wierszami to: REONUTACXDWWPAEI. Komórki o ciemniejszym tle reprezentują parę znaków (pojedynczy krok algorytmu), która zostaję zaszyfrowana (pokazują to strzałki) i uwidoczniona w tablicy pomocniczej z kryptogramem.
Deszyfrowanie przebiega w sposób analogiczny. Kryptoanaliza tej odmiany szyfru Playfaira jest znacznie utrudniona poprzez zatarcie statystycznych zależności pomiędzy kolejnymi parami liter, ponieważ w metodzie tej szyfrowane są znaki oddalone od siebie o *n*, gdzie *n* to długość wiersza w tablicy pomocniczej z tekstem jawnym (w przykładzie *n* jest równe 8).

3.2.9 Szyfr Hilla

Szyfr Hilla jest przedstawicielem grupy szyfrów wieloliterowych. Stanowi on liniowe przekształcenie znaków tekstu jawnego w taką samą liczbę znaków szyfrogramu:

$$c = \begin{bmatrix} m_1 \\ m_2 \\ \vdots \\ m_t \end{bmatrix} \cdot \begin{bmatrix} k_{11} & k_{12} & \cdots & k_{1t} \\ k_{21} & k_{22} & \cdots & k_{2t} \\ \vdots & \vdots & & \vdots \\ k_{t1} & k_{t2} & \cdots & k_{tt} \end{bmatrix} \bmod n = \begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_t \end{bmatrix}$$

Przykład 3.2.9:
Słowo do zaszyfrowania: LUKA

n = 27,

klucz: $k = \begin{bmatrix} 7 & 2 \\ 3 & 5 \end{bmatrix}$

Przy tak skonstruowanym kluczu, słowo LUKA dzieli się na dwa bloki po dwie litery każdy:

$$\begin{bmatrix} L & K \\ U & A \end{bmatrix} = \begin{bmatrix} 12 & 11 \\ 20 & 1 \end{bmatrix}$$

a następnie należy pomnożyć macierz reprezentującą słowo, przez macierz – klucz i dokonać operacji mod *n*:

$$\begin{bmatrix} 12 & 11 \\ 20 & 1 \end{bmatrix} \cdot \begin{bmatrix} 7 & 2 \\ 3 & 5 \end{bmatrix} \bmod 27 = \begin{bmatrix} 9 & 25 \\ 8 & 18 \end{bmatrix} = \begin{bmatrix} I & Y \\ H & R \end{bmatrix}$$

Tak więc szyfrując słowo LUKA szyfrem Hilla przy powyższych parametrach otrzymamy szyfrogram: IHYR.

3.2.10 Szyfr Bacona

Jeden z najciekawszych szyfrów podstawieniowych został stworzony w 1623 roku przez niejakiego Francisa Bacona. Szyfr ten znany jest obecnie jako pięciobitowy szyfr binarny. Algorytm ten w pewnym sensie obejmuje zagadnienia związane z działem kryptografii, jakim jest steganografia. Szyfrogram jest pięciokrotnie dłuższy od tekstu szyfrowanego, a ponadto nie poszczególne litery stanowią o treści szyfrogramu, ale styl jaki ma czcionka, którą litery kryptogramu są zapisane. Bacon zastosował w niniejszym algorytmie dwa rodzaje czcionki: zwykłą oraz pogrubioną. Każda litera tekstu jawnego szyfrowana jest na pięciu literach tła tekstowego. Tabela 3.8 przedstawia sposób szyfrowania

każdej z liter alfabetu, przy czym znak ‘*’ oznacza czcionkę zwykłą, natomiast litera ‘B’ – czcionkę pogrubioną.

Tabela 3.8 Szyfrowania znaków alfabetu w algorytmie Bacona

litera	kod
A	*****
B	****B
C	***B*
D	***BB
E	**B**
F	**B*B
G	**BB*
H	**BBB
I	*B***

litera	kod
J	*B**B
K	*B*B*
L	*B*BB
M	*BB**
N	*BB*B
O	*BBB*
P	*BBBB
Q	B****
R	B***B

litera	kod
S	B**B*
T	B**BB
U	B*B**
V	B*B*B
W	B*BB*
X	B*BBB
Y	BB***
Z	BB**B

Można by to także zapisać w postaci zerojedynkowej, gdzie zero oznaczałoby zwykłą czcionkę, natomiast jeden – czcionkę pogrubioną. Wtedy kod dla litery ‘A’ miałby wartość zero zapisaną w postaci binarnej na pięciu bitach, kod litery ‘B’ – wartość jeden, ‘C’ – dwa, itd.

Natomiast samą zasadę działania szyfru Bacona najlepiej obrazuje przykład 3.2.10.

Przykład 3.2.10
Słowo do zaszyfrowania: DOM

Tło tekstowe: Jutro jadę do domu

Tło tekstowe dzieli się na bloki pięcioliterowe, a następnie ich styl czcionki zmienia na pogrubiony – tak jak wymaga tego kod danej litery.

Tekst jawny: D O M

Szyfrogram: **Ju**t**ro** j**adę**d o**do**mu

Podobnie w przypadku deszyfrowania – należy podzielić szyfrogram na pięcioliterowe bloki znaków i zgodnie z kluczem zamieniać poszczególne bloki na pojedyncze litery tekstu jawnego. Jak widać w przykładzie – to nie sama treść tła tekstowego zawiera w sobie

zaszyfrowane słowo, ale sposób w jaki poszczególne litery tła tekstowego zostały zapisane do szyfrogramu – które z nich zostały wpisane zwykłą czcionką, a które pogrubioną.