W poszukiwaniu szyfru indealnego

Piotr Fulmański

piotr@fulmanski.pl
http://fulmanski.pl/tutorials/computer-science/computer-science-for-beginners/w-poszukiwaniu-szyfru-idealnego/

10 kwietnia 2019

Table of contents

Na przestrzeni stuleci narzędzia służące do zmiany informacji z czytelnej postaci na nieczytelną i na odwrót, zmieniały się wraz z rozwojem naukowym, technicznym i ogólnym wzrostem świadomości tego zagadnienia.

Język jako szyfr

- Wojna sześciodnowa (5 czerwca 1967 – 10 czerwca 1967)
  - Wojna sześciodniowa – historyczny sukces Izraela
  - Wojna szesciodniowa – jak to bylo mozliwe...?
- Historia amerykańskich *code talkers*, Indian używających m.in. języka nawaho do szyfrowanej komunikacji podczas II wojny światowej na Pacyfiku jest już dobrze znana, opowiedziana m.in. w filmie *The Windtalkers* z 2002 r. **Indianie nie stworzyli szyfru. Oni porozumiewali się swoim, tylko sobie znanym, językiem.**
  - Indiański szyfr, którego nie złamali Niemcy
  - Indiańscy szyfranci
- Kamień z Rosetty.
  Na kamieniu wyryty został tekst dwujęzyczny w trzech wersjach — po egipsku pismem hieroglificznym i demotycznym oraz po grecku. Tekst zapisany greką został szybko odczytany przez filologów. Ponieważ tekst grecki był znany, możliwe stało się odczytanie hieroglifów, czego dokonali w 1822 roku Jean-François Champollion i w 1823 roku Thomas Young.

Język jako szyfr

- Wojna sześciodnowa (5 czerwca 1967 – 10 czerwca 1967)
  - Wojna sześciodniowa – historyczny sukces Izraela
  - Wojna szesciodniowa – jak to bylo mozliwe...?
- Historia amerykańskich *code talkers*, Indian używających m.in. języka nawaho do szyfrowanej komunikacji podczas II wojny światowej na Pacyfiku jest już dobrze znana, opowiedziana m.in. w filmie *The Windtalkers* z 2002 r. **Indianie nie stworzyli szyfru. Oni porozumiewali się swoim, tylko sobie znanym, językiem.**
  - Indiański szyfr, którego nie złamali Niemcy
  - Indiańscy szyfranci
- Kamień z Rosetty.
  Na kamieniu wyryty został tekst dwujęzyczny w trzech wersjach — po egipsku pismem hieroglificznym i demotycznym oraz po grecku. Tekst zapisany greką został szybko odczytany przez filologów. Ponieważ tekst grecki był znany, możliwe stało się odczytanie hieroglifów, czego dokonali w 1822 roku Jean-François Champollion i w 1823 roku Thomas Young.

Język jako szyfr

- Wojna sześciodnowa (5 czerwca 1967 – 10 czerwca 1967)
  - Wojna sześciodniowa – historyczny sukces Izraela
  - Wojna szesciodniowa – jak to bylo mozliwe...?
- Historia amerykańskich *code talkers*, Indian używających m.in. języka nawaho do szyfrowanej komunikacji podczas II wojny światowej na Pacyfiku jest już dobrze znana, opowiedziana m.in. w filmie *The Windtalkers* z 2002 r. **Indianie nie stworzyli szyfru. Oni porozumiewali się swoim, tylko sobie znanym, językiem.**
  - Indiański szyfr, którego nie złamali Niemcy
  - Indiańscy szyfranci
- Kamień z Rosetty.
  Na kamieniu wyryty został tekst dwujęzyczny w trzech wersjach — po egipsku pismem hieroglificznym i demotycznym oraz po grecku. Tekst zapisany greką został szybko odczytany przez filologów. Ponieważ tekst grecki był znany, możliwe stało się odczytanie hieroglifów, czego dokonali w 1822 roku Jean-François Champollion i w 1823 roku Thomas Young.

Język jako szyfr

- Wojna sześciodnowa (5 czerwca 1967 – 10 czerwca 1967)
  - Wojna sześciodniowa – historyczny sukces Izraela
  - Wojna szesciodniowa – jak to bylo mozliwe...?
- Historia amerykańskich *code talkers*, Indian używających m.in. języka nawaho do szyfrowanej komunikacji podczas II wojny światowej na Pacyfiku jest już dobrze znana, opowiedziana m.in. w filmie *The Windtalkers* z 2002 r. **Indianie nie stworzyli szyfru. Oni porozumiewali się swoim, tylko sobie znanym, językiem.**
  - Indiański szyfr, którego nie złamali Niemcy
  - Indiańscy szyfranci
- Kamień z Rosetty.
  Na kamieniu wyryty został tekst dwujęzyczny w trzech wersjach — po egipsku pismem hieroglificznym i demotycznym oraz po grecku. Tekst zapisany greką został szybko odczytany przez filologów. Ponieważ tekst grecki był znany, możliwe stało się odczytanie hieroglifów, czego dokonali w 1822 roku Jean-François Champollion i w 1823 roku Thomas Young.

- **Zalety:**
  - Łatwość użycia (przy założeniu uprzedniej znajomości języka).
- **Wady:**
  - Duża podatność na złamanie szyfru.

Wniosek 1

"Szyfrowanie" przez ukrywanie może być skuteczne, ale z pewnością jest bardzo ryzykowne.

- **Zalety:**
  - Łatwość użycia (przy założeniu uprzedniej znajomości języka).
- **Wady:**
  - Duża podatność na złamanie szyfru.

Wniosek 1

"Szyfrowanie" przez ukrywanie może być skuteczne, ale z pewnością jest bardzo ryzykowne.

Kodowanie

Kodowanie to szczególny rodzaj tajnego przekazu, który z biegiem wieków stopniowo wychodził z użycia, polegający on na zastąpieniu całych słów lub zwrotów innym słowem, liczbą lub symbolem. Na przykład komunikat

Prezes założył marynarkę. Czeka na auto.

może oznaczać

Oddział komandosów zajął pozycje. Oczekuje na rozkaz rozpoczęcia ataku.

Kodowanie

Kodowanie to szczególny rodzaj tajnego przekazu, który z biegiem wieków stopniowo wychodził z użycia, polegający on na zastąpieniu całych słów lub zwrotów innym słowem, liczbą lub symbolem. Na przykład komunikat

Prezes założył marynarkę. Czeka na auto.

może oznaczać

Oddział komandosów zajął pozycje. Oczekuje na rozkaz rozpoczęcia ataku.

Kodowanie

Kodowanie to szczególny rodzaj tajnego przekazu, który z biegiem wieków stopniowo wychodził z użycia, polegający on na zastąpieniu całych słów lub zwrotów innym słowem, liczbą lub symbolem. Na przykład komunikat

Prezes założył marynarkę. Czeka na auto.

może oznaczać

Oddział komandosów zajął pozycje. Oczekuje na rozkaz rozpoczęcia ataku.

- **Zalety:**
  - Nie ma możliwości "odszyfrowania" takiego przekazu. Pod zwrotem A może być "zaszyfrowany" dowolny zwrot B, zależnie od przyjętej umowy.
- **Wady:**
  - Zdolność do przekazywania informacji ograniczona jedynie do wcześniej ustalonego zbioru "komunikatów" – brak uniwersalności.
  - Konieczność aktualizacji zbioru dopuszczalnych kodów.

Wniosek 2

Metoda szyfowania powinna być tak ogólna jak tylko jest to możliwe, pozwalając szyfrować dowolne komunikaty.

- **Zalety:**
  - Nie ma możliwości "odszyfrowania" takiego przekazu. Pod zwrotem A może być "zaszyfrowany" dowolny zwrot B, zależnie od przyjętej umowy.
- **Wady:**
  - Zdolność do przekazywania informacji ograniczona jedynie do wcześniej ustalonego zbioru "komunikatów" – brak uniwersalności.
  - Konieczność aktualizacji zbioru dopuszczalnych kodów.

Wniosek 2

Metoda szyfowania powinna być tak ogólna jak tylko jest to możliwe, pozwalając szyfrować dowolne komunikaty.

Szyfrowanie dziś

- *Szyfry* zamiast *kodów*.
- Działamy na niższym poziomie (pojedynczych znaków zamiast słów lub zwrotów): zastępujemy poszczególne znaki innymi znakami (zamiast słowa innymi słowami).
- Dwie kategorie metod szyfrowania (przestawianie, podstawianie).

Szyfry przestawieniowe

Przestawienie polega na zmianie uporządkowania znaków tekstu, czyli stworzeniu *anagramu*.

Czy to jest bezpieczne?

```
nie
nei

ine
ien

eni
ein
```

Szyfry przestawieniowe

Przestawienie polega na zmianie uporządkowania znaków tekstu, czyli stworzeniu *anagramu*.

Czy to jest bezpieczne?

```
nie
nei

ine
ien

eni
ein
```

Szyfry przestawieniowe

liczba znaków	maksymalna liczba sekwencji
3	6 (six)
5	120 (one hundred twenty)
7	5040 (five thousand, forty)
9	362880 (three hundred sixty-two thousand, eight hundred eighty)
11	3.99168 x 10^7 (39 million 916 thousand 800)
13	6.2270208 x 10^9 (6 billion 227 million 20 thousand 800)
15	1.307674368 x 10^12 (1 trillion 307 billion 674 million 368 thousand)
17	3.55687428096 x 10^14 (355 trillion 687 billion 428 million 96 thousand
19	1.21645100408832 x 10^17 (121 quadrillion ...)
21	5.109094217170944 x 10^19 (51 quintillion ...)
23	2.5852016738884976640 x 10^22 (25 sextillion ...)
25	1.5511210043330985984 x 10^25 (15 septillion ...)
27	1.0888869450418352160768 x 10^28 (10 octillion ...)
29	8.8417619937397019545436160 x 10^30 (8 nonillion ...)
31	8.2228386541779228177255628800 x 10^33 (8 decillion ...)
	8 decillion 222 nonillion 838 octillion 654 septillion
	177 sextillion 922 quintillion 817 quadrillion
	725 trillion 562 billion 880 million

Jak więc widać, istotna jest umiejętność określenia sposbu tworzenia anagramu, gdyż bez jego znajomości otrzymujemy tekst owszem niemożliwy praktycznie do odczytania przez osobę niepowołaną, ale także i przez adresata. Musimy zatem w jakiś sposób kontrolować tworzony anagram – mówiąc inaczej, musimy wymyślić schemat budowy anagramu, czyli skonstruować konkretny szyfr.

Szyfry przestawieniowe – szyfr płotkowy

Idea

TEKST_JAWNY

Szyfry przestawieniowe – szyfr płotkowy

Idea

```
TEKST_JAWNY

T
```

Szyfry przestawieniowe – szyfr płotkowy

Idea

```
TEKST_JAWNY

T
 E
```

Szyfry przestawieniowe – szyfr płotkowy

Idea

```
TEKST_JAWNY

T K
 E
```

Szyfry przestawieniowe – szyfr płotkowy

Idea

```
TEKST_JAWNY

T K
 E S
```

Szyfry przestawieniowe – szyfr płotkowy

Idea

```
TEKST_JAWNY

T K T
 E S
```

Szyfry przestawieniowe – szyfr płotkowy

Idea

```
TEKST_JAWNY

T K T
 E S _
```

Szyfry przestawieniowe – szyfr płotkowy

Idea

```
TEKST_JAWNY

T K T J
 E S _
```

Szyfry przestawieniowe – szyfr płotkowy

Idea

```
TEKST_JAWNY

T K T J
 E S _ A
```

Szyfry przestawieniowe – szyfr płotkowy

Idea

```
TEKST_JAWNY

T K T J W
 E S _ A
```

Szyfry przestawieniowe – szyfr płotkowy

Idea

```
TEKST_JAWNY

T K T J W
 E S _ A N
```

Szyfry przestawieniowe – szyfr płotkowy

Idea

```
TEKST_JAWNY

T K T J W Y
 E S _ A N
```

Szyfry przestawieniowe – szyfr płotkowy

Idea

```
TEKST_JAWNY

TKTJWY
 ES_AN
```

Szyfry przestawieniowe – szyfr płotkowy

Idea

```
TEKST_JAWNY

TKTJWY
   ES_AN
```

Szyfry przestawieniowe – szyfr płotkowy

Idea

```
TEKST_JAWNY

TKTJWY
      ES_AN
```

Szyfry przestawieniowe – szyfr płotkowy

Idea

```
TEKST_JAWNY

TKTJWY
       ES_AN
```

Szyfry przestawieniowe – szyfr płotkowy

Idea

TEKST_JAWNY

TKTJWY ES_AN

Szyfry przestawieniowe – szyfr płotkowy

Idea

TEKST_JAWNY

TKTJWYES_AN

Szyfry przestawieniowe – szyfr płotkowy

Idea

```
TEKST_JAWNY

T K T J W Y => TKTJWY
 E S _ A N  => ES_AN

               TKTJWY ES_AN
               TKTJWYES_AN
TKTJWYES_AN
```

Szyfry przestawieniowe – szyfr płotkowy

Modyfikacja 1

W metodzie można zwiększyć liczbę wierszy, na przykład do 4

```
TEKST_JAWNY

T      J       => TJ
 E    _ A       => E_A
  K T    W Y   => KTWY
   S       N   => SN

                  TJ E_A KTWY SN
                  TJE_AKTWYSN

TJE_AKTWYSN
```

Szyfry przestawieniowe – szyfr płotkowy

Modyfikacja 2

Zamiast zaczynać "wpisywanie" tekstu od górnego wiersza, można od dowolnego innego (ustalonego), na przykład szyforwanie na 4 wierszach z offsetem (przesunięciem) o 5

```
TEKST_JAWNY

.      E      A.    => EA
 .    T K    J W    => TKJW
  . .    S _    N   => S_N
   .      T      Y  => TY

                     EA TKJW S_N TY
                     EATKJWS_NTY
EATKJWS_NTY
```

Szyfry przestawieniowe – szyfr płotkowy

Łamanie siłowe

NTEUT_I_AI_RDEOEKTN

Szyfry przestawieniowe – szyfr płotkowy

Łamanie siłowe

Gdyby użyto 2 wierszy bez przesunięcia, wówczas 19 znaków podczas szyfrowania zostałoby rozmieszczonych jak poniżej

```
1 3 5 7 9 1 3 5 7 9
 2 4 6 8 0 2 4 6 8
```

co dałoby szyfrogram postaci

```
          1 1 1 1 1         1 1 1 1 1
1 3 5 7 9 1 3 5 7 9 2 4 6 8 0 2 4 6 8
N T E U T _ I _ A I _ R D E O E K T N

N T E U T _ I _ A I
 _ R D E O E K T N
```

Zatem tekstem oryginalnym musiałoby być:

```
N_TREDUETO_EIK_TANI
```

Szyfry przestawieniowe – szyfr płotkowy

Łamanie siłowe

Jak więc widać, stosując wyłącznie metodę siłową, sprawdzając kolejne możliwe "parametry" szyfru (kolejne "hasła") otzymujemy ciąg odszyfrowanych wiadomości, z których sensowna będzie najpardopodobniej tylko jedna.

```
R=2, O=0: N_TREDUETO_EIK_TANI
R=2, O=1: IN_TREDUETO_EIK_TAN
R=3, O=0: N_OIT_EAEIK_URTDTEN
R=3, O=1: TO_NIE_TAKIE_TRUDNE
```

Wniosek 3

Metoda powinna być tak skonstruowan aby znajomość sposobu szyfrowania nie była wystarczająca do odszyfrowania tekstu.
Ewentualnie i znacznie lepiej: upublicznić (odtajnić) samą metodę i jej opis, ale wprowadzić do niej mechanizm klucza, który ze względu na złożoność i mnogość alternatywnych rozwiązań zabezpiecza tekst.
Podstawowa zasada kryptologii: **dla bezpieczeństwa istotny jest klucz, a nie algorytm**.
Ostateczną postać nadał jej holenderski lingwista Auguste Kerckhoffs von Nieuwenhof w książce *La Cryptographie militaire*: **Bezpieczeństwo systemu kryptogtaficznego nie może zależeć od zachowania w tajemnicy algorytmu szyfrującego. Bezpieczeństwo zależy wyłącznie od zachowania w tajemnicy klucza.**[a]

[a] Simon Singh, *Księga szyfrow*, Wydawnictwo Albatros A. Kuryłowicz, Warszawa 2001.

Wniosek 3

Metoda powinna być tak skonstruowan aby znajomość sposobu szyfrowania nie była wystarczająca do odszyfrowania tekstu.
Ewentualnie i znacznie lepiej: upublicznić (odtajnić) samą metodę i jej opis, ale wprowadzić do niej mechanizm klucza, który ze względu na złożoność i mnogość alternatywnych rozwiązań zabezpiecza tekst.
Podstawowa zasada kryptologii: **dla bezpieczeństwa istotny jest klucz, a nie algorytm**.
Ostateczną postać nadał jej holenderski lingwista Auguste Kerckhoffs von Nieuwenhof w książce *La Cryptographie militaire*: **Bezpieczeństwo systemu kryptogtaficznego nie może zależeć od zachowania w tajemnicy algorytmu szyfrującego. Bezpieczeństwo zależy wyłącznie od zachowania w tajemnicy klucza.**[a]

[a] Simon Singh, *Księga szyfrow*, Wydawnictwo Albatros A. Kuryłowicz, Warszawa 2001.

Szyfry podstawieniowe

W przestawieniowych metodach szyfrowania każdy znak zachowuje tożsamość (nie zmienia się na żaden inny znak), ale zmienia położenie. Komplementarnym (uzupełniającym) do przestawieniowej powyżej metody szyfrowania jest szyfrowanie podstawieniowe. W metodzie tej zmienia się tożsamość litery, ale jej położenie jest ustalone.

Łączymy litery alfabetu w pary, a następnie zastępujemy litery z tekstu jawnego, literami z danej pary.

`znak`	`ABCDEFGHIJKLMNOPQRSTUVWXYZ_`
`zamiennik`	`BCDEUGFYNIJKLOMPAQR_STZVWHX`

Zauważmy, że w tym sposobie tworzenia par nie ma możliwości aby jakiś znak pojawił się więcej niż jeden raz; mowiąc dokładniej, każdy dopuszczalny znak musi pojawić się dokładnie jeden raz jako każdy z elementów pary. Na przykład litera A występuje w parach (A, B) oraz (Q, A) – raz na pierwszej pozycji i raz na drugiej.
Kompletny zestaw par staje się w tym przypadku ***kluczem***, czyli elementem niezbędnym do zaszyfrowania i odszyfrowania treści. Problem w tym, że taki klucz, jeśli jest losowy, jest trudny do zapamiętania.

Szyfry podstawieniowe

Idea

```
znak          ABCDEFGHIJKLMNOPQRSTUVWXYZ_
zamiennik     BCDEUGFYNIJKLOMPAQR_STZVWHX

TEKST_JAWNY

_UJR_XIBZOW
```

Szyfry podstawieniowe – szyfry Cezara

Idea

Względnie łatwo możemy określać podstawienie dokonując przesunięcia całego alfabetu (listy znaków) o zadaną ilość znaków. W przypadku szyfru Cezara przesunięcie to wynosiło 3 znaki

```
znak                      ABCDEFGHIJKLMNOPQRSTUVWXYZ_
przesunięcie o 3  ABC|DEFGHIJKLMNOPQRSTUVWXYZ_
zamiennik                 DEFGHIJKLMNOPQRSTUVWXYZ_ABC
```

Używając powyższych podstawień do zaszyfrowania tekstu TEKST_JAWNY, otrzymujemy:

```
TEKST_JAWNY

WHNVWCMDZQA
```

Szyfry podstawieniowe – szyfry Cezara

Łamanie siłowe

Spróbujmy rozszyfrować następujący szyfrogram

```
XSDRMIDXEOMIDXVYHRI
```

Po kolei będziemy sprawdzać wyniki otrzymane przy użyciu alfabetu przesuniętego o 1, 2, 3 itd znaki

```
BCDEFGHIJKLMNOPQRSTUVWXYZ_A XSDRMIDXEOMIDXVYHRI
ABCDEFGHIJKLMNOPQRSTUVWXYZ_ WRCQLHCWDNLHCWUWGQH

CDEFGHIJKLMNOPQRSTUVWXYZ_AB XSDRMIDXEOMIDXVYHRI
ABCDEFGHIJKLMNOPQRSTUVWXYZ_ VQBPKGBVCMKGBVTWFPG

DEFGHIJKLMNOPQRSTUVWXYZ_ABC XSDRMIDXEOMIDXVYHRI
ABCDEFGHIJKLMNOPQRSTUVWXYZ_ UPAOJFAUBLJFAUSVEOF

EFGHIJKLMNOPQRSTUVWXYZ_ABCD XSDRMIDXEOMIDXVYHRI
ABCDEFGHIJKLMNOPQRSTUVWXYZ_ TO_NIE_TAKIE_TRUDNE
```

Szyfry podstawieniowe – szyfry Cezara

Łamanie siłowe

Spróbujmy rozszyfrować następujący szyfrogram

```
XSDRMIDXEOMIDXVYHRI
```

Po kolei będziemy sprawdzać wyniki otrzymane przy użyciu alfabetu przesuniętego o 1, 2, 3 itd znaki

```
BCDEFGHIJKLMNOPQRSTUVWXYZ_A XSDRMIDXEOMIDXVYHRI
ABCDEFGHIJKLMNOPQRSTUVWXYZ_ WRCQLHCWDNLHCWUWGQH

CDEFGHIJKLMNOPQRSTUVWXYZ_AB XSDRMIDXEOMIDXVYHRI
ABCDEFGHIJKLMNOPQRSTUVWXYZ_ VQBPKGBVCMKGBVTWFPG

DEFGHIJKLMNOPQRSTUVWXYZ_ABC XSDRMIDXEOMIDXVYHRI
ABCDEFGHIJKLMNOPQRSTUVWXYZ_ UPAOJFAUBLJFAUSVEOF

EFGHIJKLMNOPQRSTUVWXYZ_ABCD XSDRMIDXEOMIDXVYHRI
ABCDEFGHIJKLMNOPQRSTUVWXYZ_ TO_NIE_TAKIE_TRUDNE
```

Szyfry podstawieniowe – szyfry Cezara

Łamanie siłowe

Spróbujmy rozszyfrować następujący szyfrogram

```
XSDRMIDXEOMIDXVYHRI
```

Po kolei będziemy sprawdzać wyniki otrzymane przy użyciu alfabetu przesuniętego o 1, 2, 3 itd znaki

```
BCDEFGHIJKLMNOPQRSTUVWXYZ_A XSDRMIDXEOMIDXVYHRI
ABCDEFGHIJKLMNOPQRSTUVWXYZ_ WRCQLHCWDNLHCWUWGQH

CDEFGHIJKLMNOPQRSTUVWXYZ_AB XSDRMIDXEOMIDXVYHRI
ABCDEFGHIJKLMNOPQRSTUVWXYZ_ VQBPKGBVCMKGBVTWFPG

DEFGHIJKLMNOPQRSTUVWXYZ_ABC XSDRMIDXEOMIDXVYHRI
ABCDEFGHIJKLMNOPQRSTUVWXYZ_ UPAOJFAUBLJFAUSVEOF

EFGHIJKLMNOPQRSTUVWXYZ_ABCD XSDRMIDXEOMIDXVYHRI
ABCDEFGHIJKLMNOPQRSTUVWXYZ_ TO_NIE_TAKIE_TRUDNE
```

Szyfry podstawieniowe – szyfry Cezara

Łamanie siłowe

Spróbujmy rozszyfrować następujący szyfrogram

```
XSDRMIDXEOMIDXVYHRI
```

Po kolei będziemy sprawdzać wyniki otrzymane przy użyciu alfabetu przesuniętego o 1, 2, 3 itd znaki

```
BCDEFGHIJKLMNOPQRSTUVWXYZ_A XSDRMIDXEOMIDXVYHRI
ABCDEFGHIJKLMNOPQRSTUVWXYZ_ WRCQLHCWDNLHCWUWGQH

CDEFGHIJKLMNOPQRSTUVWXYZ_AB XSDRMIDXEOMIDXVYHRI
ABCDEFGHIJKLMNOPQRSTUVWXYZ_ VQBPKGBVCMKGBVTWFPG

DEFGHIJKLMNOPQRSTUVWXYZ_ABC XSDRMIDXEOMIDXVYHRI
ABCDEFGHIJKLMNOPQRSTUVWXYZ_ UPAOJFAUBLJFAUSVEOF

EFGHIJKLMNOPQRSTUVWXYZ_ABCD XSDRMIDXEOMIDXVYHRI
ABCDEFGHIJKLMNOPQRSTUVWXYZ_ TO_NIE_TAKIE_TRUDNE
```

Szyfry podstawieniowe – szyfry Cezara

Łamanie siłowe

Spróbujmy rozszyfrować następujący szyfrogram

```
XSDRMIDXEOMIDXVYHRI
```

Po kolei będziemy sprawdzać wyniki otrzymane przy użyciu alfabetu przesuniętego o 1, 2, 3 itd znaki

```
BCDEFGHIJKLMNOPQRSTUVWXYZ_A XSDRMIDXEOMIDXVYHRI
ABCDEFGHIJKLMNOPQRSTUVWXYZ_ WRCQLHCWDNLHCWUWGQH

CDEFGHIJKLMNOPQRSTUVWXYZ_AB XSDRMIDXEOMIDXVYHRI
ABCDEFGHIJKLMNOPQRSTUVWXYZ_ VQBPKGBVCMKGBVTWFPG

DEFGHIJKLMNOPQRSTUVWXYZ_ABC XSDRMIDXEOMIDXVYHRI
ABCDEFGHIJKLMNOPQRSTUVWXYZ_ UPAOJFAUBLJFAUSVEOF

EFGHIJKLMNOPQRSTUVWXYZ_ABCD XSDRMIDXEOMIDXVYHRI
ABCDEFGHIJKLMNOPQRSTUVWXYZ_ TO_NIE_TAKIE_TRUDNE
```

Szyfry podstawieniowe

Tworzenie klucza w oparciu o wyrażenie kluczowe

1. wyrażenie kluczowe.....STAR_WARS
2.
3.
4.

5.

Ostatecznie:
znaki.....
zamiennik.....

Szyfry podstawieniowe

Tworzenie klucza w oparciu o wyrażenie kluczowe

1. wyrażenie kluczowe.....STAR_WARS
2. wyrażenie z usuniętymi
   powtórzeniami.....STAR_W
3.
4.

5.

Ostatecznie:
znaki.....
zamiennik.....

Szyfry podstawieniowe

Tworzenie klucza w oparciu o wyrażenie kluczowe

1. wyrażenie kluczowe.....STAR_WARS
2. wyrażenie z usuniętymi
   powtórzeniami.....STAR_W
3. zbiór znaków (znaki).....ABCDEFGHIJKLMNOPQRSTUVWXYZ_
4.

5.

Ostatecznie:
znaki.....
zamiennik.....

Szyfry podstawieniowe

Tworzenie klucza w oparciu o wyrażenie kluczowe

1. wyrażenie kluczowe.....STAR_WARS
2. wyrażenie z usuniętymi
   powtórzeniami.....STAR_W
3. zbiór znaków (znaki).....ABCDEFGHIJKLMNOPQRSTUVWXYZ_
4. zbiór znaków z usuniętymi
   znakami z wyrażenia
   kluczowego.....*BCDEFGHIJKLMNOPQ***UV*XYZ*

5.

Ostatecznie:
znaki.....
zamiennik.....

Szyfry podstawieniowe

Tworzenie klucza w oparciu o wyrażenie kluczowe

1. wyrażenie kluczowe.....STAR_WARS
2. wyrażenie z usuniętymi
   powtórzeniami.....STAR_W
3. zbiór znaków (znaki).....ABCDEFGHIJKLMNOPQRSTUVWXYZ_
4. zbiór znaków z usuniętymi
   znakami z wyrażenia
   kluczowego.....*BCDEFGHIJKLMNOPQ***UV*XYZ*
   BCDEFGHIJKLMNOPQUVXYZ
5.

Ostatecznie:
znaki.....
zamiennik.....

Szyfry podstawieniowe

Tworzenie klucza w oparciu o wyrażenie kluczowe

1. wyrażenie kluczowe.....STAR_WARS
2. wyrażenie z usuniętymi
   powtórzeniami.....STAR_W
3. zbiór znaków (znaki).....ABCDEFGHIJKLMNOPQRSTUVWXYZ_
4. zbiór znaków z usuniętymi
   znakami z wyrażenia
   kluczowego.....*BCDEFGHIJKLMNOPQ***UV*XYZ*
   BCDEFGHIJKLMNOPQUVXYZ
5. 2.+ 4. = zamiennik.....STAR_WBCDEFGHIJKLMNOPQUVXYZ

Ostatecznie:
znaki.....
zamiennik.....

Szyfry podstawieniowe

Tworzenie klucza w oparciu o wyrażenie kluczowe

1. wyrażenie kluczowe.....STAR_WARS
2. wyrażenie z usuniętymi
   powtórzeniami.....STAR_W
3. zbiór znaków (znaki).....ABCDEFGHIJKLMNOPQRSTUVWXYZ_
4. zbiór znaków z usuniętymi
   znakami z wyrażenia
   kluczowego.....*BCDEFGHIJKLMNOPQ***UV*XYZ*
   BCDEFGHIJKLMNOPQUVXYZ
5. 2.+ 4. = zamiennik.....STAR_WBCDEFGHIJKLMNOPQUVXYZ

Ostatecznie:

znaki.....ABCDEFGHIJKLMNOPQRSTUVWXYZ_

zamiennik.....STAR_WBCDEFGHIJKLMNOPQUVXYZ

Używając powyższych podstawień do zaszyfrowania tekstu TEKST_JAWNY, otrzymujemy:

```
TEKST_JAWNY

O_FNOZESUIX
```

W tym przypadku odszyfrowanie tesktu jest zadaniem znacznie trudniejszym w porównaniu z szyfrem Cezara – ze względu na występowanie wyrażenia kluczowego liczba potencjalnych kluczy jest znacznie większa.

Wniosek 4

W metodzie szyfrującej zapewnić aby ilość możliwych kluczy była na tyle duża aby nie było możliwe sprawdzenie ich wszystkich metodą siłową w akceptowalnym czasie.
UWAGA: Efektywna możliwość sprawdzenia wszystkich kluczy w akceptowalnym czasie ulega zmianom wraz z rozwojem techniki.

Niestety wciąż obowiązuje zasada, że wybranemu znakowi zawsze odpowiada ten sam zamiennik. Cecha ta pozwala efektywnie łamać szyfry tego rodzaju dzięki *analizie częstotliwościowej występowania znaków*.

Wniosek 5.1

Dokument zaszyfrowany nie powinien zawierać w sposób jawny (czytelny) żadnej charakterystyki dokumentu jawnego.

Wniosek 4

W metodzie szyfrującej zapewnić aby ilość możliwych kluczy była na tyle duża aby nie było możliwe sprawdzenie ich wszystkich metodą siłową w akceptowalnym czasie.
UWAGA: Efektywna możliwość sprawdzenia wszystkich kluczy w akceptowalnym czasie ulega zmianom wraz z rozwojem techniki.

Niestety wciąż obowiązuje zasada, że wybranemu znakowi zawsze odpowiada ten sam zamiennik. Cecha ta pozwala efektywnie łamać szyfry tego rodzaju dzięki *analizie częstotliwościowej występowania znaków*.

Wniosek 5.1

Dokument zaszyfrowany nie powinien zawierać w sposób jawny (czytelny) żadnej charakterystyki dokumentu jawnego.

Wniosek 4

W metodzie szyfrującej zapewnić aby ilość możliwych kluczy była na tyle duża aby nie było możliwe sprawdzenie ich wszystkich metodą siłową w akceptowalnym czasie.
UWAGA: Efektywna możliwość sprawdzenia wszystkich kluczy w akceptowalnym czasie ulega zmianom wraz z rozwojem techniki.

Niestety wciąż obowiązuje zasada, że wybranemu znakowi zawsze odpowiada ten sam zamiennik. Cecha ta pozwala efektywnie łamać szyfry tego rodzaju dzięki *analizie częstotliwościowej występowania znaków*.

Wniosek 5.1

Dokument zaszyfrowany nie powinien zawierać w sposób jawny (czytelny) żadnej charakterystyki dokumentu jawnego.

Wniosek 4

W metodzie szyfrującej zapewnić aby ilość możliwych kluczy była na tyle duża aby nie było możliwe sprawdzenie ich wszystkich metodą siłową w akceptowalnym czasie.
UWAGA: Efektywna możliwość sprawdzenia wszystkich kluczy w akceptowalnym czasie ulega zmianom wraz z rozwojem techniki.

Niestety wciąż obowiązuje zasada, że wybranemu znakowi zawsze odpowiada ten sam zamiennik. Cecha ta pozwala efektywnie łamać szyfry tego rodzaju dzięki *analizie częstotliwościowej występowania znaków*.

Wniosek 5.1

Dokument zaszyfrowany nie powinien zawierać w sposób jawny (czytelny) żadnej charakterystyki dokumentu jawnego.

Charakterystykę dokumentu jawnego ukryjemy, gdy jeden znak tekstu jawnego będzie zastępowany różnymi znakami w zależności od miejsca występowania znaku w tekście i znaków go poprzedzających. Ten sam znak występujący na przykład trzykrotnie po sobie powinien być zawsze szyfrowany jako trzy różne znaki.

Szyfry podstawieniowe – Enigma

Idea

Używając utworzonego wcześniej w oparciu o wyrażenie kluczowe START_WARS podstawienia

```
znaki.........................ABCDEFGHIJKLMNOPQRSTUVWXYZ_
zamiennik.....................STAR_WBCDEFGHIJKLMNOPQUVXYZ
```

zakodujemy tekst DDD jako RRR. W tym podstawieniu na przykład litera D zastępowana jest oddaloną od niej o 14 pozycji na prawo (pisać będziemy +14) literą R a litera R zastepowana jest oddaloną od niej o 5 na lewo (pisać będziemy -5) literą M. Skrótowo będziemy to zapisywać jako D+14=R, R-5=M. Stąd podstawienie to możemy zapisać w innej równoważnej postaci jako

znaki.....	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
oddalenie.....	+18	+18	-2	+14	+22	+17	-5	-5	-5	-5	-5	-5	-5	-5	-5	-5
zamiennik.....	S	T	A	R	_	W	B	C	D	E	F	G	H	I	J	K

Szyfry podstawieniowe – Enigma

Idea

Krok 1: oddalenia w pozycji wyjściowej (nieprzesunięte)

znaki.....	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
oddalenie.....+18	+18	-2	+14	+22	+17	-5	-5	-5	-5	-5	-5	-5	-5	-5	-5	
zamiennik.....	S	T	A	R	_	W	B	C	D	E	F	G	H	I	J	K

Pozwoli to zakodować pierwszą literę D jako R.

Krok 2: oddalenia przesunięte o 1 w prawo w stosnku do Kroku 1

znaki.....	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
oddalenie.....	-1	+18	+18	-2	+14	+22	+17	-5	-5	-5	-5	-5	-5	-5	-5	-5
zamiennik.....	_	T	U	B	S	A	X	C	D	E	F	G	H	I	J	K

Pozwoli to zakodować drugą literę D jako B. Podobnie jak poprzednio, wstarczy policzyć D+(-2).

Krok 3: oddalenia przesunięte o 1 w prawo w stosnku do Kroku 2

znaki.....	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
oddalenie.....	-1	-1	+18	+18	-2	+14	+22	+17	-5	-5	-5	-5	-5	-5	-5	-5
zamiennik.....	_	A	U	V	C	T	B	Y	D	E	F	G	H	I	J	K

Pozwoli to zakodować trzecią literę D jako V. Podobnie jak poprzednio, wstarczy policzyć D+18.

Tak więc ciąg DDD został zakodowany jako RBV. Jak więc widać sama procedura szyfrowania nie stała się dużo bardziej złożona od poprzednich. Deszyfrowanie (przy znajomości klucza, a więc oddalenia z Kroku 1) jest jak najbardziej wykonalne, choć wymaga więcej czasu, gdyż należy przeprowadzić proces odwrotny, a więc trzeba wyszukać w zamiennikach zaszyfrowany znak co pozwoli wyznaczyć odpowiadający jemu znak jawny.

Na zmodyfikowanej wersji tej metody, oparta była niemiecka maszyna szyfrująca Enigma. Jednak ona także posiadała słabe punkty i została złamana na początku lat 30-tych ubiegłego wieku przez Marian Rejewski oraz Henryka Zygalskiego i Jerzego Różyckiego.

Szyfry podstawieniowe – Enigma

Idea

Amerykański historyk i dziennikarz David Kahn napisał[1], że *rozwiązanie tej zagadki było oszałamiającym osiągnięciem, które wyniosło Rejewskiego do panteonu największych kryptoanalityków wszech czasów.*

[1] David Kahn, *Łamacze kodów. Tajemnice kryptologii*, Barbara Kołodziejczyk (tłum.), Warszawa: WNT, 2004

Szyfry podstawieniowe – Enigma

Idea

Jak czytamy w *Księdze szyfrów*[2]:
Jego [Rejewskiego] atak na Enigmę był jednym z największych osiągnięć w historii kryptoanalizy. Musiałem tu streścić jego pracę na kilku stronach, dlatego pominąłem wiele szczegółów matematycznych i wszystkie ślepe zaułki. Enigma jest bardzo złożoną maszyną szyfrującą i złamanie niemieckeigo szyfru wymagało ogromnej siły intelektu. Moje uproszczenia nie powinny nikogo skłonić do zlekceważenia ogromnego osiągnięcia Rejewskiego.[3]
Srategia Rejewskiego polegała na wykorzystaniu faktu, że powtórzenie jest wrogiem bezpieczeństwa: powtórzenia prowadzą do regularności, a tego właśnie trzeba kryptoanalitykom.[4]

---

[2] Simon Singh, *Księga szyfrow*, Wydawnictwo Albatros A. Kuryłowicz, Warszawa 2001)

[3] Ibidem, s. 171

[4] Ibidem, s. 165

Jak czytamy w *Księdze szyfrów*[2]:
Jego [Rejewskiego] atak na Enigmę był jednym z największych osiągnięć w historii kryptoanalizy. Musiałem tu streścić jego pracę na kilku stronach, dlatego pominąłem wiele szczegółów matematycznych i wszystkie ślepe zaułki. Enigma jest bardzo złożoną maszyną szyfrującą i złamanie niemieckeigo szyfru wymagało ogromnej siły intelektu. Moje uproszczenia nie powinny nikogo skłonić do zlekceważenia ogromnego osiągnięcia Rejewskiego.[3]
Srategia Rejewskiego polegała na wykorzystaniu faktu, że powtórzenie jest wrogiem bezpieczeństwa: powtórzenia prowadzą do regularności, a tego właśnie trzeba kryptoanalitykom.[4]

[2] Simon Singh, *Księga szyfrow*, Wydawnictwo Albatros A. Kuryłowicz, Warszawa 2001)
[3] Ibidem, s. 171
[4] Ibidem, s. 165

Wniosek 5.2

Sposób szyfrowania nie powinien dopuszczać tworzenia powtórzeń.

Wniosek 5.2

Sposób szyfrowania nie powinien dopuszczać tworzenia powtórzeń.

Szyfry podstawieniowe – XOR

Idea

Wszystkie dotychczas opisane metody, jak i wiele innych używanych współcześnie, mają jedną zasadniczą wadę: możliwe są do odszyfrowania jeśli tylko będziemy mieć wystarczająco dużo czasu. Potrzebny czas może być bardzo duży, ale zawsze będzie skończony.
Istnieje jednak pewna metoda, która ukrywa sekret na zawsze bez możliwości jego ujawnienia w przypadku niedysponowania kluczem.
Co może dziwić, metoda ta jest bardzo prosta.

Szyfry podstawieniowe – XOR

Idea

Najpierw nadajmy każdemu znakowi numer równy pozycji znaku w ciagu znaków dopuszczalnych (alfabecie).

```
                          1111111111222222
pozycja.....01234567890123456789012345 6
znak.........ABCDEFGHIJKLMNOPQRSTUVWXYZ_
```

Szyfry podstawieniowe – XOR

Idea

Teraz każdy numer zapiszmy jako ciąg dwójkowy 5-bitowy (zbiór dopuszczalnych symboli, ze względów technicznych, musiał zostać rozszerzony do wielkości $2^5 = 32$; dodane zostały symbole 1, 2, 3, 4 oraz 5)

```
                        11111111112222222231
pozycja.....01234567890123456789012345678901
znak........ABCDEFGHIJKLMNOPQRSTUVWXYZ_12345
            ||||||||||||||||||||||||||||||
            00000000000000011111111111111111
            00000000111111110000000011111111
            00001111000011110000111100001111
            00110011001100110011001100110011
kod.........01010101010101010101010101010101
```

Szyfry podstawieniowe – XOR

Idea

Następnie na każdym ciagu dwójkowym odpowiadajacym znakowi tekstu jawnego oraz ciągu dwójkowym klucza przeprowadzamy pewnego rodzaju operację dodawania według poniższych reguł:

- Jeśli odpowiednie bity tekstu jawnego i klucza są jednakowe (to znaczy oba mają wartość 0 albo oba mają wartość 1), to w tekście zaszyfrowanym stawiamy 0.
- Jeśli odpowiednie bity tekstu jawnego i klucza są różne (to znaczy jeden z nich ma wartość 0 a drugi wartość 1), to w tekście zaszyfrowanym stawiamy 1.

Taka operacja nazwyana jest w informatyce operacja XOR. Przeprowadzając ją na bitach tekstu jawnego TEKST_JAWNY i klucza DK_SERK_QCV otrzymamy tekst zaszyfrowany. Co istone, w tym przypadku klucz nie musi być permutacją (wymieszaniem) zbioru dopuszczalnych symboli, ale może być dowolną ich kombinacją

Szyfry podstawieniowe – XOR

Idea

tekst jawny	T	E	K	S	T	_	J	A	W	N	Y
klucz	D	K	_	S	E	R	K	_	Q	C	V

XOR
tekst
zaszyfrowany

Szyfry podstawieniowe – XOR

Idea

tekst jawny	T	E	K	S	T	_	J	A	W	N	Y
	10011	00100	01010	10010	10011	11010	01001	00000	10110	01101	11000
klucz	D	K	_	S	E	R	K	_	Q	C	V
	00011	01010	11010	10010	00100	10001	01010	11010	10000	00010	10101
XOR											
tekst											
zaszyfrowany											

Szyfry podstawieniowe – XOR

Idea

tekst jawny		T	E	K	S	T	_	J	A	W	N	Y
	10011	00100	01010	10010	10011	11010	01001	00000	10110	01101	11000
klucz		D	K	_	S	E	R	K	_	Q	C	V
	00011	01010	11010	10010	00100	10001	01010	11010	10000	00010	10101
XOR	1										
tekst zaszyfrowany											

Szyfry podstawieniowe – XOR

Idea

tekst jawny		T	E	K	S	T	_	J	A	W	N	Y
	10011	00100	01010	10010	10011	11010	01001	00000	10110	01101	11000
klucz		D	K	_	S	E	R	K	_	Q	C	V
	00011	01010	11010	10010	00100	10001	01010	11010	10000	00010	10101
XOR	10										
tekst zaszyfrowany											

Szyfry podstawieniowe – XOR

Idea

tekst jawny		T	E	K	S	T	_	J	A	W	N	Y
	10011	00100	01010	10010	10011	11010	01001	00000	10110	01101	11000
klucz		D	K	_	S	E	R	K	_	Q	C	V
	00011	01010	11010	10010	00100	10001	01010	11010	10000	00010	10101
XOR	100										
tekst zaszyfrowany											

Szyfry podstawieniowe – XOR

Idea

tekst jawny	T	E	K	S	T	_	J	A	W	N	Y
	10011	00100	01010	10010	10011	11010	01001	00000	10110	01101	11000
klucz	D	K	_	S	E	R	K	_	Q	C	V
	00011	01010	11010	10010	00100	10001	01010	11010	10000	00010	10101
XOR	1000										
tekst zaszyfrowany											

Szyfry podstawieniowe – XOR

Idea

tekst jawny	T	E	K	S	T	_	J	A	W	N	Y
	10011	00100	01010	10010	10011	11010	01001	00000	10110	01101	11000
klucz	D	K	_	S	E	R	K	_	Q	C	V
	00011	01010	11010	10010	00100	10001	01010	11010	10000	00010	10101
XOR	10000										
tekst zaszyfrowany											

Szyfry podstawieniowe – XOR

Idea

tekst jawny	T	E	K	S	T	_	J	A	W	N	Y
	10011	00100	01010	10010	10011	11010	01001	00000	10110	01101	11000
klucz	D	K	_	S	E	R	K	_	Q	C	V
	00011	01010	11010	10010	00100	10001	01010	11010	10000	00010	10101
XOR	10000										
tekst zaszyfrowany	Q										

Szyfry podstawieniowe – XOR

Idea

tekst jawny		T	E	K	S	T	_	J	A	W	N	Y
	10011	00100	01010	10010	10011	11010	01001	00000	10110	01101	11000
klucz		D	K	_	S	E	R	K	_	Q	C	V
	00011	01010	11010	10010	00100	10001	01010	11010	10000	00010	10101
XOR	10000	0									
tekst zaszyfrowany		Q									

Szyfry podstawieniowe – XOR

Idea

tekst jawny		T	E	K	S	T	_	J	A	W	N	Y
	10011	00100	01010	10010	10011	11010	01001	00000	10110	01101	11000
klucz		D	K	_	S	E	R	K	_	Q	C	V
	00011	01010	11010	10010	00100	10001	01010	11010	10000	00010	10101
XOR	10000	01									
tekst zaszyfrowany		Q									

Szyfry podstawieniowe – XOR

Idea

tekst jawny		T	E	K	S	T	_	J	A	W	N	Y
	10011	00100	01010	10010	10011	11010	01001	00000	10110	01101	11000
klucz		D	K	_	S	E	R	K	_	Q	C	V
	00011	01010	11010	10010	00100	10001	01010	11010	10000	00010	10101
XOR	10000	011									
tekst zaszyfrowany		Q									

Szyfry podstawieniowe – XOR

Idea

tekst jawny		T	E	K	S	T	_	J	A	W	N	Y
	10011	00100	01010	10010	10011	11010	01001	00000	10110	01101	11000
klucz		D	K	_	S	E	R	K	_	Q	C	V
	00011	01010	11010	10010	00100	10001	01010	11010	10000	00010	10101
XOR	10000	0111									
tekst zaszyfrowany		Q									

Szyfry podstawieniowe – XOR

Idea

tekst jawny		T	E	K	S	T	_	J	A	W	N	Y
	10011	00100	01010	10010	10011	11010	01001	00000	10110	01101	11000
klucz		D	K	_	S	E	R	K	_	Q	C	V
	00011	01010	11010	10010	00100	10001	01010	11010	10000	00010	10101
XOR	10000	01110									
tekst zaszyfrowany		Q									

Szyfry podstawieniowe – XOR

Idea

tekst jawny		T	E	K	S	T	_	J	A	W	N	Y
	10011	00100	01010	10010	10011	11010	01001	00000	10110	01101	11000
klucz		D	K	_	S	E	R	K	_	Q	C	V
	00011	01010	11010	10010	00100	10001	01010	11010	10000	00010	10101
XOR	10000	01110									
tekst zaszyfrowany		Q	O								

Szyfry podstawieniowe – XOR

Idea

. . . aż w końcu

tekst jawny	T	E	K	S	T	_	J	A	W	N	Y
	10011	00100	01010	10010	10011	11010	01001	00000	10110	01101	11000
klucz	D	K	_	S	E	R	K	_	Q	C	V
	00011	01010	11010	10010	00100	10001	01010	11010	10000	00010	10101
XOR	10000	01110	10000	00000	10111	01011	00011	11010	00110	01111	01101
tekst zaszyfrowany	Q	O	Q	A	X	L	D	_	G	P	N

Szyfry podstawieniowe – XOR

Idea

Tak więc tekst jawny TEKST_JAWNY przy pomocy klucza DK_SERK_QCV został zaszyfrowwany jako QOQAXLD_GPN

Deszyfrowanie przebiega dokładnie analogicznie. Spróbujmy odszyfrować tekst QEYLSHXRL5CEVJBZJOK wiedząc, że został zaszyfrowany kluczem DKCG_DNCLVKAP_QNKDO.

Szyfry podstawieniowe – XOR

Idea

tekst zaszyfrowany	Q	E	Y	L	S	H	X	R	L	5	C
klucz	D	K	C	G	_	D	N	C	L	V	K

XOR
tekst jawny

Szyfry podstawieniowe – XOR

Idea

tekst										
zaszyfrowany	Q	E	Y	L	S	H	X	R	L	5	C
	10000	00100	11000	01011	10010	00111	10111	10001	01011	11111	00010
klucz	D	K	C	G	_	D	N	C	L	V	K
	00011	01010	00010	00110	11010	00011	01101	00010	01011	10101	01010
XOR											
tekst jawny											

Szyfry podstawieniowe – XOR

Idea

tekst										
zaszyfrowany	Q	E	Y	L	S	H	X	R	L	5	C
	10000	00100	11000	01011	10010	00111	10111	10001	01011	11111	00010
klucz	D	K	C	G	_	D	N	C	L	V	K
	00011	01010	00010	00110	11010	00011	01101	00010	01011	10101	01010
XOR	10011	01110	11010	01101	01000	00100	11010	10011	00000	01010	01000
tekst jawny											

Szyfry podstawieniowe – XOR

Idea

tekst											
zaszyfrowany	Q	E	Y	L	S	H	X	R	L	5	C
	10000	00100	11000	01011	10010	00111	10111	10001	01011	11111	00010
klucz	D	K	C	G	_	D	N	C	L	V	K
	00011	01010	00010	00110	11010	00011	01101	00010	01011	10101	01010
XOR	10011	01110	11010	01101	01000	00100	11010	10011	00000	01010	01000
tekst jawny	T	O	_	N	I	E	_	T	A	K	I

Zauważmy jednak, iż w tej metodzie szyfrowania nie ma możliwości siłowego znalezienia poprawnego klucza metodą próbowania wszystkich możliwych kluczy i eliminowania wiadomości bezsensownych. Problem polega na tym, że **wykonując próby, otrzymamy wszystkie możliwe wiadomości jakie dają się zapisać na liczbie znaków równej liczbie znaków szyfrogramu** (w naszym przypadku 19). Spróbujmy odszyfrować wiadomość QEYLSHXRL5CEVJBZJOK używając kilku przykładowych kluczy

```
wiadomość           klucz               tekst jawny
QEYLSHXRL5CEVJBZJOK T3QZIOTDYFNMRDMRNUQ ?
QEYLSHXRL5CEVJBZJOK T3QZIOTDYFDVMRCTHUQ ?
QEYLSHXRL5CEVJBZJOK WPWZGOTLG5YXVD1DTUQ ?
QEYLSHXRL5CEVJBZJOK WPWZGOTLG5YJ3N1DTUQ ?
QEYLSHXRL5CEVJBZJOK T3QZIOTDYFQP1EF1QDS ?
QEYLSHXRL5CEVJBZJOK T3QZIOTDYFNKXONNYDS ?
```

Szyfry podstawieniowe – XOR

Łamanie siłowe

wiadomość	klucz	tekst jawny
QEYLSHXRL5CEVJBZJOK	T3QZIOTDYFNMRDMRNUQ	DZIS_JEST_PIEKNIE__
QEYLSHXRL5CEVJBZJOK	T3QZIOTDYFDVMRCTHUQ	DZIS_JEST_BRZYDKO__
QEYLSHXRL5CEVJBZJOK	WPWZGOTLG5YXVD1DTUQ	GLOSUJE_NA_TAK_____
QEYLSHXRL5CEVJBZJOK	WPWZGOTLG5YJ3N1DTUQ	GLOSUJE_NA_NIE_____
QEYLSHXRL5CEVJBZJOK	T3QZIOTDYFQP1EF1QDS	DZIS_JEST_SLONECZNY
QEYLSHXRL5CEVJBZJOK	T3QZIOTDYFNKXONNYDS	DZIS_JEST_POCHMURNY

Dotychczasowe wnioski

- "Szyfrowanie" przez ukrywanie może być skuteczne, ale z pewnością jest bardzo ryzykowne.
- Metoda szyfowania powinna być tak ogólna jak tylko jest to możliwe, pozwalając szyfrować dowolne komunikaty.
- Bezpieczeństwo systemu kryptogtaficznego nie może zależeć od zachowania w tajemnicy algorytmu szyfrującego. Bezpieczeństwo zależy wyłącznie od zachowania w tajemnicy klucza.
- W metodzie szyfrującej zapewnić aby ilość możliwych kluczy była na tyle duża aby nie było możliwe sprawdzenie ich wszystkich metodą siłową w akceptowalnym czasie.
- Dokument zaszyfrowany nie powinien zawierać w sposób jawny (czytelny) żadnej charakterystyki dokumentu jawnego.
- Sposób szyfrowania nie powinien dopuszczać tworzenia powtórzeń.

Ostania metoda wydaje się być idealną metodą szyfrowania – jest bardzo prosta i nie daje szans na odczytanie wiadomości. Jedyny problem z nią związany dotyczy samego klucza – aby ten sposób szyfrowania nie dopuszczał do tworzenia powtórzeń, **klucz powinien być długości równej długości szyfrowanego tekstu**. W ten oto sposób natrafiamy na zagadnienie bezpiecznego sposobu dystrybucji (przekazywania) kluczy, które jednakże samo w sobie jest zupełnie inną historią wymagającą osobnej opowieści.