

# [BSS]-Lab1-śr16-KrzysztofRudnicki

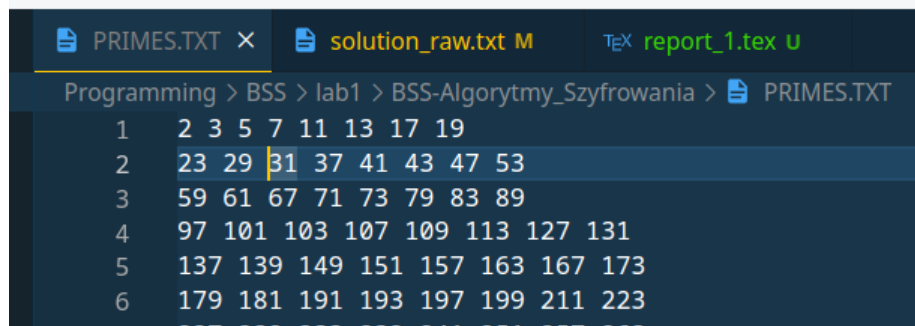
Krzysztof Rudnicki

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:

29

Druga liczba:

1080

Oblicz NWD

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

Liczba  $d = 149$

Odwrotność w grupie modulo r

Baza:

29

Moduł:

1080

Odwróć

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

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 application interface. The top screenshot shows the 'Szyfr frazowy' (Phrase cipher) tab selected. The 'Fraza' (Phrase) field contains 'DYZIO' and the 'Litera' (Letter) dropdown is set to 'C'. Below the input fields, a 2x26 grid of letters is displayed, with the first row being 'ABCDEFGHIJKLMN OPQRSTUVWXYZ' and the second row being 'WXDYZIOABCEFGHJKLMNPQRSTU V'. The output field shows the plaintext 'PTAKI LATAJA KLUCZEM'. The bottom screenshot shows the same interface, but the output field now displays the ciphertext 'KPWEB FWPWCW EFQDVZG'.

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

Zaszyfrowany klucz sesyjny  
Fraza: 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:

Wykładnik:

Moduł:

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

Odszyfrowany klucz sesyjny odkodowałem: kryza, o

Otrzymałem wiadomość: QNVVK XSLN BK WNNB GKC

Menu

Różne Faktoryzacja i pierwszość Logarytm dyskretny Szyfr frazowy CRC32

Fraza:  Litera:

ABCDEFGHIJKLMNOPQRSTUVWXYZ  
IJKLMNOPQRSTUVWXYZABCDEFGHI

**QNVVK XSLN BK WNNB GKC**

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

The screenshot shows a web application titled "B55 - Laboratorium 1". It has a "Menu" bar with tabs: "Różne", "Faktoryzacja i pierwszość", "Logarytm dyskretny", "Szyfr frazowy", and "CRC32". The "Szyfr frazowy" tab is active. Below the menu, there is a "Fraza:" input field containing "kryza" and a "Litera:" dropdown menu set to "o". Below these, there are two rows of alphabet characters: "ABCDEFGHIJKLMNOPQRSTUVWXYZ" and "IJKLMNOPQRSTUVWXYZABCDEFGHI". At the bottom, a text box displays the decrypted message "HELLO NICE TO MEET YOU" in orange text.

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

Z klucza publicznego otrzymałem  $n_2 = 1763$

Dokonałem faktoryzacji klucza publicznego  $n = 43 \cdot 41$ ,  $p = 43$ ,  $q = 41$

The screenshot shows a web application with two side-by-side panels for factoring. The left panel is titled "Faktoryzacja Pollard rho" and the right panel is titled "Faktoryzacja Pollard p-1". Both panels have a "Liczba do faktoryzacji:" label above an input field containing "1763". Below the input field is a "Faktoryzuj" button. At the bottom of each panel, the result of the factoring is displayed: "1763 = 43 · 41".

Wyzaczyłem  $\phi(n) = (p - 1) \cdot (q - 1) = 42 * 40 = 1680$

Przygotowania do algorytmu Shanksa

$c = 168, 1621, 1632, 665, 178 \text{ } \underline{1734}$

$m = 68, 89, 90, 73, 79, \text{ } \underline{67}$

$n_2 = 1763$

**Algorytm Shanksa** Algorytm z programu był dość zawodny, często nie dawał żadnych rezultatów, na przykład dla  $a = 168, y = 68, n = 1763$

**x=log<sub>a</sub>y (mod n)**

Shanks

Znajdź logarytm

a: 168

y: 68

n: 1763

Nie znaleziono logarytmu

Log

Algorytm zadziałał dla  $a_1 = 1632, y_1 = 90, n = 1763$  dając wynik  $d_s = 121$

Algorytm zadziałał dla  $a_2 = 665, y_2 = 73, n = 1763$  dając wynik  $d_s = 23$

Algorytm zadziałał dla  $a_3 = 178, y_3 = 79, n = 1763$  dając wynik  $d_s = 35$

Algorytm zadziałał dla  $a_4 = 1734, y_4 = 67, n = 1763$  dając wynik  $d_s = 275$

$x = \log_a y \pmod n$

Shanks

Lo

Znajdź logarytm

a:

y:   $\log_{1734} 67 \pmod{1763} = 275$

n:

Log

Sprawdziłem czy otrzymane wartości  $d_s$  spełniają wymaganie  $e \cdot d_s \pmod{\phi(n)}$

$$e = 11, d_s = \{121, 23, 35, 275\}, n = 1763, \phi(n) = 1680$$

$$11 \cdot \mathbf{121} \pmod{1680} = 1331$$

$$11 \cdot \mathbf{23} \pmod{1680} = 253$$

$$11 \cdot \mathbf{35} \pmod{1680} = 385$$

$$11 \cdot \mathbf{275} \pmod{1680} = 1345$$



#### Mnożenie w grupie moduł

Czynnik:

11



Moduł:

1680

Czynnik:

121



Pomnóż

$$11 \cdot 121 \bmod 1680 = 1331$$

Żadna z tych wartości nie spełnia wymagań

Następnie posłużyłem się metodą brutalną dla wartości które zadziały przy Algorytmie Shanksa

Log n		
a:	<input type="text" value="1632"/>	<div>51</div> <div>191</div>
y:	<input type="text" value="90"/>	<div>331</div> <div>471</div>
n:	<input type="text" value="1763"/>	<div>611</div> <div>751</div> <div>891</div> <div>1031</div> <div>1171</div> <div>1311</div> <div>1451</div> <div>1591</div> <div>1731</div>

Log n

a:	665	23
		107
y:	73	191
		275
n:	1763	359
		443
		527
		611
		695
		779
		863
		947
		1031
		1115
		1199
		1283
		1367
		1451
		1535
		1619
		1703

Log n

a:

178

y:

79

n:

1763

11  
35  
59  
83  
107  
131  
155  
179  
203  
227  
251  
275  
299  
323  
347  
371  
395  
419  
443  
467  
491  
515  
539  
563  
587  
611  
635  
659  
683  
707  
731  
755  
779  
803  
827  
851  
875  
899  
923  
947  
971  
995  
1019  
1043  
1067  
1091<sup>12</sup>  
1115  
1139  
1163  
1187

Znajdź logarytm

Log n

a:	<input type="text" value="1734"/>	611 1451
y:	<input type="text" value="67"/>	
n:	<input type="text" value="1763"/>	

Dla  $e = 11$ ,  $n = 1680$ , i  $d = 611$

Mnożenie w grupie moduł

Czynnik:	<input type="text" value="11"/>	Moduł:	<input type="text" value="1680"/>
Czynnik:	<input type="text" value="611"/>	<input type="button" value="Pomnóż"/>	

$11 \cdot 611 \bmod 1680 = 1$

$d = 611$  jest jednym z elementów klucza prywatnego, drugim jest  $n_2 = 1763$

## 5 Podpis Cyfrowy CRC

Dla tekstu: **PTAKI LATAJA KLUCZEM**, wyznaczyłem wartość CRC:  
**2457674121**

Różne	Faktoryzacja i pierwszość	Logarytm dyskretny	Szyfr frazowy	CRC32
-------	---------------------------	--------------------	---------------	-------

PTAKI LATAJA KLUCZEM

CRC32	hex=0x927D2189	dec=2457674121
-------	----------------	----------------

Podzieliłem na mniejsze grupy: 24, 57, 67, 41, 21

Zaszyfrowałem wartość crc

$d = 149$ ,  $n = 1147$

Podpis cyfrowy: 890, 1091, 583, 617, 189

Wiadomość: PTAKI LATAJA KLUCZEM  
Obliczona wartość CRC: 2457674121  
Klucz prywatny:  $d = 149$ ,  $n = 1147$ ,

Potęgowanie w grupie modulo  $r$

Podstawa:

Wykładnik:

Moduł:

Oblicz potęgę

$$24^{149} \bmod 1147 = 890$$

Podpis cyfrowy: 890, 1091, 583, 617, 189