Szyfr Cezara. Kółko Informatyczne, 20 marca 2012

Jest to szyfr za pomocą którego Juliusz Cezar szyfrował swoje listy do Cycerona. Jako ciekawostkę można podać, że szyfr ten był podobno używany jeszcze w 1915 roku w armii rosyjskiej, gdyż tylko tak prosty szyfr wydawał się zrozumiały dla sztabowców[1].

Wersja podstawowa: Każdą literę tekstu jawnego zamieniamy na literę przesuniętą o 3 miejsca w prawo. I tak literę A szyfrujemy jako literę D, literę B jako E itd. W przypadku litery Z wybieramy literę C. W celu odszyfrowania tekst powtarzamy operację tym razem przesuwając litery o 3 pozycje w lewo.

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
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

Przykład: szyfrujemy zdanie „**Lubię szkołę**”. Po pierwsze – w naszym alfabecie (patrz tabela) nie ma wielkich liter, polskich znaków i spacji. Dlatego będziemy szyfrować tekst „**lubieszkole**”. Przesunięcia odczytujemy z tabeli: l → o, u → x, b → e, i → l, e → h, s → v, z → c, k → n, o → r, l → o, e → h. Otrzymujemy napis „**oxelhvcnroh**”.

Zauważ, w jaki sposób zaszyfrowaliśmy literę **z**: ponieważ nie było liter na prawo od z zaczęliśmy znów od początku tabeli (alfabet się „zawinął”).

Ćwiczenie: zaszyfruj swoje imię i nazwisko za pomocą szyfru Cezara.

Wersja rozszerzona: Wybieramy hasło (klucz) szyfrowania. Przykładowo, niech kluczem tym będzie słowo CEZAR. Litery klucza mają swoje pozycje w alfabecie: 2, 4, 25, 0, 17. Kolejne litery szyfrowanego tekstu będziemy kolejno przesuwać o 2, 4, 25, 0, 17, 2, 4, 25, … pozycji w prawo (zamiast o trzy – odległość przesunięcia wyznaczana jest za pomocą klucza).

Przykład: Szyfrogram „**pmdzxchzmjkiymrvilakaozuncdzmqgwtmrbiqdrlifrfbrzlzedae** ” powstał za pomocą szyfru Cezara. Kluczem było słowo „**cezar**”. Odszyfrowujemy:

P – C = 15 - 2 = 14 = **N** M – E = 12 – 4 = 8 = **I** D – Z = 3 – 25 = **-22**

Co zrobić z -22? Chodzi o literę o 22 miejsca w lewo od litery a. Alfabet znowu się zawija! Pierwszą literą na lewo od a jest z; drugą y = z – 1; trzecią x = z – 2; … dwudziestą drugą wyznaczymy odejmując od z = 25 liczbę 21 – jest to czwarta litera, czyli **E**!

Odszyfrowaliśmy w ten sposób pierwsze trzy litery tekstu: **NIE**.

Postępując podobnie odczytamy całość:

niezgadamsiezmatematykauwazamzesumazerdajegroznaliczbe

Ćwiczenie: wykorzystując jako klucz swoje imię zaszyfruj następującą sentencję pochodzącą od Hugona Steinhausa:

Matematyk zrobi to lepiej.

1 http://www.kryptografia.com/algorytmy/cezar.html

1. Przeczytaj uważnie poniższy program. Za chwilę będziesz musiał wyjaśnić pozostałym jego działanie (linijka po linijce).

```
string s;

cout << "Podaj tekst do zaszyfrowania: ";
getline(cin, s);

cout << "Zaszyfrowany tekst: ";

for (int i = 0; i < s.length(); i++) {
      char c = s[i];

      c = c + 3;
      if (c > 'z') { c = c - 26; }

      cout << c;
}
cout << endl;
```

   Uwaga: `getline? length?` „Google is your friend”

2. Gdy wszystkie programy zostaną objaśnione, kod tego programu znajdziesz na stronie

   `http://www.mimuw.edu.pl/~amn/20marca/`

   w pliku szyfr1.cpp. Zapisz ten kod i zmodyfikuj tak, by Twój program mógł szyfrować i odszyfrowywać napisy. Program na początku pyta o to, czy użytkownik chce szyrować czy odszyfrowywać napis.

3. Wyzwanie, które po napisaniu programów podejmiemy wspólnie:

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

Uwaga: szyfrogram pochodzi z książki J. Verne „2000 mil po Amazonce”, z **angielskiego** tłumaczenia. Możesz założyć, że jest on zaszyfrowany rozszerzonym szyfrem Cezara. Spróbujemy razem znaleźć klucz do tego szyfru!

Szyfr Cezara. Kółko Informatyczne, 20 marca 2012

Jest to szyfr za pomocą którego Juliusz Cezar szyfrował swoje listy do Cycerona. Jako ciekawostkę można podać, że szyfr ten był podobno używany jeszcze w 1915 roku w armii rosyjskiej, gdyż tylko tak prosty szyfr wydawał się zrozumiały dla sztabowców[2].

Wersja podstawowa: Każdą literę tekstu jawnego zamieniamy na literę przesuniętą o 3 miejsca w prawo. I tak literę A szyfrujemy jako literę D, literę B jako E itd. W przypadku litery Z wybieramy literę C. W celu odszyfrowania tekst powtarzamy operację tym razem przesuwając litery o 3 pozycje w lewo.

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
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

Przykład: szyfrujemy zdanie „**Lubię szkołę**”. Po pierwsze – w naszym alfabecie (patrz tabela) nie ma wielkich liter, polskich znaków i spacji. Dlatego będziemy szyfrować tekst „**lubieszkole**”. Przesunięcia odczytujemy z tabeli: l → o, u → x, b → e, i → l, e → h, s → v, z → c, k → n, o → r, l → o, e → h. Otrzymujemy napis „**oxelhvcnroh**”.

Zauważ, w jaki sposób zaszyfrowaliśmy literę **z**: ponieważ nie było liter na prawo od z zaczęliśmy znów od początku tabeli (alfabet się „zawinął”).

Ćwiczenie: zaszyfruj swoje imię i nazwisko za pomocą szyfru Cezara.

Wersja rozszerzona: Wybieramy hasło (klucz) szyfrowania. Przykładowo, niech kluczem tym będzie słowo CEZAR. Litery klucza mają swoje pozycje w alfabecie: 2, 4, 25, 0,17. Kolejne litery szyfrowanego tekstu będziemy kolejno przesuwać o 2, 4, 25, 0,17, 2, 4, 25, … pozycji w prawo (zamiast o trzy – odległość przesunięcia wyznaczana jest za pomocą klucza).

Przykład: Szyfrogram „**pmdzxchzmjkiymrvilakaozuncdzmqgwtmrbiqdrlifrfbrzlzedae** ” powstał za pomocą szyfru Cezara. Kluczem było słowo „**cezar**”. Odszyfrowujemy:

P – C = 15 - 2 = 14 = **N** M – E = 12 – 4 = 8 = **I** D – Z = 3 – 25 = **-22**

Co zrobić z -22? Chodzi o literę o 22 miejsca w lewo od litery a. Alfabet znowu się zawija! Pierwszą literą na lewo od a jest z; drugą y = z – 1; trzecią x = z – 2; … dwudziestą drugą wyznaczymy odejmując od z = 25 liczbę 21 – jest to czwarta litera, czyli **E**!

Odszyfrowaliśmy w ten sposób pierwsze trzy litery tekstu: **NIE**.

Postępując podobnie odczytamy całość:

niezgadamsiezmatematykauwazamzesumazerdajegroznaliczbe

Ćwiczenie: wykorzystując jako klucz swoje imię zaszyfruj następującą sentencję pochodzącą od Hugona Steinhausa:

Matematyk zrobi to lepiej.

2 http://www.kryptografia.com/algorytmy/cezar.html

1. Przeczytaj uważnie poniższy program. Za chwilę będziesz musiał wyjaśnić pozostałym jego działanie (linijka po linijce).

```
string s;
string alfabet = "abcdefghijklmnopqrstuvwxyz";
string doidehw = "defghijklmnopqrstuvwxyzabc";

cout << "Podaj tekst do zaszyfrowania: ";
getline(cin, s);
cout << "Zaszyfrowany tekst: ";

for (int i = 0; i < s.length(); i++) {
      char c = s[i];
      char f = '*';

      for (int j = 0; j < alfabet.length(); j++) {
            if (alfabet[j] == c) {
                  f = doidehw[j];
            }
      }
      cout << f;
}
```

   Uwaga: `getline? length?` „Google is your friend”

2. Gdy wszystkie programy zostaną objaśnione, kod tego programu znajdziesz na stronie `http://www.mimuw.edu.pl/~amn/20marca/` w pliku szyfr2.cpp. Zapisz ten kod i zmodyfikuj tak, by Twój program mógł szyfrować i odszyfrowywać napisy. Program na początku pyta o to, czy użytkownik chce szyrować czy odszyfrowywać napis.

4. Wyzwanie, które po napisaniu programów podejmiemy wspólnie:

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

Uwaga: szyfrogram pochodzi z książki J. Verne „2000 mil po Amazonce”, z **angielskiego** tłumaczenia. Możesz założyć, że jest on zaszyfrowany rozszerzonym szyfrem Cezara. Spróbujemy razem znaleźć klucz do tego szyfru!

Szyfr Cezara. Kółko Informatyczne, 20 marca 2012

Jest to szyfr za pomocą którego Juliusz Cezar szyfrował swoje listy do Cycerona. Jako ciekawostkę można podać, że szyfr ten był podobno używany jeszcze w 1915 roku w armii rosyjskiej, gdyż tylko tak prosty szyfr wydawał się zrozumiały dla sztabowców[3].

Wersja podstawowa: Każdą literę tekstu jawnego zamieniamy na literę przesuniętą o 3 miejsca w prawo. I tak literę A szyfrujemy jako literę D, literę B jako E itd. W przypadku litery Z wybieramy literę C. W celu odszyfrowania tekst powtarzamy operację tym razem przesuwając litery o 3 pozycje w lewo.

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
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

Przykład: szyfrujemy zdanie „**Lubię szkołę**”. Po pierwsze – w naszym alfabecie (patrz tabela) nie ma wielkich liter, polskich znaków i spacji. Dlatego będziemy szyfrować tekst „**lubieszkole**”. Przesunięcia odczytujemy z tabeli: l → o, u → x, b → e, i → l, e → h, s → v, z → c, k → n, o → r, l → o, e → h. Otrzymujemy napis „**oxelhvcnroh**”.

Zauważ, w jaki sposób zaszyfrowaliśmy literę **z**: ponieważ nie było liter na prawo od z zaczęliśmy znów od początku tabeli (alfabet się „zawinął”).

Ćwiczenie: zaszyfruj swoje imię i nazwisko za pomocą szyfru Cezara.

Wersja rozszerzona: Wybieramy hasło (klucz) szyfrowania. Przykładowo, niech kluczem tym będzie słowo CEZAR. Litery klucza mają swoje pozycje w alfabecie: 2, 4, 25, 0, 17. Kolejne litery szyfrowanego tekstu będziemy kolejno przesuwać o 2, 4, 25, 0, 17, 2, 4, 25, … pozycji w prawo (zamiast o trzy – odległość przesunięcia wyznaczana jest za pomocą klucza).

Przykład: Szyfrogram „**pmdzxchzmjkiymrvilakaozuncdzmqgwtmrbiqdrlifrfbrzlzedae** ” powstał za pomocą szyfru Cezara. Kluczem było słowo „**cezar**”. Odszyfrowujemy:

P – C = 15 - 2 = 14 = **N** M – E = 12 – 4 = 8 = **I** D – Z = 3 – 25 = **-22**

Co zrobić z -22? Chodzi o literę o 22 miejsca w lewo od litery a. Alfabet znowu się zawija! Pierwszą literą na lewo od a jest z; drugą y = z – 1; trzecią x = z – 2; … dwudziestą drugą wyznaczymy odejmując od z = 25 liczbę 21 – jest to czwarta litera, czyli **E**!

Odszyfrowaliśmy w ten sposób pierwsze trzy litery tekstu: **NIE**.

Postępując podobnie odczytamy całość:

niezgadamsiezmatematykauwazamzesumazerdajegroznaliczbe

Ćwiczenie: wykorzystując jako klucz swoje imię zaszyfruj następującą sentencję pochodzącą od Hugona Steinhausa:

Matematyk zrobi to lepiej.

3 http://www.kryptografia.com/algorytmy/cezar.html

1. Przeczytaj uważnie poniższy program. Za chwilę będziesz musiał wyjaśnić pozostałym jego działanie (linijka po linijce).

```
string s,k;

cout << "Podaj tekst do zaszyfrowania: "; getline(cin, s);
cout << "Podaj klucz (hasło): "; getline(cin, k);

cout << "Zaszyfrowany tekst: ";

for (int i = 0; i < s.length(); i++) {
      unsigned char c = s[i];
      unsigned char p = k[i % k.length()] - 'a';

      c = c + p;
      if (c > 'z') { c = c - 26; }

      cout << c;
}
cout << endl;
```

   Uwaga: `getline? length?` „Google is your friend”

2. Gdy wszystkie programy zostaną objaśnione, kod tego programu znajdziesz na stronie `http://www.mimuw.edu.pl/~amn/20marca/` w pliku szyfr3.cpp. Zapisz ten kod i zmodyfikuj tak, by Twój program mógł szyfrować i odszyfrowywać napisy. Program na początku pyta o to, czy użytkownik chce szyrować czy odszyfrowywać napis.

3. Wyzwanie, które po napisaniu programów podejmiemy wspólnie:

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

Uwaga: szyfrogram pochodzi z książki J. Verne „2000 mil po Amazonce”, z **angielskiego** tłumaczenia. Możesz założyć, że jest on zaszyfrowany rozszerzonym szyfrem Cezara. Spróbujemy razem znaleźć klucz do tego szyfru!