# Spis treści

**1 RSA** **1**
1.1 Definicja . . . . . 1
1.2 Trudność problemu . . . . . 1
1.3 Przykład . . . . . 1

# 1 RSA

Asymetryczny algorytm szyfrujący, w którym każda strona ma parę kluczy: publiczny i prywatny. Enkrypcja odbywa się przy pomocy klucza publicznego drugiej strony, a dekrypcja przy pomocy klucza prywatnego.

## 1.1 Definicja

Dla danych liczb pierwszych $p$ i $q$.

$$n = pq$$

$$\varphi(n) = (p-1)(q-1)$$

Następnie wybieramy liczbę $e$ względnie pierwszą z $\varphi(n)$. Klucz prywatny $d$ musi spełniać warunek $ed \equiv 1 \pmod{\varphi(n)}$, zatem

$$d = e^{-1} \pmod{\varphi(n)}$$

$(n, e)$ tworzy klucz publiczny, a $(n, d)$ klucz prywatny.

Szyfrowanie wiadomości $M$ odbywa się za pomocą wzoru:

$$C = M^e \pmod{n}$$

Odkrycie wiadomości $M$ odbywa się za pomocą wzoru:

$$M = C^d \pmod{n}$$

## 1.2 Trudność problemu

Trudność wynika ze znalezienia $\varphi(n)$, a ponieważ weryfikacja czy znalezione $\varphi(n)$ jest poprawne wymaga zastosowania rozszerzonego algorytmu Euklidesa; odszyfrowanie wiadomości $C$ wymaga znalezienia $d$.

## 1.3 Przykład

$$p = 7, q = 11 \Rightarrow n = 77, \varphi(n) = 60$$

$$e = 13 \Rightarrow d = 37 \Rightarrow \begin{cases} (n, e) = (77, 13) \\ (n, d) = (77, 37) \end{cases}$$

$$M = 15 \Rightarrow C = 15^{13} \pmod{77} = 64$$

$$C = 64 \Rightarrow M = 64^{37} \pmod{77} = 15$$