Laboratorium z kryptografii
Zajęcia 13-14: Algorytm szyfrowania ElGamal

1 Pierwiastki pierwotne

Definicja 1 *Rząd elementu modulo.*
Niech dane będą dwie, względnie pierwsze liczby naturalne $a, b > 1$. Rzędem elementu a modulo b nazywa się najmniejszą naturalną liczbę dodatnią c taką, że $a^c = 1 \pmod b$. Liczba c oznaczona została jako $c = ord_b a$

Twierdzenie 1 *.*
Niech $a^d = 1 \pmod b$, wtedy:

1. *$ord_b a | d$ (rząd a modulo b jest dzielnikiem d).*
2. *Niech $\varphi(x)$ będzie funkcją Eulera (oznaczającą ilość liczb naturalnych, dodatnich, mniejszych od x względnie pierwszych z x), wtedy $ord_b a$ jest dzielnikiem $\varphi(b)$. W szczególności jeżeli $b = n$, gdzie n jest liczbą pierwszą ($\varphi(n) = n-1$), to $ord_n a|(n-1)$.*
3. *Jeżeli $ord_n a = c$, gdzie n jest liczbą pierwszą, to zbiór $\{0, a, a^2, \ldots, a^{n-1}\}$ jest pełnym układem reszt z dzielenia modulo n.*

Twierdzenie 2 *Pierwiastek pierwotny modulo.*
Niech dane będą dwie względnie pierwsze liczby naturalne, dodatnie a oraz b. Liczba a nazywa się pierwiastkiem pierwotnym modulo b jeżeli $ord_b a = \varphi(b)$.

2 Algorytm

Algorytm szyfrowania ElGamal, podobnie jak RSA, operuje na kluczu publicznym oraz prywatnym, którego bezpieczeństwo oparte jest na liczbach pierwszych. Dla wybranej liczby pierwszej n wybiera się liczbę $1 < r < n-1$ będącą jej pierwiastkiem pierwotnym. Na podstawie twierdzeń 1 oraz 2, określenie czy dana liczba jest pierwiastkiem pierwotnym sprowadza się do warunku, że jeżeli:

$$n - 1 = p_1^{x_1} \cdot \ldots \cdot p_m^{x_m}, \tag{1}$$

gdzie p_i to dzielniki pierwsze liczby $n-1$, to dla każdego $i \in \{1, \ldots, m\}$ musi zachodzić:

$$r^{\frac{n-1}{p_i}} \neq 1 \pmod n. \tag{2}$$

Dodatkowo losuje się liczbę $1 < k < n-1$. Obliczając a zadane przez (3) otrzymuje się klucz publiczny (n, r, a) oraz klucz prywatny (n, r, a, k).

$$a = r^k \pmod n \tag{3}$$

Szyfrogram dla pewnego tekstu $t < n$ stanowi para liczb (c_1, c_2) zadana przez (4) oraz (5) otrzymana dla losowej liczby $1 < j < n-1$ [1].

$$c_1 = r^j \pmod n \tag{4}$$
$$c_2 = t \cdot a^j \pmod n \tag{5}$$

Odszyfrowanie tekstu odbywa się poprzez wyliczenie wartości $t_{odszyfr}$

$$t_{odszyfr} = c_2 \cdot c_1^{n-1-k} \pmod n \tag{6}$$

[1]losowanej przez nadawce - odbiorca nie musi jej znać

3 Przykłady

a) Niech liczba pierwsza $n = 257$, pierwiastek pierwotny $r = 3$ oraz losowa „tajna" $k = 21$.
Ponieważ $r^k \pmod n = 112$, to klucz publiczny wynosi (257,3,112) i jest wysyłany do nadawców.
Nadawca losuje swoją liczbę $j = 72$ i wysyła tekst $t = 138$.
Szyfrogram w postaci (137,229) przesyłany jest do odbiorcy.
Odbiorca odszyfrowuje wiadomość: $c_2 \cdot c_1^{n-1-k} = 138 \pmod n$

b) Niech liczba pierwsza $n = 2539$, pierwiastek pierwotny $r = 2$ oraz losowa „tajna" $k = 51$.
Ponieważ $r^k \pmod n = 403$, to klucz publiczny wynosi (2539,2,403) i jest wysyłany do nadawców.
Nadawca losuje swoją liczbę $j = 15$ i wysyła tekst $t = 1308$.
Szyfrogram w postaci (2300,516) przesyłany jest do odbiorcy.
Odbiorca odszyfrowuje wiadomość: $c_2 \cdot c_1^{n-1-k} = 1308 \pmod n$

c) Niech liczba pierwsza $n = 827$, pierwiastek pierwotny $r = 21$ oraz losowa „tajna" $k = 651$.
Ponieważ $r^k \pmod n = 578$, to klucz publiczny wynosi (827,21,578) i jest wysyłany do nadawców.
Nadawca losuje swoją liczbę $j = 345$ i wysyła tekst $t = 700$.
Szyfrogram w postaci (162,601) przesyłany jest do odbiorcy.
Odbiorca odszyfrowuje wiadomość: $c_2 \cdot c_1^{n-1-k} = 700 \pmod n$

d) Niech liczba pierwsza $n = 37813$, pierwiastek pierwotny $r = 36410$ oraz losowa „tajna" $k = 6739$.
Ponieważ $r^k \pmod n = 6024$, to klucz publiczny wynosi (37813,36410,6204) i jest wysyłany do nadawców.
Nadawca losuje swoją liczbę $j = 34310$ i wysyła tekst $t = 300$.
Szyfrogram w postaci (29918,14172) przesyłany jest do odbiorcy.
Odbiorca odszyfrowuje wiadomość: $c_2 \cdot c_1^{n-1-k} = 300 \pmod n$

4 Zadania

Zadanie:

1. Dla zadanych w konsoli liczb $n < 32000$, r, k, j oraz t napisać program szyfrujący algorytmem ElGamal. Program ma zwracać klucz publiczny oraz szyfrogram jeżeli zadana liczba n jest pierwsza oraz r jest jej pierwiastkiem pierwotnym lub wyświetlać powiadomienie o błędzie (i jego typie) w przeciwnym wypadku.

Punktacja:

- 3 punkty - prawidłowa generacja klucza publicznego oraz szyfrogramu dla $n < 1000$
- 3 punkty - prawidłowa generacja klucza publicznego oraz szyfrogramu dla $n \geqslant 1000$
- 4 punkty - prawidłowo działająca kontrola błędów