Kryptografia
Laboratorium nr 5

Stefan Sokołowski

Zadanie 1 (rozkład na czynniki)**:**

Proszę napisać program rozkładający daną liczbę naturalną $n \geqslant 2$ na iloczyn liczb pierwszych; np.

$$60 \quad \longrightarrow \quad 2 \cdot 2 \cdot 3 \cdot 5$$

Proszę przetestować program dla jakichś dużych liczb i zwrócić uwagę na jego czas działania ($\pi \times$oko...). Żeby liczba mogła być **naprawdę** duża, należy użyć jakiegoś typu „długich” `int`-ów zamiast zwykłych.

Zadanie 2 (RSA)**:**

Proszę przećwiczyć szyfrowanie/odszyfrowywanie RSA w następujący sposób:

1. Podzielić się na grupy po 2–3 osoby.
2. Każda grupa powinna wymyślić własne klucze RSA publiczny (n, e) i prywatny (n, d) szyfrowania RSA[1]; wielkość n w kluczu publicznym powinna być liczbą 4-cyfrową, a e 2-cyfrową.
3. Następnie proszę podać do wiadomości (np. wypisać na tablicy) klucz publiczny, a prywatny zachować w tajemnicy.
4. W końcu proszę przyjąć ode mnie ciąg liczb — zaszyfrowanych kluczem publicznym pojedynczych znaków ASCII — odszyfrować własnym kluczem prywatnym każdą z nich i całość podać do wiadomości.

Uwaga:

W zasadzie wystarczy zaprogramować odszyfrowywanie pojedynczej liczby, a następnie ręczna zamiana na znak ASCII. Ale patrz następne zadanie.

Zadanie 3 (RSA)**:**

Program z zad. 2 tak poprawić, żeby wczytywał ciąg liczb i drukował od razu odszyfrowany tekst, a nie pojedynczy znak.

---

[1] Por. `stefan.info.pl/Dydaktyka/Krypto/Slajdy/04a.pdf` str. 4.