

### Piotr Dondalski – kolokwium 1 (Algorytm RSA)

$$p = 5$$

$$q = 7$$

$$e = 23$$

Moduł n:

$$n = p * q = 5 * 7 = 35$$

Funkcja Eulera (moduł fi):

$$fi = (p-1) * (q-1)$$

$$fi = (5-1) * (7-1) = 24$$

Wyznaczamy następnie wykładnik prywatny d, który ma być odwrotnością modulo fi liczby e

$$d * 23 \bmod 24 = 1$$

Liczbą spełniającą ten warunek jest 23, więc:

$$d = 23$$

klucz publiczny (e, n): (23,35)

klucz tajny (d, n): (23,35)

Szyfrowanie liczby 9:

$$t = 9$$

$$c = 9^{23} \bmod 35 = 4$$

$$c = 4 \quad \leftarrow \text{zaszyfrowana liczba 9}$$

Odszyfrowanie:

$$t = 4^{23} \bmod 35 = 9$$

$$t = 9 \quad \leftarrow \text{odszyfrowana liczba 9}$$

Klucz działa poprawnie, nastąpiło prawidłowe zaszyfrowanie i odszyfrowanie.

Użyte strony WWW i Aplikacje:

kalkulator naukowy, [https://eduinf.waw.pl/inf/alg/001\\_search/0009.php](https://eduinf.waw.pl/inf/alg/001_search/0009.php)

[https://eduinf.waw.pl/inf/alg/001\\_search/0067.php?fbclid=IwAR3RT0jJ90gKHTzI-k7hKoRVhTv5Yt2xx\\_sHLQqTg9ck6lp2j-fMKFDwl4g](https://eduinf.waw.pl/inf/alg/001_search/0067.php?fbclid=IwAR3RT0jJ90gKHTzI-k7hKoRVhTv5Yt2xx_sHLQqTg9ck6lp2j-fMKFDwl4g)