(wyjaśnienia pojęć z wykładu – opisy z wikipedii)

Szyfr Cezara – w kryptografii jedna z najprostszych technik szyfrowania. Jest to rodzaj szyfru podstawieniowego, w którym każda litera tekstu jawnego (niezaszyfrowanego) zastępowana jest oddaloną od niej o stałą liczbę pozycji w alfabecie inną literą, przy czym kierunek zamiany musi być zachowany. Nie rozróżnia się przy tym liter dużych i małych. Nazwa szyfru pochodzi od Juliusza Cezara, który prawdopodobnie używał tej techniki do komunikacji ze swymi przyjaciółmi.

Alfabet:	AĄBCĆDEĘFGHIJKLŁMNŃOÓPRSŚTUWYZŹŻ	Tekst:	ALA MA KOTA
Szyfr:	CĆDEĘFGHIJKLŁMNŃOÓPRSŚTUWYZŹŻAĄB	Szyfrogram:	CNC OC MRYC

Słownie	Matematycznie:
Klucz - o ile przesuwamy	k
Szyfrowanie – przesunięcie w prawo o tyle liter ile w kluczu	$E_k(x) \equiv x+n \pmod{32}$
Deszyfrowanie – przesunięcie w lewo o tyle liter ile w kluczu	$D_k(x) \equiv x-n \pmod{32}$

Ćwiczenie 1
Szyfr nie jest bezpieczny jeśli, zbiór możliwych wiadomości jest mały, a na dodatek stosuje się do zakodowania każdej z nich tego samego klucza...
Mamy wiadomości : TAK, NIE, NIE WIEM
i szyfrogramy : ÓLG, ÓLGXŹLGO, YCM
Który szyfrogram odpowiada, której wiadomości? Jaki klucz zastosowano?
W tym szyfrze jak w Enigmie – spację zastąpiono symbolem X. Bywa też, że spacje się pomija.

Ćwiczenie 2
Znajomość treści kodowanej wiadomości pozwala na lepsze ataki na metodę szyfrowania. Tak było z niemieckimi meldunkami podczas II wojny światowej, których schematyczność pozwoliła na lepsze łamanie Enigmy.

1) Wiemy, że wiadomość zaczyna się w następujący sposób: „CZESC...”
2) Wiemy, że szyfrowanie jest metodą Cezara na alfabecie:
   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
3) Co kryje się pod szyfrogramem:
   VSXLV IHSRVS LMHPDX
4) Jakiego klucza użyto do zakodowania tej wiadomości?

Ćwiczenie 3
Jednym z najprostszych, ale jednocześnie najbardziej czasochłonnych ataków, jest atak *brute-force*. Polega on na sprawdzeniu wszystkich kombinacji szyfrowania. Próbuje się kolejno wszystkie wartości klucza, odszyfrowuje i sprawdza czy wiadomość ma jakiś sens.

1) Wiemy, że szyfrowanie jest metodą Cezara na alfabecie:
   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

Rozszyfruj komendy:

2) DWDNRZDF
3) YGMIOEG
4) RTBGITWRQYCE
5) GWTSNH

Szyfr Vigenère'a - Działanie szyfru Vigenere'a oparte jest na następującej tablicy:

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

Jak można zauważyć, każdy z wierszy tablicy odpowiada szyfrowi Cezara, przy czym w pierwszym wierszu przesunięcie wynosi 0, w drugim 1 itd.

Aby zaszyfrować pewien tekst, potrzebne jest słowo kluczowe. Słowo kluczowe jest tajne i mówi, z którego wiersza (lub kolumny) należy w danym momencie skorzystać.

Przypuśćmy, że chcemy zaszyfrować prosty tekst, np.: TO JEST BARDZO TAJNY TEKST

Do tego celu użyjemy znanego tylko nam słowa kluczowego, np. TAJNE

Na początku zauważamy, że użyte słowo kluczowe jest zbyt krótkie, by wystarczyło do zaszyfrowania całego tekstu, więc należy użyć jego wielokrotności. Będzie to miało następującą postać:

```
TO JEST BARDZO TAJNY TEKST
TA JNET AJNETA JNETA JNETA
```

Następnie wykonujemy szyfrowanie w następujący sposób: litera szyfrogramu odpowiada literze z tabeli znajdującej się na przecięciu wiersza, wyznaczanego przez literę tekstu jawnego i kolumny wyznaczanej przez literę słowa kluczowego, np. po kolei T i T daje M, O i A daje O itd. W efekcie otrzymujemy zaszyfrowany tekst:

```
MO SRWM BJEHSO CNNGY CROLT
```

Odszyfrowywanie przebiega bardzo podobnie. Bierzemy kolejne litery szyfrogramu oraz odpowiadające im litery słowa kluczowego (podobnie, jak przy szyfrowaniu). Wybieramy kolumnę odpowiadającą literze słowa kluczowego. Następnie w tej kolumnie szukamy litery szyfrogramu. Numer wiersza odpowiadający znalezionej literze jest numerem litery tekstu jawnego. Np. w kolumnie T litera M znajduje się w wierszu T, w kolumnie A litera O znajduje się w wierszu O itd.

Szyfr Vernama – szyfr idealny; z kluczem jednorazowym (*one-time pad*); do dziś używany w miejscach wymagających szczególnego bezpieczeństwa;

wiadomość jest postaci ciągu 0 i 1 np. 10101110
klucz jest ciągiem 0 i 1 równym wiadomości losowo wygenerowanym np. 00011010

szyfrowanie i deszyfrowanie to operacja dodawania klucza metodą modulo 2 na każdej z pozycji, przykładowo:

szyfrowanie		operacje mod 2	deszyfrowanie	
wiadomość	10101110	0+0 = 0 (mod 2)	szyfrogram	10110100
klucz	00011010	1+0 = 0+1 = 1 (mod 2)	klucz	00011010
szyfrogram	10110100	1+1 = 0 (mod 2)	wiadomość	10101110

Metoda generacji i użycia klucza kryptograficznego wymaga by:
1. Klucz użyty do szyfrowania wiadomości był dłuższy lub równy szyfrowanej wiadomości.
2. Klucz musi być wygenerowany w sposób całkowicie losowy (nie może istnieć sposób na odtworzenie klucza na podstawie znajomości działania generatorów liczb pseudolosowych).
3. Klucz nie może być użyty do zaszyfrowania więcej niż jednej wiadomości.

Uwagi:
ad 3) Ćwiczenie 1 obrazuje, czemu tak ważne jest stosowanie za każdym razem innego klucza.
ad 1) skoro, za każdym razem szyfrujemy innym kluczem, oznacza to, że kluczy musi istnieć przynajmniej tyle samo, co możliwych wiadomości, aby to było możliwe muszą być co najmniej tak samo długie;

Przypomnienie: **Tw ([Sha49])** Jesli szyfr jest idealnie tajny, to |K| >= |M|.
|K| - oznacza tu moc, czyli liczność zbioru możliwych kluczy,
a |M| wiadomości, które można kodować

!!! Tej metody nie da się złamać prezentowaną w Ćwiczeniu 3 metodą *brute-force* !!!

System binarny (dwójkowy) a system dziesiętny
Zapis w systemie dziesiątkowym: $87 = 8 \cdot 10^1 + 7 \cdot 10^0$
Zamiana przebiega następująco:
szukam największą potęgę 2 mniejszą od danej liczby 87 – $2^6 = 23$ (na „2 do 6" pozycji jest 1)
i znowu 23 - $2^4 = 7$ (na „do 4" jest 1) potem 7 – 4 = 3 (na „do 2"); 3 – 2 = 1 (na „do 1");
1-1 = 0 (na „do 0") Kończymy jak otrzymamy 0, może to nastąpić wcześniej, w pozostałe pozycje wpisujemy 0;
zatem 87 w systemie dwójkowym $87 = 0 \cdot 2^7 + 1 \cdot 2^6 + 0 \cdot 2^5 + 1 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0$ to 1010111

komputer działa w tym systemie binarnym; jednym ze sposobów kodowania jest kod ASCII;
Dla liter mamy odpowiednio:

65- A	66 - B	67 - C	68 - D	69 - E		70 - F
71 - G	72 - H	73 - I	74 - J	75 - K		76 - L
77 - M	78 - N	79 - O	80 - P	81 - Q		82 - R
83 - S	84 - T	85 - U	86 - V	87 - W	88 - X	89 - Y	90 - Z

Mamy zatem W → 87 → 01010111

Ćwiczenie 4
Jako szyfrujący:
a) otrzymujesz parę – wiadomość, tajne słowo – szyfrujesz wiadomość za pomocą tego słowa szyfrem Vigenère'a
b) otrzymujesz parę – wiadomość, klucz – zamieniasz wiadomość na ciąg zer i jedynek (dla każdej litery odnajdujesz jej kod ASCII i zapisujesz go w systemie binarnym tak aby zapis dla każdej litery składał się z 8 cyfr – dodaj ewentualnie 0 z przodu), stosując klucz szyfrem Vernama kodujesz wiadomość;
zestaw I:
JEDEN, ZSRR
MOSKWA, 10110101 01010010 10111010 11010101 00011100 11010001
zestaw II:
DRUGI, ZSRR
IRKUCK, 01101010 10101010 00010101 11101010 10101010 01010100
zestaw III:
JEDEN, USA
BOSTON, 10110011 01011110 10100010 11000101 01011100 11110001
zestaw IV:
DRUGI, USA
SEATLE, 01101000 10100100 00010111 11001010 10101011 01011000

Jako deszyfrujący:
a) za pomocą tajnego słowa odszyfrowujesz szyfrogram literowy za pomocą szyfru Vigenère'a,
b) znając treść pierwszej wiadomości wiesz z którego klucza skorzystać; zrób to dla drugiej wiadomości zaszyfrowanej szyfrem Vernama
Zestaw A (odpowiada zestawom I i II)
tajne słowo → ZSRR
klucz pierwszy 10110101 01010010 10111010 11010101 00011100 11010001
klucz drugi 01101010 10101010 00010101 11101010 10101010 01010100

Zestaw B (odpowiada zestawom III i IV)
tajne słowo → USA
klucz pierwszy 10110011 01011110 10100010 11000101 01011100 11110001
klucz drugi 01101000 10100100 00010111 11001010 10101011 01011000

Ćwiczenie 5
Atak *men-in-the-middle* polegać może na tym, że przechwytujemy i zmieniamy wiadomość.
A(licja) może wysyłać wiadomość do B(anku) o treści "wpłać moje pieniądze na konto_Alicji".
E(wa) przechwytuje wiadomość i zmienia ją na "wpłać moje pieniądze na konto_Ewy", wprowadzając Bank w błąd że niby jest Alicją.
Zakładamy, że stosowany jest szyfr Vernama, oraz że Ewa zna wiadomość i przechwyciła jej szyfrogram wysłany przez Alicję. W jaki sposób ma zaszyfrować swoją wiadomość, tak aby Bank po odszyfrowaniu otrzymał to co chce Ewa.

Rozwiązanie:
wystarczy dodać to co wiemy z tym co chcemy uzyskać, czyli zastosować operacje:
$c \oplus m \oplus m1$ gdzie symbol plusa w kółku oznacza szyfrowanie Vernama – dodawanie bit po bicie (czyli pozycja po pozycji metodą mod 2); c to szyfrogram a m to wiadomość Alicji; m1 wiadomość Ewy;
Bank wykonuje następującą czynność:
$c1 \oplus k = c \oplus m \oplus m1 \oplus k = m \oplus k \oplus m \oplus m1 \oplus k = m1$