## I. Kryptoanaliza monoalfabetycznego szyfru podstawieniowego

W kryptoanalizie korzysta się z analizy częstości występowania poszczególnych liter alfabetu.

ALFABET ANGIELSKI

- Prawdopodobieństwo wystąpienia 26 liter alfabetu języka angielskiego

| A | B | C | D | E | F | G | H | I | J | K | L | M |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0,082 | 0,015 | 0,028 | 0,043 | 0,127 | 0,022 | 0,020 | 0,061 | 0,070 | 0,002 | 0,008 | 0,040 | 0,024 |
| N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| 0,067 | 0,075 | 0,019 | 0,001 | 0,060 | 0,063 | 0,091 | 0,028 | 0,010 | 0,023 | 0,001 | 0,020 | 0,001 |

- Słowa jednoliterowe to z reguły I lub A.
- Najczęściej występujące słowa trzyliterowe to AND lub THE.
- Podział zbioru liter na 5 grup
  - E ok. 0,12
  - T, A, O, I, N, S, H, R ok. 0,06-0,09
  - D, L ok. 0,04
  - C, U, M, W, F, G, Y, P, B ok. 0,015-0,028
  - V, K, J, X, Q, Z ok. 0,01
- Grupy liter
  - 30 najczęściej występujących grup dwuliterowych (w porządku malejącym)
    TH, HE, IN, ER, AN, RE, ED, ON, ES, ST, EN, AT, TO, NT, HA, ND, OU, EA, NG, AS, OR, TI, IS, ET, IT, AR, TE, SE, HI, OF
  - 13 najczęściej występujących grup trzyliterowych (w porządku malejącym)
    THE, ING, AND, HER, ERE, ENT, THA, NTH, WAS, ETH, FOR, DTH

ALFABET POLSKI
http://docs8.chomikuj.pl/294087016,0,0,Cz%C4%99sto%C5%9B%C4%87-wyst%C4%99powania-liter-w-j%C4%99zyku-polskim.doc

- w kolejności alfabetycznej

| A | Ą | B | C | Ć | D | E | Ę | F | G | H | I | J |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 8,61% | 1,11% | 1,49% | 3,82% | 0,56% | 3,33% | 8,78% | 1,40% | 0,36% | 1,40% | 0,93% | 8,65% | 2,81% |
| K | L | Ł | M | N | Ń | O | Ó | P | R | S | Ś | T |
| 2,95% | 2,19% | 1,36% | 3,35% | 5,60% | 0,12% | 7,34% | 0,79% | 2,74% | 3,72% | 4,17% | 0,84% | 4,30% |
| U | W | Y | Z | Ź | Ż | | | | | | | |
| 2,05% | 4,25% | 3,85% | 5,67% | 0,06% | 1,24% | | | | | | | |

- w kolejności częstości występowania

| E | I | A | O | Z | N | T | W | S | Y | C | R | M |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 8,78% | 8,65% | 8,61% | 7,34% | 5,67% | 5,60% | 4,30% | 4,25% | 4,17% | 3,85% | 3,82% | 3,72% | 3,35% |
| D | K | J | P | L | U | B | Ę | G | Ł | Ż | Ą | H |
| 3,33% | 2,95% | 2,81% | 2,74% | 2,19% | 2,05% | 1,49% | 1,40% | 1,40% | 1,36% | 1,24% | 1,11% | 0,93% |
| Ś | Ó | Ć | F | Ń | Ź | | | | | | | |
| 0,84% | 0,79% | 0,56% | 0,36% | 0,12% | 0,06% | | | | | | | |

---

**[Zadanie 01]**
Zaimplementuj narzędzie ułatwiające kryptoanalizę tekstu zaszyfrowanego monoalfabetycznym szyfrem podstawieniowym (dla tekstów angielskich). Przetestuj program na szyfrogramieH UINF NIAP NIAP OCSO H UINF INOCHIT. (tekst angielski)

---

**[Zadanie 02]**
Zaimplementuj narzędzie ułatwiające kryptoanalizę tekstu zaszyfrowanego monoalfabetycznym szyfrem podstawieniowym (dla tekstów polskich). Przetestuj program na szyfrogramie w języku polskim.

---