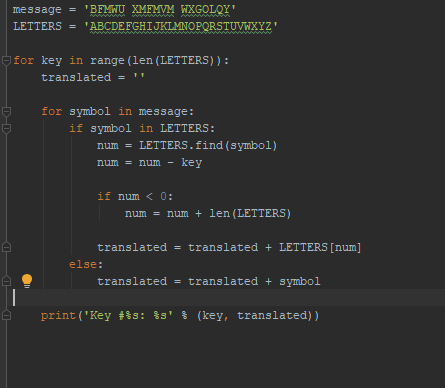
|  |  |  |
| --- | --- | --- |
| Cyberbezpieczeństwo | | Kielce,08/12/2018 |
| Laboratorium 6 |  | |
| Wyk. Foltyn Piotr, Jakub Adamski, Szymon Ciepluch, Albert Bińkowski | | Ocena: |

## Cel:

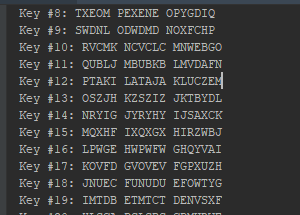
1. Złamanie szyfru drugiej część zespołu używając przygotowanego specjalnie programu
2. Zapoznanie się z kodem szyfrującym hasło
3. Opis metody deszyfrowania metodą częstotliwościową
4. Opis metody deszyfrowania metodą Vignere

## Opis:

Część 1:  
 

Kod Program deszyfrujący

Program odwraca szyfr cezara. Sprawdza po kolei wszystkie 25 liter alfabetu, a następnie korzystając z metody brute force dokonuje odszyfrowania podanego ciągu znaków zgłoszonego jako messege.  
Metoda ta sprawdza się tylko w przypadku najprostszych haseł i nie zadziała w przypadku podwójnego szyfru cezara.



Kod Odszyfrowana wiadomość

Szyfrowanie kodu:

Przykładowy sposób zaszyfrowania słowa „DOM” przy stałej = 3.

szyfrowanie litery D:

ABC**D**EFGHIJKLMNOPQRSTUVWXYZ

→ przesunięcie o 3 ->

ABCDEF**G**HIJKLMNOPQRSTUVWXYZ

szyfrowanie litery O:

ABCDEFGHIJKLMN**O**PQRSTUVWXYZ

→ przesunięcie o 3 ->

ABCDEFGHIJKLMNOPQ**R**STUVWXYZ

szyfrowanie litery M:

ABCDEFGHIJKL**M**NOPQRSTUVWXYZ

→ przesunięcie o 3 ->

ABCDEFGHIJKLMNO**P**QRSTUVWXYZ

Szyfrogram słowa „DOM” = „GRP”.

Jednym ze sposób na złamanie powyższego szyfru, jest **analiza częstości występowania danego znaku** w danym języku. Znając najczęściej występujący znak (np. w angielskim jest to litera 'e'), należy odszukać w szyfrogramie najczęściej występującą literę, na tej podstawie z kolei, odczytać klucz (przesunięcie).

**Auguste Kerckhoffs** w 1883 roku sformułował wiele praktycznych rad i opartych na doświadczeniu reguł postępowania, w tym ujęty w sześciu punktach wzór praktycznego szyfrowania:

1. System powinien być, jeśli nie teoretycznie, to w praktyce nie do złamania.

2. Projekt systemu nie powinien wymagać jego tajności, a ewentualne jego ujawnienie nie powinno przysparzać kłopotów korespondentom (zasada Kerckhoffsa).

3. Klucz powinien być: możliwy do zapamiętania bez notowania i dodatkowo – łatwy do zmienienia.

4. Kryptogramy powinny być możliwe do przesłania drogą telegraficzną.

5. Aparatura i dokumenty powinny być możliwe do przeniesienia i obsłużenia przez jedną osobę.

6. System powinien być prosty – nie wymagający znajomości wielu reguł ani nie obciążający zbytnio umysłu.

Najlepiej jest znana zasada druga, zwana zasadą Kerckhoffsa. Jej ideą jest, żeby **bezpieczeństwo kryptosystemu zależało wyłącznie od jego klucza**, natomiast by było niezależne od zachowania tajności jakiejkolwiek innej części systemu.

**Confusion and diffusion**:  
  
W kryptografii **confusion** i **diffusion** są dwiema właściwościami działania bezpiecznego szyfrowania zidentyfikowanego przez Claude'a Shannona w jego opublikowanym w 1945 roku raporcie A Mathematical Theory of Cryptography . Te właściwości, o ile są obecne, działają w celu udaremnienia stosowania statystyk i innych metod kryptoanalizy.  
Koncepcje te są również ważne w projektowaniu wydajnych funkcji skrótu i generatorów liczb pseudolosowych, w których dekorelacja wygenerowanych wartości ma ogromne znaczenie.

**Confusion** oznacza, że każda cyfra binarna (bit) tekstu zaszyfrowanego powinna zależeć od kilku części klucza, przesłaniając połączenia między tymi dwoma.

**Diffusion** oznacza, że jeśli zmienimy pojedynczy bit zwykłego tekstu, to (statystycznie) połowa bitów w zaszyfrowanym tekście powinna się zmienić, i podobnie, jeśli zmienimy jeden bit zaszyfrowanego tekstu, wówczas powinna zmienić się około połowa bitów tekstowych. Ponieważ bit może mieć tylko dwa stany, kiedy wszystkie zostaną ponownie ocenione i zmienione z jednej pozornie losowej pozycji na drugą, połowa bitów zmieni się.

## Podsumowanie:

Szyfr Cezara jest najprostrzym sposobem szyfrowania, jednak i tak lepiej jest zaszyfrować wiadomość niż wysłać ją bez jakiegokolwiek zabezpieczenia.  
Istnieje kilka zasad według których powinno się szyfrować wiadomości.