

[BSS]-Lab1-śr16-KrzysztofRudnicki

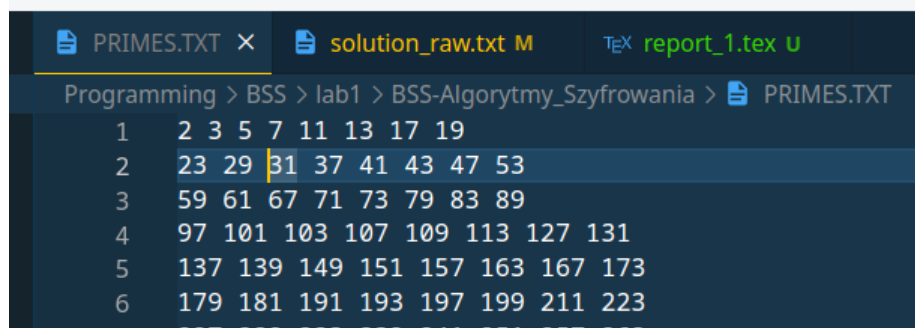
Krzysztof Rudnicki

March 28, 2024

1 Generacja kluczy

Wybrane liczby Wybrałem najniższe liczby pierwsze z przedziału 30 - 100
p - 31, q - 37

Sprawdziłem że liczby 31 i 37 są pierwsze



```
PRIMES.TXT x solution_raw.txt M TeX report_1.tex U
Programming > BSS > lab1 > BSS-Algorytmy_Szyfrowania > PRIMES.TXT
1 2 3 5 7 11 13 17 19
2 23 29 31 37 41 43 47 53
3 59 61 67 71 73 79 83 89
4 97 101 103 107 109 113 127 131
5 137 139 149 151 157 163 167 173
6 179 181 191 193 197 199 211 223
7 227 229 233 239 241 251 257 263
```

$$n = p * q = 31 * 37 = 1147$$

$$\rho(n) = (p - 1) * (q - 1) = 30 * 36 = 1080$$

Wybrałem liczbę e = 29 Sprawdziłem, że jest względnie pierwsza względem 1080

NWD M

Pierwsza liczba:

Druga liczba:

$$\text{NWD}(29, 1080) = 1$$

Liczba $d = 149$

Odwrotność w grupie modulo r

Baza:

Moduł:

$$29^{-1} \bmod 1080 = 149$$

Klucz publiczny: $e = 29$, $n = 1147$
Klucz prywatny: $d = 149$, $n = 1147$

2 Szyfrowanie

Fraza: DYZIO, litera: C

Zakodowana Frazą: 68, 89, 90, 73, 79
Zakodowana litera: 67

Przygotowana wiadomość: PTAKI LATAJA KLUCZEM

Wiadomość zaszyfrowana kluczem sesyjnym: KPWEB FWPWCW
EFQDVZG

The image shows two screenshots of a cryptographic software interface. The top screenshot shows the 'Szyfr frazowy' (Phrase cipher) tab selected. The 'Fraza' (Phrase) field contains 'DYZIO' and the 'Litera' (Letter) field contains 'C'. Below the fields, a table of letters is displayed: 'ABCDEFGHIJKLMNOPQRSTUVWXYZ' and 'WXDYZIOABCEFGHJKLMNPQRSTU'. The 'PTAKI LATAJA KLUCZEM' message is entered in the text area. The bottom screenshot shows the same interface, but the 'Frazą' (Phrase) field now contains 'KPWEB FWPWCW EFQDVZG'.

Klucz pobrany od kolegi: $e_2 = 11$, $n_2 = 1763$

Zaszyfrowany klucz sesyjny
Frazą: 168, 1621, 1632, 665, 178
Litera: 1734

Potęgowanie w grupie modulo r

Podstawa:

Wykładnik:

Moduł:

$68^{11} \bmod 1763 = 167$

Klucz sesyjny przed zakodowaniem: DYZIO, C

Po Zakodowaniu: 68, 89, 90, 73, 79, __67__

Po Zaszyfrowaniu: 168, 1621, 1632, 665, 178, __1734__

Wiadomość przed zaszyfrowaniem: PTAKI LATAJA KLUCZEM

Wiadomość po zaszyfrowaniu: KPWEB FWPWCW EFQDVZG

3 Odszyfrowanie

Otrzymałem klucz sesyjny: 423 65 693 1100 8 __1073__

Odszyfrowałem go korzystając z mojego klucza prywatnego Klucz prywatny: $d = 149$, $n = 1147$

Odszyfrowany klucz sesyjny: 107, 114, 48, 122, 97, __111__

Potęgowanie w grupie modulo r

Podstawa: 423

Wykładnik: 149

Moduł: 1147

Oblicz potęgę

$423^{149} \bmod 1147 = 107$

Odszyfrowany klucz sesyjny odkodowałem: kryza, o

Otrzymałem wiadomość: QNVVK XSLN BK WNNB GKC

Menu

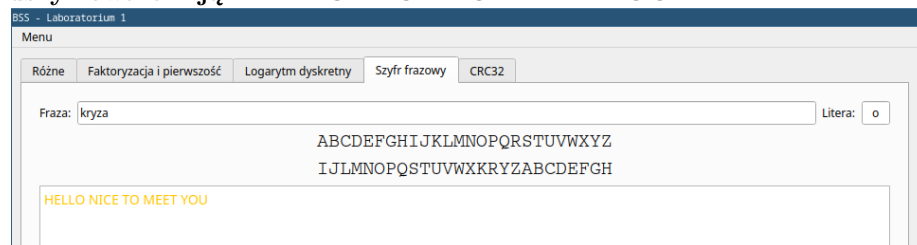
Różne Faktoryzacja i pierwszość Logarytm dyskretny Szyfr frazowy CRC32

Fraza: kryza Litera: o

ABCDEFGHIJKLMNOPQRSTUVWXYZ
IJKLMNOPQRSTUVWXYZABCDEFGHI

QNVVK XSLN BK WNNB GKC

Odszyfrowałem ją: **HELLO NICE TO MEET YOU**



Otrzymany klucz sesyjny zaszyfrowany: 423 65 693 1100 8 __1073__
po odszyfrowaniu: 107, 114, 48, 122, 97, __111__
po odkodowaniu: kryza, o

Wiadomość zaszyfrowana: QNVVK XSLN BK WNNB GKC
Wiadomość odszyfrowana: **HELLO NICE TO MEET YOU**

4 Łamanie klucza prywatnego