

Szymon Adach  
Łukasz Gołębiewski  
Piotr Stańczyk

# Kryptosystem ElGamal

## 1. Cel

Celem zadana jest implementacja kryptosystemu ElGamal poprzez umożliwienia wygenerowania poprawnych kluczy oraz przeprowadzenie za ich pomocą asymetrycznego szyfrowania wiadomości. Klucz publiczny używany jest do zaszyfrowania wiadomości do postaci szyfrogramu, klucz prywatny używany jest do odszyfrowania szyfrogramu.

## 2. Działanie

Kryptosystem ElGamal jest zdefiniowany na grupie cyklicznej. Bezpieczeństwo kryptosystemu wynika z trudności obliczenia logarytmu dyskretnego zdefiniowanego w takiej grupie.

### Generacja kluczy:

Jako  $p$  zostanie wybrana duża liczba pierwsza przynajmniej o długości 1024 bitów. Liczba pierwsza gwarantuje nam że będzie tylko jedno rozwiązanie  $u$  logarytmu dyskretnego (przy założeniu że  $u$  jest mniejsze od rzędu  $p$ , w przeciwnym przypadku rozwiązaniem będzie każda liczba  $u + pn$ , co wynika z Małego Twierdzenia Fermata). Wielkość liczby pierwszej zwiększa ilość możliwych reszt modulo co zwiększa trudność obliczenia logarytmu dyskretnego.

Jako  $g$  wybierana jest losowo liczba rzędu  $p - 1$ .

Następnie wybierana jest losowo liczba  $x$  z przedziału  $\{1, \dots, p-1\}$ . Obliczana jest wartość

$$h \equiv g^x \pmod{p}.$$

Zbiór  $\{p, g, h\}$  będzie stanowił klucz publiczny, natomiast zbiór  $\{p, g, x\}$  to klucz prywatny. Wartość  $h$  może być podana publicznie właśnie ze względu na wcześniej omawiany problem obliczania wartości logarytmu dyskretnego.

## Szyfrowanie:

Szyfrowanie wiadomości  $m$  jest wykonywane za pomocą klucza publicznego.

- Wiadomość  $m$  jest kodowana jako element  $m'$  grupy rzędu  $p$ .
- Wybierane jest losowe  $y$  z przedziały  $\{1, \dots, p-1\}$  oraz obliczona wartość  $c \equiv g^y \pmod{p}$ .
- Obliczana jest wartość  $s \equiv h^y \pmod{p} \equiv g^{xy} \pmod{p}$ .
- Obliczana jest wartość  $d \equiv m's \pmod{p}$ .
- Wysyłany jest szyfrogram jako para  $(c, d)$ .

## Deszyfrowanie:

Odszyfrowanie szyfrogramu czyli pary  $(c, d)$  wykonywane jest za pomocą klucza prywatnego.

- Obliczana jest wartość  $s \equiv c^x \pmod{p}$ .
- Obliczana jest wartość  $m' \equiv ds^{-1} \pmod{p}$  a następnie  $m'$  jest kodowane z powrotem do  $m$ .

## 3. Implementacja

Implementacja algorytmu została wykonana w języku C++. Do obsługi typów większych niż 64 bity wykorzystywana jest klasa przechowująca liczbę w postaci tablicy liczb 32 bitowych. Liczba przechowywana jest w postaci Little-Endian a podstawa w jakiej przechowywana jest część liczby w pojedynczym elemencie tablicy wynosi  $10^9$ . W naszej implementacji wykorzystywane są algorytmy optymalizujące np. algorytm Karatsuby dla operacji mnożenia.

Przy kodowaniu czyli zamianie wiadomości na element grupy  $G$ , tekst dzielony jest na kilka wiadomości tak, aby wartość każdej wiadomości po mapowaniu na element  $G$  była mniejsza od rzędu grupy. Przy szyfrowaniu dla każdej wydzielonej części tekstu na nowo losowana jest wartość  $y$  oraz obliczana wartość  $c$  co dodatkowo pozwala poprawić bezpieczeństwo algorytmu. Dzięki temu że tekst przy kodowaniu zamieniany jest na tablicę bajtów można szyfrować dowolne znaki np. znaki polskie czy chińskie.

Przy losowaniu liczby pierwszej o podanej przez użytkownika ilości bitów wykorzystywany jest test pierwszości Millera-Rabina. Dodatkowo losowana liczba zawsze jest nieparzysta oraz sprawdzane jest czy dzieli się bez reszty z którąś z 1000 pierwszych liczb pierwszych. Jeśli tak liczba jest losowana ponownie bez przejścia do testu Millera-Rabina. Użytkownik podaje również liczbę iteracji dla których przeprowadzany jest test.

Program działa w dwóch trybach. Pierwszy to tryb szyfrowania: następuje generacja kluczy oraz odczytanie wiadomości z pliku, następnie klucze oraz szyfrogram są zapisywane do określonych plików. Drugi tryb to tryb deszyfrowania: program odczytuje klucze oraz szyfrogram z podanych plików, następnie zapisuje odszyfrowaną wiadomość do pliku.

Argumenty uruchomienia programu dla trybu szyfrowania:

elgamal encr {ilość bitów liczby pierwszej do wygenerowania} {ilość iteracji w teście Solovaya-Strassena} {liczba reprezentująca w jakim systemie liczbowym zapisać szyfrogram} {ścieżka do jakiej zapisać klucz publiczny} {ścieżka do jakiej zapisać klucz prywatny} {ścieżka do jakiej zapisać szyfrogram}

Argumenty uruchomienia programu dla trybu deszyfrowania:

elgamal decr {ścieżka do szyfrogramu} {ścieżka do klucza prywatnego} {liczba reprezentująca w jakim systemie liczbowym zapisano szyfrogram} {ścieżka do jakiej zapisać odszyfrowaną wiadomość}

## 4. Dyskusja

Kryptosystem Elgamal jest jednym z najpopularniejszych obok RSA systemów szyfrowania asymetrycznego. Szyfrowanie asymetryczne umożliwia nam zaszyfrowanie wiadomości do adresata gdzie tylko adresat będzie mógł ją odczytać.

Wadą systemu jest jego deformowalność czyli możliwość zmiany szyfrogramu bez znajomości tekstu jawnego przez co może być podatny na atak z wybranym szyfrogramem. Dla przykładu dla nieznanej wiadomości  $m$  oraz jej szyfrogramu  $(c, d)$  można łatwo skonstruować poprawny szyfrogram postaci  $(c, 2d)$  dla wiadomości  $2m$ .

Wadą może być również czas generowania kluczy w szczególności dla bardzo dużych liczb np. czas znalezienia losowej 2048 bitowej bezpiecznej liczby pierwszej.

## 5. Bibliografia

Bruce Schneier: *Applied Cryptography*

Taher ElGamal: *A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms*  
<http://caislab.kaist.ac.kr/lecture/2010/spring/cs548/basic/B02.pdf>