Nr. albumu: 210254
Imię i nazwisko:
Patryk Lisik

Nr. albumu: 210310
Imię i nazwisko:
Adam Sadowski

Nr. albumu: 210279
Imię i nazwisko:
Barbara
Morawska

Kierunek: Informatyka
rok akademicki: 2018/2019
grupa poniedziałek 12:30

Kryptografia

Szyfr ElGamel'a

1 Wstęp

Kryptosystem ElGamel'a jest szyfrem asymetrycznym bazującym na problemie logarytmu dyskretnego w ciele liczb całkowitych modulo duża liczba pierwsza.

2 Zasada działania

1. Po stronie odbiorcy:
   (a) Wybór dużej liczby pierwszej – p
   (b) Wybór α takiego, że $\alpha \in \{2, 3 \dots p-1\}$
   (c) Wybór klucza prywatnego k_{pr} takiego, że $k_{pr} = d \in \{2, 3 \dots p-2\}$
   (d) Obliczenie klucza publicznego $k_{pb} = \beta \equiv \alpha^{k_{pr}} \pmod{p}$
   (e) Publikujemy (β, α, p) jako klucz publiczny
2. Po stronie nadawcy:
   (a) Wybór klucza prywatnego $i \in \{2, 3 \dots, p-2\}$
   (b) Obliczenie klucza publicznego $k_E \equiv \alpha^i \pmod{p}$
   (c) Obliczanie klucza maskującego/sesji $k_M \equiv \beta^i \pmod{p}$
   (d) Szyfrowanie wiadomości $Y \equiv X \cdot k_M \pmod{p}$, gdzie:
      - X - niezaszyfrowana wiadomość
      - Y - zaszyfrowana wiadomość
   (e) Publikujemy (Y, K_E)
3. Po stronie odbiorcy:
   (a) Obliczanie klucza maskującego/sesji $k_M \equiv k_m^d \pmod{p}$
   (b) Deszyfrowanie wiadomości $X \equiv Y \cdot k_M^{-1} \pmod{p}$, gdzie:
      - X - niezaszyfrowana wiadomość
      - Y - zaszyfrowana wiadomość
   (c) Profit

3 Implementacja

Program zaimplementowana w języku Python3. Odbiorca i nadawca są dwoma oddzielnymi skryptami komunikującymi się za pomocą plików.

3.1 Generowanie dużych liczb pierwszych

3.1.1 Test Millera–Rabina

3.2 Szybkie potęgowanie modulo p

3.3 Szybkie odwracanie modulo p

3.4 Szyfrowanie