

# Szyfrowanie RSA

Stefan Sokołowski

Elbląg, 16 V 2025

Założmy, że

- (a)  $p$  i  $q$  są różnymi (dużymi) liczbami pierwszymi,  $r = p \cdot q$ ;  
wtedy funkcja Eulera wyraża się tak:  $\varphi(r) = (p - 1) \cdot (q - 1)$ ;
- (b)  $e \in \{2, 3, \dots, r - 1\}$  jest względnie pierwsze z  $\varphi(r)$ .

## Klucz jawny i szyfrowanie:

Kluczem jawnym jest para  $(r, e)$  (czynniki  $p$  i  $q$  **nie są** ujawniane). Szyfrowanie liczby  $L \in \{1, 2, \dots, r - 1\}$ :

$$L \mapsto C = L^e \bmod r$$

## Klucz tajny i odszyfrowywanie:

Kluczem tajnym jest para  $(r, d)$ , gdzie  $d$  jest odwrotnością liczby  $e$  modulo  $\varphi(r)$ :

$$e \cdot d \equiv_{\varphi(r)} 1 \tag{1}$$

Znając  $p$  i  $q$  możemy wyznaczyć  $\varphi(r)$ , a następnie  $d$  (przez rozszerzony algorytm Euklidesa); ale znając tylko  $r$  nie możemy tego zrobić, bo rozkład  $r$  na iloczyn  $p \cdot q$  jest trudny obliczeniowo.

Odszyfrowanie dokonuje się przez:

$$C \mapsto L' = C^d \bmod r$$

## Zadanie 1:

Wyznaczyć wzór na szyfrowanie kluczem publicznym (jawnym) oraz wzór na odszyfrowywanie w oparciu o liczby pierwsze  $p = 19$  i  $q = 47$  oraz liczbę  $e = 5$ . Zilustrować szyfrowanie oraz odszyfrowywanie liczb 413 oraz 38.

## Rozwiązanie:

Liczymy iloczyn  $r = pq = 19 \cdot 47 = 893$ . Ogłaszamy parę  $(r, e) = (893, 5)$  jako **klucz jawny**. Dla wyznaczenia klucza tajnego należy znaleźć takie  $d$ , żeby

$$5 \cdot d + 828 \cdot k = 1 \quad \text{dla pewnego } k$$

Z rozszerzonego algorytmu Euklidesa wynika, że  $d = 497$ . Wobec tego za **klucz tajny** będzie służyć para  $(r, e) = (893, 497)$ .

**Szyfrowanie liczby 413:**

$$C \equiv_{893} 413^5 \equiv_{893} 580$$

Odszyfrowywanie liczby 580:

$$\begin{aligned} L &\equiv_{893} 580^{497} \equiv_{893} (580^{10})^{49} \cdot 580^7 \equiv_{893} 788^{49} \cdot 737 \equiv_{893} (788^{10})^4 \cdot 788^9 \cdot 737 \\ &\equiv_{893} 465^4 \cdot 761 \cdot 737 \equiv_{893} 766 \cdot 53 \equiv_{893} 413 \end{aligned}$$

**Szyfrowanie liczby 38:**

$$C \equiv_{893} 38^5 \equiv_{893} 171$$

Odszyfrowywanie liczby 171:

$$\begin{aligned} L &\equiv_{893} 171^{497} \equiv_{893} (171^{10})^{49} \cdot 171^7 \equiv_{893} 874^{49} \cdot 608 \equiv_{893} (874^{10})^4 \cdot 874^9 \cdot 608 \\ &\equiv_{893} 380^4 \cdot 779 \cdot 608 \equiv_{893} 209 \cdot 342 \equiv_{893} 38 \end{aligned}$$

---

## Zadanie 2:

Wyznaczyć wzór na szyfrowanie oraz wzór na odszyfrowywanie RSA jeśli

(a)  $p = 17, q = 59, e = 5$

(b)  $p = 23, q = 31, e = 29$

W każdym z tych przypadków wyliczyć zaszyfrowaną postać liczby  $L = 300$  oraz odszyfrowaną postać wyniku tego szyfrowania.

---

## ZABAWA W SZYFROWANIE

1. Proszę dobrać się w grupy po 3–4 osoby.
  2. Każda grupa wymyśla własny klucz prywatny i publiczny szyfrowania RSA; wielkość  $r$  w kluczu publicznym powinna być liczbą 4-cyfrową, a  $e$  2-cyfrową.
  3. Każda grupa wypisuje na tablicy swój **identyfikator** (wymyśloną nazwę) oraz **klucz publiczny** (prywatny zachowuje w tajemnicy).
  4. Każda grupa dostaje ode mnie wiadomość (liczbę) zaszyfrowaną jej kluczem, odszyfrowuje ją i postać odszyfrowaną wypisuje na tablicy.
  5. Wyznaczona **przeze mnie** osoba z grupy opowiada, w jaki sposób odszyfrowywano; proszę zadbać, żeby **wszyscy** to rozumieli.
  6. Za poprawne odszyfrowanie i opowiedzenie członkowie grupy otrzymują po 5 pkt. (pół sprawdzianu).
-