Zadanie 1. Szyfrowanie RSA. Wykorzystaj podane na wykładach algorytmy do rozwiązania poniższych zadań[1].

a) Sprawdź, że liczby $p = 2903$ i $q = 4091$ są prawdopodobnie pierwsze z poziomem ufności 95 % (tj. $\Pr(p \notin \mathbb{P}) \leqslant 0{,}05$ i $\Pr(q \notin \mathbb{P}) \leqslant 0{,}05$). (2 p.)

b) Niech $n = pq$. Niech $e = 4097$. Sprawdź, że $\operatorname{nwd}(n, e) = 1$, oraz znajdź d takie, aby zachodziło

$$ed \equiv 1 \pmod{(p-1)(q-1)}.$$

(2 p.)

c) Zamień wiadomość „`Att`” na wartość liczbową w następujący sposób:

$$m = \mathrm{ASCII}(\texttt{A}) \cdot 256^2 + \mathrm{ASCII}(\texttt{t}) \cdot 256 + \mathrm{ASCII}(\texttt{t}) \tag{1}$$

i zaszyfrują ją jako $c \equiv m^e \pmod{n}$. (2 p.)

d) Odszyfruj kryptogram $c = 128\,895$ wg reguły $m \equiv c^d \pmod{n}$ i skonwertuj na 3-literowy łańcuch textowy wg wzoru

$$\begin{aligned}
\mathrm{ASCII}(z_1) &= \left\lfloor \frac{c}{256^2} \right\rfloor, \\
\mathrm{ASCII}(z_2) &= \left\lfloor \frac{c \mod 256^2}{256} \right\rfloor, \\
\mathrm{ASCII}(z_3) &= c \mod 256
\end{aligned}$$

(odwrócenie wzoru (1)). (2 p.)

e) Zaatakuj schemat szyfrowania, rozkładając na czynniki pierwsze moduł $n = 11\,876\,173$ za pomocą algorytmu ρ Pollarda. (2 p.)

[1] Rozwiąż zadanie za pomocą napisanych samodzielnie programów (języki: C/C++, Java, Python, Fortran, Bash) lub przez obliczenia na kartce. W przesłanym rozwiązaniu zamieść programy (w archiwum `.zip`) lub obliczenia (operacje arytmetyczne na liczbach naturalnych można wykonać za pomocą kalkulatora).