Laboratorium nr 1
„Podstawy kryptografii i kryptoanalizy”

Wprowadzenie

Klasyczne algorytmy szyfrowania danych (szyfry klasyczne) możemy podzielić na cztery grupy:

- **Proste** (monoalfabetyczne) – pojedynczy znak zastępowany jest innym znakiem pojedynczym,
- **Homofoniczne** - pojedynczy znak zastępowany jest innym znakiem pojedynczym, ale wybieranych z grupy homofonów (różnych wartości jakie może przyjąć znak),
- **Poligramowe** – szyfrowane są grupy znaków,
- **Wieloalfabetowe** – złożenie kilku prostych szyfrów podstawieniowych używanych dla różnych alfabetów.

Na wykładzie omówiliśmy szczegółowo każdą z grup oraz przeanalizowaliśmy przykładowe szyfry. Dla przypomnienia, poniżej opisane są zasady działania szyfru Playfaira i Vigenere’a.

- **Szyfr Playfair** (szyfrujemy pary liter)

  Konstruujemy macierz umożliwiającą szyfrowanie dwuznaków przy użyciu przykładowego klucza: MARCIN. Jeśli w wyrazie stanowiącym klucz, jakaś litera się powtarza to zapisujemy ją tylko jeden raz (wtedy gdy pojawia się po raz pierwszy). Pozostałe elementy wypełniamy resztą liter (w porządku alfabetycznym):

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

  Przykład szyfowania:

  WT OR EK → YQ KI DL

  Zasady:

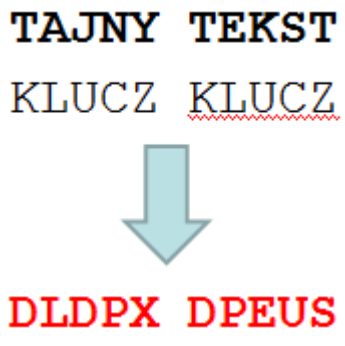
  — jeśli dwa szyfrowane znaki leżą w tym samym wierszu macierzy to zastępujemy każdy z nich jego prawostronnym następnikiem (np. SU → TP)
  — jeśli dwa szyfrowane znaki leżą w tej samej kolumnie to zastępujemy każdy z nich jego dolnym następnikiem (np. PV → VM)
  — w pozostałych przypadkach stosujemy uzupełnienie prostokątne (np. WT → YQ)

- **Szyfr Vigenère'a**

Konstruujemy macierz o takich własnościach że każdy kolejny wiersz i każda kolejna kolumna zawiera alfabet przesunięty o jedną literę:

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

Szyfrując pierwszą literę tekstu (szukamy jej w pierwszym wierszu) przy użyciu pierwszej litery klucza (szukamy jej w pierwszej kolumnie), jako wynik otrzymujemy literę, która pojawia się na przecięciu wiersza z kolumną. Przykładowo:



Ćwiczenia

1. Proszę uruchomić komputery i na pulpicie stworzyć nowy katalog „*bezpieczenstwo*”. W tym katalogu proszę przechowywać wszystkie pliki, które będą wykorzystywane podczas zajęć. Po zakończeniu zajęć – proszę usunąć katalog wraz z całą zawartością.

Prosty (monoalfabetyczny) szyfr podstawieniowy

czyli dlaczego dawniej szyfrogramy łamali lingwiści

2. Pierwszym ćwiczeniem będzie złamanie poniższego szyfrogramu:

   WXQOWK LXCFRXBCXUAWJO R URXLXCFRXBCXUAWJO J AKAWXQOBM WXNXRUSDEQOWKBCUKBM FDEPACOQK UO NOLDEOWDEROBM

   Wiemy że szyfrogram powstał przy użyciu prostego szyfru podstawieniowego, zatem znaki zdradzają strukturę języka (polskiego).

   Wskazówki:

   - sprawdź jaka jest częstość występowania poszczególnych liter w języku polskim. Aby ułatwić zliczanie znaków w szyfrogramie, warto użyć programów takich jak: http://jumk.de/wortanalyse/word-analysis.php lub http://www.csgnetwork.com/documentanalystcalc.html
   - zwróć uwagę na najczęściej występujące litery oraz na najpopularniejsze dwuznaki i trójznaki w języku polskim
   - w szyfrogramie zachowano podział na wyrazy (spacje są w odpowiednich miejscach)

Szyfr homofniczny

czyli jak utrudnić pracę lingwiście

3. Zaproponuj własny szyfr homofoniczny i zaszyfruj nim tekst jawny z poprzedniego ćwiczenia. Nowy szyfr homofoniczny powinien zamaskować charakterystykę językową tekstu jawnego. Jako alfabetu stosowanego w szyfrogramie możesz użyć liczb dwucyfrowych.

   Narysuj dwa wykresy przedstawiające ilość wystąpień każdego znaku w szyfrogramie:

   - dla prostego szyfru podstawieniowego (z pierwszego ćwiczenia)
   - dla Twojego szyfru homofonicznego

   Skomentuj oba wykresy.

Poligramowy szyfr Playfaira

czyli jak bezpieczne były (a może są?) szyfry wojskowe…

4. Gdy kuter torpedowy PT-109, dowodzony przez podporucznika J.F. Kennedy'ego (późniejszego prezydenta Stanów Zjednoczonych), został zatopiony przez japoński niszczyciel „Amagiri", 2 sierpnia 1943 roku w australijskiej stacji odbiorczej odebrano następujący szyfrogram utworzony przy użyciu szyfru Playfaira:

   KXJEY UREBE ZWEHE WRYTU HEYFS
   KREHE GOYFI WTTTU OLKSY CAJPO
   BOTEI ZONTX BYBWT GONEY CUZWR
   GDSON SXBOU YWRHE BAAHY USEDQ

   Rozszyfruj wiadomość wiedząc że marynarka wojenna zwykle używała klucza: **ROYAL NEW ZEALAND NAVY**

   (Uwaga: dwuznak 'TT' w szyfrogramie odpowiadał dwuznakowi 'TT' w teście jawnym)

Wieloalfabetowy szyfr Vigenère'a

czyli dlaczego one-time-pad jest bezpieczny

5. Przy użyciu szyfru Vigenere'a z kluczem '**OFSTH**' zaszyfrowano wyraz '**KOTEK**'. Otrzymano szyfrogram '**YTLXR**' (proszę sprawdzić czy szyfrogram nie ma błędów).

   Ponieważ klucz ma taką samą długość jak tekst jawny oraz został wygenerowany w sposób losowy, zaszyfrowana wiadomość jest bezpieczna (analogia do szyfru *one-time-pad*). Dlaczego? Jeśli nie znamy klucza to jesteśmy zmuszeni sprawdzić wszystkie jego kombinacje. Wtedy, jako wynik deszyfrowania dostaniemy wszystkie możliwe wyrazy pięcioliterowe (również wszystkie te które mają sens). Przykładowo, proszę odszyfrować tekst przy użyciu klucza '**XFZWR**'.

   Jako ćwiczenie proszę wymyślić dowolne słowo pięcioliterowe. Następnie znaleźć klucz, za pomocą którego można odszyfrować podany szyfrogram (czyli 'YTLXR') otrzymując wymyślone przez siebie słowo.

Szyfr Beale'a

czyli jak zostać właścicielem skarbu wartego 63 mln dolarów

6. Historia zna wiele zaszyfrowanych/zakodowanych wiadomości, które do tej pory nie zostały odczytane. Część z nich związana jest z barwnymi opowieściami o ukrytych skarbach. Jednym z nich jest szyfr Beale'a. Na osobę, która zdoła odczytać wiadomość, podobno czeka ok. 63 mln dolarów w złocie, srebrze i klejnotach.

„Skarb miał należeć do Thomasa Jeffersona Beale'a, który ukrył go gdzieś w stanie Virginia w USA. Pudełko zawierające zaszyfrowane informacje dotyczące skarbu oddał zaprzyjaźnionemu Robertowi Morrisowi na przechowanie. Mężczyzna obiecał nie otwierać go przez 10 lat, ale jeśli Beale przez ten czas się po nie zgłosi, mógł to zrobić. Gdy nikt nie przyjechał, Morris otworzył pudełko i próbował rozszyfrować trzy zawarte w nim wiadomości. Na próżno. W końcu pod koniec życia oddał je przyjacielowi Jamesowi B Wardowi, który spędził dwadzieścia lat na rozszyfrowywaniu dokumentów. Przy pomocy tekstu Deklaracji niepodległości Stanów Zjednoczonych udało mu się odczytać tylko jeden z dokumentów. Pozostałe dwa opublikował w 1885 roku w broszurze: The Beale Papers."[1]

Znajdź w Internecie trzy zaszyfrowane dokumenty. Pierwszy tekst - opisuje lokalizację, drugi (jako jedyny rozwiązany) – zawartość skarbca, a trzeci – wymienia nazwiska właścicieli skarbu i ich krewnych. Spróbuj je odszyfrować. Jeśli Ci się uda – będziesz zwolniony z egzaminu ☺

Sprawozdanie

W sprawozdaniu z laboratorium nr 1 należy opisać wykonane ćwiczenia i ich wyniki. W szczególności należy odpowiedzieć na zadane pytania. Dodatkowo we wnioskach (lub wstępie) należy wyjaśnić zasadę działania szyfrów podstawieniowych i przedstawieniowych oraz odpowiedzieć na pytanie dlaczego szyfr **one-time-pad** jest uważany za bezpieczny.

[1] Tekst pochodzi ze strony: http://niewiarygodne.pl/gid,15402335,img,15402424,kat,1017185,page,12,title,10-tajemniczych-tekstow-ktorych-nie-udalo-sie-rozszyfrowac,galeriazdjecie.html?smgajticaid=616946