Uniwersytet Jagielloński w Krakowie

Wydział Fizyki, Astronomii i Informatyki Stosowanej

Hanna Tułowiecka

Nr albumu: 1027756

Krzywe eliptyczne i ich zastosowanie w kryptografii

Praca magisterska
na kierunku Informatyka Stosowana

Praca wykonana pod kierunkiem
Dr Jerzy Martyna
Instytut Informatyki i Matematyki Komputerowej

Kraków 2017

Oświadczenie autora pracy

Świadom odpowiedzialności prawnej oświadczam, że niniejsza praca dyplomowa została napisana przeze mnie samodzielnie i nie zawiera treści uzyskanych w sposób niezgodny z obowiązującymi przepisami.

Oświadczam również, że przedstawiona praca nie była wcześniej przedmiotem procedur związanych z uzyskaniem tytułu zawodowego w wyższej uczelni.

Kraków, dnia Podpis autora pracy

Oświadczenie kierującego pracą

Potwierdzam, że niniejsza praca została przygotowana pod moim kierunkiem i kwalifikuje się do przedstawienia jej w postępowaniu o nadanie tytułu zawodowego.

Kraków, dnia Podpis kierującego pracą

Spis treści

1 Wstęp

1.1 Wprowadzenie

Zagadnienia kryptograficzne są kluczowe w zapewnieniu bezpieczeństwa danych we współczesnym świecie. Dwa problemy matematyczne: problem logarytmu dyskretnego i problem rozkładu liczb całkowitych na czynniki pierwsze stanowią główne narzędzia kryptografii asymetrycznej. Trudność w ich rozwiązywaniu decyduje o bezpieczeństwie systemów kryptograficznych.
Istotną rolę odgrywa tu logarytm dyskretny. Istnieje hipoteza ([6], str. 20), że rozwiązanie problemu logarytmu dyskretnego jest równoważne złamaniu wielu ważnych i szeroko używanych systemów kryptograficznych z kluczem publicznym. Stąd też uważa się również, że systemy te są bezpieczne dopóty, dopóki problem logarytmu dyskretnego uważany jest za trudny. Z kolei odszyfrowanie w systemie ElGamala polega na odpowiednim użyciu klucza prywatnego. Problem logarytmu dyskretnego jest ściśle związany z rozkładem liczb na czynniki pierwsze, czyli z zagadnieniem faktoryzacji. W przypadku, gdy nie znamy klucza prywatnego, a dążymy do odszyfrowania zaszyfrowanej wiadomości, ninejsza praca przedstawia, jak zgodnie z algorytmem Pohlinga-Hellmana problem logarytmu dyskretnego sprowadzić do zagadnienia faktoryzacji. Następnie idąc drogą Pollarda, zostało pokazane, jak rozwiązywać zagadnienie faktoryzacji i w jakich sytuacjach jest to możliwe. Postępy w badaniach logarytmu dyskretnego i faktoryzacji mogą zagrażać bezpieczeństwu systemów kryptograficznych. Aby tym zagrożeniom zapobiec użyto w ostatnich latach w kryptografii tzw. krzywych eliptycznych (ang. *elliptic curves*). Zgodnie z definicją podaną przez [2], str. 280: "Krzywą eliptyczną nad ciałem K, o charakterystyce różniej od 2 i 3, nazywamy zbiór punktów (x, y) spełniających równianie $y^2 = x^3 + ax + b$, wraz z dodatkowym punktem O_E, nazywanym punktem w nieskończoności".

1.2 Cel pracy

Celem pracy jest objaśnienie matematycznych podstaw krzywych eliptycznych oraz pokazanie ich zastosowania w kryptografii na przykładzie algorytmu ElGamala opartego o krzywe eliptyczne. Drugim celem pracy jest wykazanie, że na drodze programowej można stosować krzywe eliptyczne dla zagadnień szyfrowania danych.

1.3 Studium wykonalności

Napisany w ramach pracy magisterskiej program komputerowy ma charakter naukowy i zarazem dydaktyczny. Program umożliwia m.in. rysowanie wykresów $E(F_p)$, liczenia sumy i odwrotności punktów należących do $E(F_p)$ oraz ich szyfrowania i odszyfrowywania punktów metodą ElGamala na krzywej eliptycznej. Program może znaleźć również zastosowanie na zajęciach dydaktycznych z kryptografii do demonstracji działania algorytmu ElGamala na krzywej eliptycznej oraz do sprawdzenia umiejętności studentów. Zdaniem autora pracy nie są znane programy komputerowe, które mogą być zastosowane zarówno do testów, jak i demonstracji na ćwiczeniach z kryptografii.

1.4 Treść pracy

W pracy zostało przedstawione pojęcie krzywych eliptycznych, zaprezentowano ich własności oraz pokazano, że szyfrowanie tekstów przy ich użyciu zwiększa trudność przy odszyfrowywaniu. Praca składa się z trzech części: matematycznej, kryptograficznej i programistycznej. W części matematycznej (rozdział 2) zawarte zostały wszystkie pojęcia i twierdzenia przydatne w zrozumieniu części kryptograficznej (rozdział 3). W drugiej części pracy (rozdział 3) przedstawione zostało szyfrowanie i odszyfrowywanie wiadomości tekstowych w systemie ElGamala z użyciem klucza publicznego i klucza prywatnego.
W części programistycznej (rozdział 4) zostały zaprezentowane funkcjonalności programu implementujące algorytm ElGamala oparty o krzywe eliptyczne. W tej części został również opisany sposób korzystania z aplikacji.

2 Część teoretyczna

Przy opracowywaniu treści tego rozdziału korzystano z pozycji: [2], [3], [6], [7], [8], [9].

2.1 Arytmetyka reszt z dzielenia liczb całkowitych

Dane są liczby całkowite a i b, $b \neq 0$. Aby podzielić liczbę a przez liczbę b, poszukujemy liczb całkowitych q i r takich, by

$$a = qb + r, 0 \leqslant r < |b|. \tag{1}$$

Wzór (1) nazywamy wzorem na dzielenie z resztą. Liczbę q nazywamy ilorazem liczb a i b, natomiast r nazywamy resztą z dzielenia a i b. Jeśli $r = 0$, to mówimy, że a jest podzielne przez b lub, że b jest dzielnikiem a, co zapisujemy $b|a$.

Definicja 1
Dane są liczby całkowite a i b, przynajmniej jedna z nich jest różna od zera. Największym wspólnym dzielnikiem liczb (NWD) a i b nazywamy liczbę całkowitą $d > 0$ taką, że

1. $d|a, d|b$
2. *jeżeli* $c|a, c|b$, *to* $c \leqslant d$.

Używać będziemy oznaczenia $NWD(a, b) = d$.

Dla wyznaczenia $NWD(a, b)$ bardzo pożyteczne jest następujące twierdzenie:

Twierdzenie 1
Jeżeli $a = qb + r$, *to* $NWD(a, b) = NWD(b, r)$.

Twierdzenie to uzasadnia tzw. algorytm Euklidesa znajdowania $NWD(a, b)$ ([2], str. 20). Dostarcza ono następującego sposobu postępowania:

$a = q_1 b + r_1$
$b = q_2 r_1 + r_2$
$r_1 = q_3 r_2 + r_3$
.
.
.
$r_{n-1} = q_{n+1} r_n + 0.$

Stąd wynika, że $NWD(a, b) = rn$.

Bardzo ważne dla naszych celów jest następujące twierdzenie:

Twierdzenie 2
Dane są liczby a i b całkowite ($a, b \in \mathbb{Z}$), przynajmniej jedna z nich jest różna od zera. Wówczas istnieją liczby całkowite x, y takie, że $NWD(a, b) = ax+by$.

Definicja 2
Liczby $a, b \in \mathbb{Z}$, $a \cdot b \neq 0$ nazywamy względnie pierwszymi $\Leftrightarrow$ gdy $NWD(a, b) = 1$.

Z definicji 3 i twierdzenia 2 wynika kolejne twierdzenie:

Twierdzenie 3
Dane są liczby $a, b \in \mathbb{Z}$, przynajmniej jedna z nich jest różna od 0. Wówczas $NWD(a, b) = 1 \Leftrightarrow$ istnieją liczby $x, y \in \mathbb{Z}$ takie, że $ax + by = 1$.

Sposób obliczania liczb x i y, występujących w twierdzeniach 2 i 3, dostarcza rozszerzony algorytm Euklidesa ([2], str. 24). Polega on na następującym postępowaniu:
$a = q_1 b + r_1$, stąd $r_1 = a - q_1 b = ax_1 + by_1$
$b = q_2 r_1 + r_2$, stąd $r_2 = b - q_2 r_1 = b - q_2(a - q_1 b) = ax_2 + byz$
i tak dalej.
Ostatecznie, korzystając z twierdzenia 1, dostajemy twierdzenie 2.

Definicja 3
Dana jest liczba naturalna p oraz liczby $a, b \in \mathbb{Z}$. Liczby a i b nazywamy przystającymi modulo p, co notujemy $a \equiv b \,(mod\, p)$, wtedy i tylko wtedy, gdy różnica $a - b$ jest podzielna przez p.

$a \equiv b \pmod{p}$ oznacza, że istnieje liczba k taka, że $a - b = kp$ lub $a = b + kp$.

Przykład 1
$12 \equiv 3 \pmod{9}$, bo $12 - 3 = 9$ jest podzielne przez 9.
$19 \equiv 4 \pmod{5}$, bo $19 - 4 = 15$ jest podzielne przez 5.

Dowolną liczbę całkowitą a można podzielić przez p według wzoru (1). Mamy więc

$$a = q \cdot p + r, 0 \leqslant r \leqslant p - 1 \tag{2}$$

Stąd, zgodnie z definicją podzielności, stwierdzamy, że $a - r = qp$. Zatem $a - r$ jest podzielne przez p. Mamy więc równość

$$a \equiv r \,(mod\, p). \tag{3}$$

Każda liczba całkowita przystaje modulo p do jednej z liczb ze zbioru $\{0, 1, \ldots, p-1\}$. Zbiór ten oznaczamy przez F_p. W zbiorze $\mathbb{Z}$ liczb całkowitych definiujemy działanie dodawania modulo p w następujący sposób. Niech $a, b \in \mathbb{Z}$. Aby otrzymać sumę $a+b$ modulo p obliczmy zwykłą sumę $a+b$ przez p według wzoru (2): $a+b = q \cdot p + r$. Następnie, zgodnie ze wzorem (3), dostajemy $a + b = r\,(mod\,p)$.

Przykład 2
$13 + 10 = 3\,(mod\,5)$, bo $13 + 10 = 23 = 4 \cdot 5 + 3$. Zatem $r = 3$.

Zasada dodawania liczb całkowitych modulo p polega na tym, że wynik tego dodawania jest elementem zbioru F_p. W zbiorze F_p, ze względu na dodawanie, definiuje się element neutralny i przeciwny. Elementem neutralnym w zbiorze F_p jest liczba 0. Dla każdego $a \in F_p$ mamy $a + 0 = a\,(mod\,p)$. Elementem przeciwnym do liczby $a \in F_p$ jest liczba $p - a$. Dla każdego $a \in F_p$ mamy $a + (p - a) = 0\,(mod\,p)$.

Podobnie w zbiorze liczb całkowitych definiuje się działanie mnożenia modulo p. Mamy $a \cdot b = q \cdot p + r$, $a \cdot b = r\,(mod\,p)$. W zbiorze F_p, ze względu na mnożenie, definiuje się element neutralny – jest nim liczba 1, $a \cdot 1 = a\,(mod\,p)$ oraz element odwrotny – jest nim element $\hat{a} \in F_p$ taki, że $a \cdot \hat{a} = 1\,(mod\,p)$.

Powstaje pytanie, jak wyznaczyć element $\hat{a}$ odwrotny do elementu a? Z równości $a \cdot \hat{a} = 1\,(mod\,p)$ wynika, że liczba $a \cdot \hat{a} - 1$ jest podzielna przez p. Zatem istnieje liczba $k \in \mathbb{Z}$, taka, że zachodzi równość

$$a\hat{a} - 1 = kp,\ czyli\ \ a\hat{a} - kp = 1 \tag{4}$$

stąd i z twierdzenia 3 wnioskujemy, że liczby a i p są względnie pierwsze. Wystarczy więc w twierdzeniu 3 podstawić $x = \hat{a}$, $b = p$, $y = -k$ czyli $a\hat{a} - kp = 1$, aby otrzymać $NWD(a \cdot p) = 1$.

Twierdzenie 4
Liczba $a \in F_p$ ma element odwrotny $\Leftrightarrow NWD(a \cdot p) = 1$.

Element $\hat{a} \in F_p$ odwrotny do $a \in F_p$ tworzymy jako współczynnik x występujący przy a w równości $ax + by = 1$ w twierdzeniu 3. Element $\hat{a} \in F_p$ odwrotny do $a \in F_p$ oznaczać będziemy jako $\hat{a} = a_p$.

Przykład 3
Znaleźć element odwrotny do $7 \in F_{13}$.
Bierzemy równość $7\hat{a} - 13k = 1$ jako szczególny przypadek (4). Zachodzi ona dla $\hat{a} = 2$ i $k = 1$. Zatem elementem odwrotnym do $7 \in F_{13}$ jest $2 \in F_{13}$.

Element $0 \in F_p$ nie ma elementu odwrotnego, ponieważ dla dowolnego $\hat{a} \in F_p$ zachodzi równość $0 \cdot \hat{a} = 0\,(mod\, p) \neq 1 \in F_p$ (względnie $NWD(0,p) = p \neq 1$). Element $a \in F_p$, który ma element odwrotny w F_p, nazywamy odwracalnym w F_p.

Zbiór elementów odwracalnych w F_p oznaczamy przez F_p^*. Zatem $F_p^* = \{a \in F_p : NWD(a,p) = 1\}$

Jeżeli p jest liczbą pierwszą, to $NWD(a,p) = 1$ dla każdej liczby a całkowitej dodatniej mniejszej niż p, stąd wynika, że $F_p^* = F_p \backslash \{0\} = \{1, \ldots, p-1\}$.

W odróżnieniu od F_p, które ma p elementów, F_p^* ma $p-1$ elementów. Jeżeli liczba p jest liczbą złożoną i $1 < k < p$ jest podzielnikiem p, to $NWD(k,p) \geqslant k > 1$. Stąd wynika na mocy twierdzenia 4, że liczba $k \in F_p$ nie ma elementu odwrotnego w F_p. Rozważmy $F_4 = \{0,1,2,3\}$ oraz element $2 \in F_4$. $NWD(2,4) = 2 > 1$. Zatem element $2 \in F_4$ nie ma elementu odwrotnego w F_4. Stąd $F_4^* = 1,3$. Ale element $2 \in F_5$ ma element odwrotny w F_5, bo $NWD(2,5) = 1$. Z twierdzenia 4 wynika, że $2x - 5k = 1$, co zachodzi dla $x = 3$, $k = 1$. Zatem $2_5 = 3 \in F_5$.

Twierdzenie 4 będzie odgrywało bardzo ważną rolę przy rozwiązywaniu kongruencji (rozdział 2.4) i w chińskim twierdzeniu o resztach (rozdział 2.4).

Niech $\ell(p)$ oznacza liczbę elementów zbioru F_p^*. Funkcję $\ell(p)$ nazywamy *funkcją Eulera*. Wyżej wykazaliśmy, że jeżeli p jest liczbą pierwszą to $\ell(p) = p - 1$. Dowodzi się ponadto, że $\ell(p \cdot q) = \ell(p) \cdot \ell(q)$, gdy $NWD(p,q) = 1$.

2.2 Algebraiczne ujęcie zagadnienia

W algebrze wprowadza się pojęcie grupy. Ma ono zastosowanie w kryptografii.

Niech G oznacza dowolny zbiór (niekoniecznie zbiór liczb).

Odwzorowanie $G \times G \to G$, które każdej parze punktów ze zbioru G przyporządkowuje punkt zbioru G, nazywamy działaniem w zbiorze G.

Dla przykładu w zbiorze liczb całkowitych działaniem jest zwykłe dodawanie lub mnożenie liczb. W zbiorze F_p działaniem jest dodawanie liczb modulo p lub mnożenie liczb modulo p.

Definicja 4
Niech G będzie dowolnym zbiorem. Działanie określone w G oznaczymy symbolem $\circ : G \times G \to G$. Parę $(G, \circ)$ złożoną ze zbioru G i z działania $\circ$ nazywamy grupą wtedy i tylko wtedy, gdy:

1. *$a \circ b \in G$ dla dowolnych $a, b \in G$ (domkniętość)*
2. *$a \circ (b \circ c) = (a \circ b) \circ c$ dla dowolnych $a, b, c \in G$ (łączność)*
3. *istnieje $e \in G$ takie, że $a \circ e = e \circ a = a$ dla dowolnego $a \in G$ (istnienie elementu neutralnego)*

4. *dla dowolnego* $a \in G$ *istnieje* $a^{-1} \in G$ *takie, że* $a \circ a^{-1} = a^{-1} \circ a = e$ *(istnienie elementu odwrotnego)*

Jeśli grupa ma dodatkową własność

5. $a \circ b = b \circ a$ *dla dowolnych* $a, b \in G$ *(przemienność)*

to nazywamy ją grupą abelową (Abel – nazwisko matematyka norweskiego).

Jeśli zbiór G *ma skończoną liczbę elementów, to grupę* $(G, \circ)$ *nazywamy skończoną.*

Przykład 4

1. Jako zbiór G rozważmy zbiór $\mathbb{Z}$ liczb całkowitych. Jako działanie $\circ$ w $\mathbb{Z}$ dodawanie, oznaczmy je symbolem $+$. Para $(\mathbb{Z}, +)$ stanowi przykład grupy abelowej i nieskończonej. Elementem neutralnym jest liczba 0, elementem odwrotnym jest $a^{-1} = -a$. Element odwrotny często nazywamy w tym przypadku przeciwnym. Analogicznie zbiór liczb rzeczywistych $\mathbb{R}$ z działaniem dodawania jest grupą abelową nieskończoną.

2. Jako zbiór G rozważmy zbiór F_p i działanie dodawanie modulo p. Jest to przykład grupy abelowej skończonej. Elementem neutralnym jest 0, elementem przeciwnym $a^{-1} = p - a$. Grupy z dodawaniem (niekoniecznie liczb) nazywamy grupami addytywnymi.

3. Jako zbiór G nazywamy zbiór $\mathbb{R}\backslash\{0\}$ i działanie mnożenia oznaczane $\cdot$. Elementem neutralnym jest tu liczba 1, elementem odwrotnym $a^{-1} = \frac{1}{a}$. Para $(R\backslash\{0\}, \cdot)$ jest grupą abelową nieskończoną. Zauważmy, że zbiór $\mathbb{R}$ w tym samym działaniu nie jest grupą, bo 0 nie ma elementu odwrotnego.

4. Jako zbiór G rozważmy zbiór F_p i działanie mnożenia modulo p. Nie każdy element zbioru F_p ma element odwrotny. Zatem F_p nie jest grupą. Ale, jeśli p jest liczbą pierwszą zbiór elementów odwracalnych zbioru F_p, oznaczany wcześniej przez F_p^*, jest grupą abelową skończoną. Elementem neutralnym jest 1. Element odwrotny uzyskuje się metodą omówioną wcześniej. Istnieje więc istotna różnica między zbiorem F_p z działaniem dodawania modulo p, a zbioru F_p z działaniem mnożenia modulo p.

2.3 Reszty kwadratowe

Niech p będzie nieparzystą liczbą pierwszą ($p > 2$). Rozważmy zbiór $F_p^* = \{1, 2, \ldots, p-1\}$. Mówimy, że liczba $b \in F_p^*$ jest pierwiastkiem kwadratowym modulo p liczby $a \Leftrightarrow b^2 = a \,(mod\, p)$.

Mówimy również, że liczba a jest kwadratem liczby b modulo p. Powstaje pytanie, które z liczb $1, 2, \ldots, p-1$ są kwadratami liczb ze zbioru F_p^*? Odpowiemy na to pytanie w szczególnym przypadku $F_{13}^* = \{1, 2, \ldots, 12\}$. Podnieśmy do kwadratu modulo 13 kolejne liczby z F_{13}^*.

Otrzymamy:

$1^2 = 1\,(mod\,13)$ $2^2 = 4\,(mod\,13)$ $3^2 = 9\,(mod\,13)$ $4^2 = 3\,(mod\,13)$
$5^2 = 12\,(mod\,13)$ $6^2 = 10\,(mod\,13)$ $7^2 = 10\,(mod\,13)$ $8^2 = 12\,(mod\,13)$
$9^2 = 3\,(mod\,13)$ $10^2 = 9\,(mod\,13)$ $11^2 = 4\,(mod\,13)$ $12^2 = 1\,(mod\,13)$

Widzimy, że jedynie liczby $1, 4, 9, 3, 12, 10$ są kwadratami modulo 13 liczb ze zbioru F_{13}^*. Nazywamy je resztami kwadratowymi.
Powstałe liczby $2, 5, 6, 7, 8, 11$ nazywamy nieresztami kwadratowymi.

W tych działach kryptografii, w których używa się logarytmu dyskretnego jest bardzo ważne, aby umieć dzielić przez p potęgi $a^k = a \cdot a \cdot a \cdot a \ldots k$ razy. Niezwykle pomocne jest do tego Małe twierdzenie Fermata.

Twierdzenie 5 (Małe twierdzenie Fermata, [2], str. 59)
Niech a będzie liczbą całkowitą, p – liczbą pierwszą dodatnią. Wówczas zachodzi równość $a^p \equiv a\,(mod\,p)$

Twierdzenie 6 (inna forma małego twierdzenia Fermata, [2], str. 60)
Niech p będzie liczbą pierwszą dodatnią, a - liczbą całkowitą nie dzielącą się przez p. Wówczas $a^{p-1} \equiv 1\,(mod\,p)$

Twierdzenie Fermata pozwala w szczególności obliczać potęgi a^k z bardzo dużymi wykładnikami przy pomocy obliczania potęg z wykładnikami znacznie mniejszymi. Na czym to polega? Dane są liczby: k - całkowita dodatnia, p – pierwsza dodatnia, a całkowita. Niech $k > p$.

1. Jeżeli a dzieli się przez p, to a^k też dzieli się przez p. Stąd wynika, że $a^k \equiv 0\,(mod\,p)$.

2. Gdy a nie dzieli się przez p, wówczas wykładnik k w potędze a^k dzielimy przez $p-1$. Mamy więc $k = (p-1)q + r, 0 \leqslant r < p-1$.

Zatem $a^k = a^{[(p-1)q+r]} = a^{(p-1)q}a^r$. Z twierdzenia Fermata (twierdzenie 6) mamy $a^{p-1} \equiv 1\,(mod\,p)$. Zatem

$$a^k \equiv a^r\,(mod\,p) \tag{5}$$

Przykład 5
Obliczyć $2^{54321}\,(mod\,13)$.
Wykładnik 54321 dzielimy z resztą przez $12 = (13-1)$.

Dostajemy $54321 = 456 \cdot 12 + 9$. Mamy resztę $r = 9$.
Zatem ze wzoru (5): $2^{54321} \equiv 2^9 \,(mod\, 13)$. Stąd wynika, że zamiast dzielić liczbę 2^{54321} przez 13 wystarczy podzielić 2^9 przez 13. Dostajemy $2^9 \equiv 5 \,(mod\, 13)$. Zatem $2^{54321} = 5 \,(mod\, 13)$.

Przykład ten jest małą próbką wykorzystania twierdzenia Fermata. Chodzi teraz o to, aby liczbę $a^r \,(mod\, p)$ z liczbą r małą w stosunku do liczby k, dało się obliczyć bezpośrednio.

2.4 Rozwiązanie kongruencji

Niech liczby $a, b \in \mathbb{Z}, p \in \mathbb{N}$ będą dane.

$$ax \equiv b \,(mod\, p) \tag{6}$$

Równanie to nosi nazwę kongruencji. Zawiera ono niewiadomą x. Chodzi o znalezienie rozwiązania x. Trzeba stwierdzić, że nie każde równanie postaci (6) ma rozwiązanie. Dla przykładu rozważmy równanie $2x \equiv 1 \,(mod\, 4)$. Wystarczy ograniczyć się do badania tego rozwiązania w zbiorze $F_4 = \{0, 1, 2, 3\}$, gdyż każda liczba całkowita jest przejściem modulo 4 do jednej z liczb ze zbioru F_4. Podstawiając liczby $0, 1, 2, 3$ do $2x$, dostajemy po lewej stronie tego równania liczby $0, 2, 4, 6$. Żadna z nich nie jest równa $1 \,(mod\, 4)$. Ale równanie (6) $xa = 1$ ma rozwiązanie. Jest ono postaci $x = b + kp, k \in \mathbb{Z}$.

Prawdziwe jest twierdzenie:

Twierdzenie 7
Równanie $ax \equiv b \,(mod\, p)$ ma rozwiązanie wtedy i tylko wtedy, gdy $NWD(a, p)$ jest dzielnikiem b.

Twierdzenie 5 do przykładu $2x \equiv 1 \,(mod\, 4)$ nie ma zastosowania, bo $NWD(2, 4) = 2$ nie jest dzielnikiem 1. Przed rozwiązaniem równań postaci (6), które mają rozwiązania bierzemy razem znane nam już fakty. Równanie (6) można zapisać również w ten sposób.

$$ax = b + kp \tag{7}$$

Przykład 6

$$7x \equiv 5 \,(mod\, 13) \tag{8}$$

$NWD(7, 13) = 1$. Zatem na mocy twierdzenia 4, element 7 w F_{13} ma element odwrotny i wynosi on 2 (patrz Przykład 3), czyli równanie (8) mnożymy obustronnie przez 2. Dostajemy $2 \cdot 7x \equiv 2 \cdot 5 \,(mod\, 13)$, czyli $x = 10 \,(mod\, 13)$, czyli $x = 10 + 13k$.

Przykład 7
Rozwiążmy równanie

$$14x \equiv 21\,(mod\,49) \tag{9}$$

$NWD(14,49) = 7 \neq 1$. Zatem element 14 nie ma odwrotnego w F_{49} Jednakże $NWD(14,49) = 7$ jest dzielnikiem 21 i zgodnie z twierdzeniem 5 równanie (9) ma rozwiązanie. Znajdziemy to rozwiązanie. Równanie (9) zapisanie w formie $14x = 21+49k$ dzielimy przez 7 i dostajemy $2x = 3+7k$, czyli $2x \equiv 3\,(mod\,7)$. Element 2 ma element odwrotny w F_7 bo $NWD(2,7) = 1$. Znajdziemy go z równania $2\hat{a} - 7k = 1$, kładąc $\hat{a} = 4, k = 1$. Zatem element odwrotny do 2 w F_7 wynosi 4. Mnożymy równanie $2x \equiv 3\,(mod\,7)$ przez 4 i dostajemy $4 \cdot 2x \equiv 4 \cdot 3\,(mod\,7)$, czyli $x = 12\,(mod\,7)$, czyli $x = 5\,(mod\,7), x = 5 + 7k$.

2.5 Chińskie twierdzenie o resztach

Rozważmy układ dwóch kongruencji

$$\begin{aligned} x &\equiv a\,(mod\,p) \\ x &\equiv b\,(mod\,p) \end{aligned} \tag{10}$$

Załóżmy, że $NWD(p,q) = 1$. Rozwiązanie pierwszego z nich ma postać

$$x = a + p \cdot y, y \in \mathbb{Z}. \tag{11}$$

Rozwiązanie podane przez wzór (11) powinno spełnić drugie równanie przedstawione przez równość (10). Dlatego wstawiamy go do niego, otrzymując $a + py = b\,(mod\,p)$, czyli

$$py = (b - a)\,(mod\,q) \tag{12}$$

Ponieważ $NWD(p,q) = 1$ i liczba 1 jest dzielnikiem liczby $b - a$, na podstawie twierdzenia 5 wnosimy, że równanie (12) (ze względu na niewiadomą y) ma rozwiązanie. Aby go otrzymać postępujemy tak, jak w przypadku jednego rozwiązania. Znajdujemy najpierw element odwrotny do p w F_q. Element ten istnieje na mocy twierdzenia 4 i otrzymujemy go rozszerzoną metodą Euklidesa. Oznaczamy go przez $\hat{a}$. Mamy więc $\hat{a}p = 1\,(mod\,p)$. Mnożąc równanie (12) przez $\hat{a}$ dostajemy

$\hat{a}py = (a-b)\hat{a}\,(mod\,q)$, czyli $y = (a-b)\hat{a}\,(mod\,q)$, zatem $y = (a-b)\hat{a}+lq$. Stąd i z równania (11) mamy $x = a + p\hat{a}(b - a) + pql$, czyli

$$x = a + p\hat{a}(b - a)\,(mod\,pq) \tag{13}$$

Otrzymaliśmy wówczas

Twierdzenie 8
Układ kongruencji (10) przy założeniu $NWD(p,q) = 1$ *ma rozwiązanie (*13*) w* F_{pq}.

Twierdzenie to jest prawdziwe w przypadku ogólnym
$x \equiv a_1 \,(mod, p_1)$
.
.
.
$x \equiv a_k \,(mod\, p_k)$ przy założeniu, że liczby $p_1, \ldots, p_k$ są parami względnie pierwsze, tzn., że $NWD(p_i, p_j) = 1$ dla $j \neq i$. Rozwiązanie otrzymuje się w $F_{p_1 \cdots p_k}$.

2.6 Zastosowanie chińskiego twierdzenia o resztach do obliczania potęg

Zilustrujemy zastosowanie chińskiego twierdzenia o resztach do obliczania potęgi $2^{5423} \,(mod\, 5005)$. Chodzić nam będzie w zasadzie nie o otrzymanie konkretnego wyniku, ale o dokładne przedstawienie idei tego twierdzenia. Konkretne jego zastosowanie wystąpi w algorytmie Pohlinga-Hellmana ([2], str. 268). Rozważmy najpierw sytuację ogólniejszą: obliczenie $a^m \,(mod\, p)$. Dane liczby a i m są całkowite, liczba $p = p_1 \ldots p_k$, gdzie p_i są liczbami pierwszymi takimi, że $0 < p_1 < \ldots < p_k$. Obliczamy najpierw

$$\begin{gathered} a^m \,(mod\, p_1) = r_1, 0 \leqslant r_1 < p_1 \\ . \\ . \\ . \\ a^m \,(mod\, p_k) = r_k, 0 \leqslant r_k < p_k \end{gathered} \tag{14}$$

i rozważmy układ równań

$$\begin{gathered} x = r_1 \,(mod\, p_1) \\ . \\ . \\ . \\ x = r_k \,(mod\, p_k) \end{gathered} \tag{15}$$

Ponieważ $p_1, \ldots, p_k$ są liczbami pierwszymi różnymi między sobą to p_i, p_k są względnie pierwsze. Można więc do układu równań (15) zastosować chińskie twierdzenie o resztach. Wynika z niego, że istnieje rozwiązanie układu

równań (15) w $F_{p_1 \ldots p_k}$. Oznaczamy go przez x. Jest ono równe $a^m \, (mod \, p_1 \ldots p_k)$. Widzimy więc, że aby obliczyć $a^m \, (mod \, p_1 \ldots p_k)$ w rozważanym przypadku wystarczy obliczyć $r_1, \ldots, r_k$ we wzorach (14), rozwiązując układ równań (15) i z twierdzenia chińskiego o resztach wywnioskować ile wynosi $a^m \, (mod \, p)$.

Przejdźmy do zapowiedzianego przykładu.

Przykład 8

$2^{5423} \, (mod \, 5005)$. Zauważmy, że $5005 = 5 \cdot 7 \cdot 11 \cdot 13 = p_1 \cdot p_2 \cdot p_3 \cdot p_4$. Korzystamy teraz z prostej wersji twierdzenia Fermata (twierdzenie 5), Dokonujemy dzielenia liczby 5423 kolejno przez liczby $5 - 1 = 4$, $7 - 1 = 6$, $11 - 1 = 10$, $13 - 1 = 12$. Otrzymujemy reszty równe odpowiednio $3, 5, 3, 11$. Zatem układ równań (14) w naszym przypadku ma postać:

$$\begin{aligned} 2^{5423} &= 2^3 \, (mod \, 5) \\ 2^{5423} &= 2^5 \, (mod \, 7) \\ 2^{5423} &= 2^3 \, (mod \, 11) \\ 2^{5423} &= 2^{11} \, (mod \, 13) \end{aligned} \tag{16}$$

Układ ten po dokonaniu redukcji modulo ma postać:

$$\begin{aligned} 2^{5423} &= 3 \, (mod \, 5) \\ 2^{5423} &= 4 \, (mod \, 7) \\ 2^{5423} &= 8 \, (mod \, 11) \\ 2^{5423} &= 7 \, (mod \, 13) \end{aligned} \tag{17}$$

Zatem układ równań (15) w naszym przypadku ma postać:

$$\begin{aligned} x &= 3 \, (mod \, 5) \\ x &= 4 \, (mod \, 7) \\ x &= 8 \, (mod \, 11) \\ x &= 7 \, (mod \, 13) \end{aligned} \tag{18}$$

zauważmy, że na mocy (17) liczba 2^{5423} spełnia układ (20)

Z twierdzenia 6 wynika, że układ równań (20) należy do zbioru $F_{5 \cdot 7 \cdot 11 \cdot 13}$

3 Część kryptograficzna - metody szyfrowania i odszyfrowania wiadomości tekstowych

Część kryptograficzna pracy zawiera metody szyfrowania i odszyfrowania wiadomości tekstowych. Przedstawione metody opierają się na pojęciu logarytmu dyskretnego, najpierw w grupie multiplikatywnej liczb całkowitych z działaniem mnożenia liczb modulo p. Następnie systemy kryptograficzne zostały przedstawione przy użyciu grup addytywnych z działaniami dodawania punktów położonych na krzywych eliptycznych. Z porównania tych dwóch wyjść wynika, że szyfrowanie przy użyciu krzywych eliptycznych daje dużo więcej możliwości stworzenia utrudnień do odszyfrowania dla osoby trzeciej. Uzyskuje się to dzięki dużej swobodzie wyboru krzywej eliptycznej przy szyfrowaniu. Daje to szansę uzyskania bezpieczniejszego systemu kryptograficznego. Zacytujmy opinię ([7], str. 221): „Możliwe jest to że, problem logarytmu dyskretnego na krzywych eliptycznych okaże się trudniejszy do rozwiązania niż problem logarytmu dyskretnego w ciałach skończonych." Wiadomo również, że bezpieczeństwo systemów kryptograficznych zależy od trudności rozwiązania problemu logarytmu dyskretnego.
Przy opracowywaniu treści tego rozdziału korzystano z pozycji: [2], [3], [6], [7], [9].

3.1 Szyfrowanie i odszyfrowanie w systemie ElGamala

Stosować będziemy grupę multiplikatywną $F_p^* = \{1, 2, \ldots, p-1\}$ liczb całkowitych z mnożeniem modulo p. Liczba p jest liczbą pierwszą. Używać będziemy klucza publicznego i prywatnego oraz związku między nimi.

$$r^k \equiv a \,(mod\, p) \tag{19}$$

Kluczem publicznym jest tu trójka (p, r, a), kluczem prywatnym jest liczba k. Wybieramy najpierw liczby p i r oraz liczbę całkowitą k z przedziału $2 \leqslant k \leqslant p-2$. Liczba a wybierania jest tak, by zachodziła równość (19). Zakładamy, że liczba p nie jest dzielnikiem liczby r. Zakładamy, że nadawca N wiadomości zna jedynie klucz publiczny odbiorcy O. Zakładamy również, że odbiorca, oprócz swojego klucza publicznego, dysponuje swoim kluczem prywatnym.
Aby wysłać wiadomość tekstową W nadawca N znajduje najpierw jej odpowiednik liczbowy. Dokonuje tego przy pomocy przyporządkowania literom alfabetu kolejnych liczb całkowitych. Następnie nadawca N wybiera losowo liczbę całkowitą $j \in [2, p-2]$. Zauważmy, że j jest wybrana z tego samego przedziału co k. Zakodowaną wiadomość przedstawia w formie pary liczb (C_1, C_2), gdzie $C_1 = r^j \,(mod\, p)$, $C_2 = Wa^j \,(mod\, p)$.
Para $(C1, C2)$ jest teraz przekazywana odbiorcy O.
Odbiorca odszyfrowuje ją w następujący sposób.
Oblicza $P{=}C_2C_1^{p-1-k} \,(mod\ p)$, a następnie stwierdza, że liczba
$P = C_2C_1^{p-1-k} = W$

Fakt, że $P = W$ uzasadnia następującym rachunkiem:

$$P = C_2C_1^{p-1-k} = Wa^j(r^j)^{p-1-k} = W(r^k)^j r^{j(p-1-k)} = Wr^{kj+jp-j-jk} = Wr^{j(p-1)} = W(r^{p-1})^j = W$$

W części początkowej tej dłuższej równości korzystaliśmy z równości (19), w części końcowej korzystaliśmy z twierdzenia Fermata (twierdzenie 6). Podsumowując zauważmy, że do wysłania wiadomości nadawca powinien dysponować kluczem publicznym odbiorcy. wiadomość Odbiorca powinien dysponować swoim kluczem publicznym i swoim kluczem prywatnym. Do wysłania wiadomości nie jest potrzebny nadawcy ani jego klucz publiczny, ani jego klucz prywatny. Warto dodać, że nadawca może wysłać tę samą wiadomość przy użyciu różnych liczb $j = \{2, 3, ..., p-2\}$. W każdym z tych przypadków odbiorca dostaje tę samą wiadomość. Stosowanie przez nadawcę różnych wartości liczby j może mieć znaczenie dla zwiększenia bezpieczeństwa przesyłania wiadomości. Sprawia się bowiem więcej trudności próbującym odszyfrować wiadomość.

3.2 Algorytm Pohliga – Hellmana znajdowania klucza prywatnego

Przypuśćmy, że otrzymaliśmy zaszyfrowaną wiadomość, ale nie dysponujemy odpowiednim kluczem i nie jesteśmy w stanie jej odszyfrować. Nasze próby odszyfrowania natrafiają na trudności pochodzące stąd, że nie są znane ogólne metody, przy pomocy których byłoby możliwe rozwiązanie kongruencji (19) lub przedstawianie liczb całkowitych w formie iloczynów liczb pierwszych (lub ich potęg) w rozsądnym czasie. Algorytm, który jest treścią tego paragrafu, podaje sposób znajdowania logarytmów dyskretnych w bardzo szczególnym przypadku. Okazuje się, że w tym przypadku problem logarytmów dyskretnych daje się sprowadzić do zagadnienia faktoryzacji. Z kolei temu zagadnieniu będzie poświęcony algorytm w następnym paragrafie. Powróćmy do równania (19)

$$r^x \equiv a \,(mod\, n)$$

z niewiadomą x. Rozwiązanie równania (19), jeśli istnieje, oznaczamy przez $x(n)$. Załóżmy, że liczba n jest postaci

$$n = p_1^{\varepsilon(p_1)} p_2^{\varepsilon(p_2)} ... \, p_m^{\varepsilon(p_m)} \tag{20}$$

gdzie $p_1, ..., p_m$ są liczbami pierwszymi, $\varepsilon(p_i)$ są wykładnikami naturalnymi.

Definiujemy liczby $n_{p_i} = \dfrac{n}{p_i^{\varepsilon(p_i)}}, r_{p_i} = r^{n_{p_i}}, a_{p_i} = a^{n_{p_i}}$ i rozważamy równanie

$$r_{p_i}^x = a_{p_i} \,(mod\, p_i^{\varepsilon(p_i)}), i = 1, ..., m \tag{21}$$

Zakładamy, że równanie (21) ma rozwiązanie. Oznaczamy go przez $x(p_i)$. Rozwiązanie należy do $F_{p_i^{\varepsilon(p_i)}}$. Rozważmy układ kongruencji.

$$x = x(pi) \,(mod\, p_i^{\varepsilon(p_i)}), i = 1, ..., m \tag{22}$$

Twierdzenie 9
Twierdzenie ([2], str. 269). Rozwiązanie problemu (22) istnieje i jest rozwiązaniem równania (19). Należy ono do F_n, gdzie n jest określone wzorem (20)

W dowodzie tego twierdzenia wykorzystuje się chińskie twierdzenie o resztach. Widzimy więc, że rozwiązanie problemu logarytmu dyskretnego można uzyskać poprzez równość (20), a więc poprzez umiejętność przedstawiania liczby całkowitej w formie iloczynów postaci (20), czyli twierdzeniu dotyczącym faktoryzacji.

3.3 Metoda *p-1* Pollarda do faktoryzacji

Prawdziwe i ważne dla kryptografii jest

Twierdzenie 10 ([2], str. 30)
Każda liczba całkowita $n \geqslant 2$ *jednoznacznie wyraża się wzorem* $n = p_1^{\varepsilon(p_1)}...p_m^{\varepsilon(p_m)}$ *gdzie* $p_1, ..., p_m$ *są zawsze liczbami pierwszymi takimi, że* $1 < p_1 < p_2 < ... < p_m, \varepsilon(1), ..., \varepsilon(m)$ *są liczbami naturalnymi.*

Dla kryptografii bardzo ważnym problemem jest znajdowanie tych liczb efektywnie.
Zauważmy, że każda z liczb $p_1, ..., p_m$ jest dzielnikiem liczby n. Problem, o którym mowa wyżej, sprowadza się do znalezienia dzielników pierwszych liczby n wraz z krotnościami. Oznaczamy jeden z nich przez p. Jedną z metod dla znalezienia p jest algorytm $p-1$ Pollarda. Głównym narzędziem tego algorytmu jest Małe twierdzenie Fermata ([2], str. 60). Niech a będzie liczbą całkowitą, p liczbą pierwszą dodatnią, która nie jest dzielnikiem liczby a. Wówczas

$$a^{p-1} \equiv 1 \,(mod\, p) \tag{23}$$

z twierdzenia Fermata wyciągniemy wnioski. Po pierwsze, każda liczba k postaci $k = l(p-1)$ (l jest liczbą naturalną) ma własność

$$a^k \equiv 1 \,(mod\, p) \tag{24}$$

Istotnie, $a^k = a^{l(p-1)} = (a^{p-1})^l \equiv 1^l = 1 \,(mod\, p)$.
Po drugie, liczba $a^k - 1$ jest podzielna przez p dla $k = l(p-1)$.
Powracamy do wyznaczenia podzielnika pierwszego p liczby n. Z tego co dotąd napisaliśmy wynika, że p obok tego, że jest podzielnikiem liczby n jest też podzielnikiem liczby $a^k - 1$ dla $k = l(p-1)$. Rozważmy więc $NWD(a^{k-1}, n)$. Możliwe są dwa przypadki ze względu na k i a.

1. $NWD(a^k - 1, n) = n$
2. $NWD(a^k - 1, n) < n$

W przypadku 1. nie otrzymujemy dzielników liczby n mniejszych od n. Przypadek 2. mówi, że dzielników liczby n należy szukać wśród dzielników liczby $a^k - 1$ mniejszych niż n. Wystarczy więc obliczać $NWD(a^k - 1, n)$ z takim doborem k i a, aby $NWD(a^k - 1, n) < n$. Ale pojawia się tu istotna trudność. Zauważmy, że liczba $a^k - 1 = a^{l(p-1)} - 1$, gdzie l jest dowolnie wybraną liczbą naturalną, zależy od p, która jest dzielnikiem poszukiwanym, a więc nieznanym. Wobec tego liczby $a^{l(p-1)} - 1$ też nie znamy. Jak obliczyć

jej dzielniki. Obliczenie jej dzielników jest możliwe, ale niestety przy ograniczających założeniach o p.

Zakładamy zatem, że liczba $p-1$ (całkowita) wyraża się wzorem

$$p-1 = q_1^{\sigma_1}...q_s^{\sigma_s} \tag{25}$$

gdzie q_i są liczbami pierwszymi, $1 < q_1 < ... < q_s, \sigma_i$ są liczbami naturalnymi. Takie liczby istnieją na podstawie twierdzenia 10. Są one odpowiednikami liczb p_i oraz ε_i z wzoru (20). Liczb q_i oraz σ_i oczywiście nie znamy, ale nie będzie potrzebne ich wyznaczanie. Ograniczające założenie jest następujące. Niech B będzie liczbą daną dodatnią. Zakładamy, że występujące w (25) czynniki spełniają nierówność

$$q_i^{\sigma_i} \leqslant B, i = 1, ..., s \tag{26}$$

Trudność, która wystąpiła wyżej, pokonujemy w sposób następujący. Wybieramy liczbę k jako iloczyn dostatecznie wielu początkowych liczb pierwszych z dostatecznie dużymi wykładnikami potęgowymi tak, by wyrażenie dla k zawierało wszystkie czynniki iloczynu (22). Tak wybrane k jest wielokrotnością liczby $p-1$. Dzięki temu dla tego k zachodzi (19). Wybieramy teraz a, np. $a = 2$. Przy tak wybranych liczbach k i a obliczamy $NWD(a^k - 1, n)$ i sprawdzamy czy $NWD(a^k - 1, n) < n$. Jeżeli tak jest, to droga do obliczenia p okazała się skuteczna. Jeżeli nierówność $NWD(a^k - 1, n) < n$ nie zachodzi, to musimy procedurę rozpocząć od początku z innym wyborem B. Zauważmy to, co bardzo istotne. Nigdzie nie potrzebowaliśmy znać wartości liczbowej p.

3.4 Krzywe eliptyczne

Zanim przystąpimy do omawiania szyfrowania tekstów z wykorzystaniem krzywych eliptycznych, powróćmy do szyfrowania tekstów w oparciu o problem logarytmu dyskretnego w grupie multiplikatywnej ciała skończonego F_p. Używa się tam klucza publicznego i prywatnego oraz związku między nimi.

$$r^k \equiv a \, (mod \, p) \tag{27}$$

Ustala się klucz publiczny jako trójkę (p, r, n). Liczba k jest kluczem prywatnym. Potęga r^k powstała dzięki możliwości dzielenia elementów w ciele F_p: $r^k = r \cdot r....r \, (k \; razy)$. Trudności w rozwiązywaniu problemu znalezienia k całkowitego przy danych p, r, a dały możliwość stworzenia skutecznych systemów kryptograficznych. W ostatnich dziesięcioleciach do tworzenia systemów

kryptograficznych użyto innego równania niż (27). Zastosowano równanie

$$kP = B \tag{28}$$

gdzie P i B są punktami krzywej eliptycznej nad F_p. Stanowią one klucz publiczny. Liczba k jest liczbą całkowitą i stanowi klucz prywatny. Dla punktów krzywej eliptycznej definiuje się działanie dodawania. Symbolem kP oznaczamy punkt krzywej otrzymany przez dodanie do siebie punktu P k razy. Zatem punkty P i B są elementami grupy addytywnej (z dodawaniem). Okazało się, że metody z użyciem krzywych eliptycznych są korzystniejsze niż metody wcześniejsze oparte na ciałach skończonych F_p. Powód leży w tym, że tym razem istnieje bardzo duża możliwość tworzenia grup punktów na krzywej oraz istnieje większa swoboda w wyborze krzywej eliptycznej niż było to z wyborem ciała skończonego. Nie dla wszystkich krzywych przy danych punktach P i B trudno znaleźć k. Problem teraz polega na tym, aby znaleźć klasy krzywych eliptycznych, dla których równanie (28) z niewiadomą k jest bardzo trudno rozwiązać. Od rozwiązania tego problemu zależy bezpieczeństwo systemów kryptograficznych. Przed wysłaniem do odbiorcy wiadomość tekstowa powinna być zakodowana przy pomocy krzywych eliptycznych.
Rozważmy jednostkę tekstu, której odpowiada liczba naturalna m. Chcemy ją zakodować przy pomocy punktu na krzywej eliptycznej $E : y^2 = x^3 + ax + b$, to znaczy chcemy liczbie m przyporządkować jednoznacznie taki punkt $P(x, y) \in E$, aby otrzymać z niego z powrotem liczbę m. Wybieramy ciało F_p z liczbą pierwszą p i liczbę naturalną $\alpha > 0$. Zakładamy, że dla danej liczby M zachodzą równości $0 \leqslant m \leqslant M$ oraz $p > M\alpha$. Rozważmy liczbę $x = m\alpha + j$ gdzie $j \in \{0, 1, ..., \alpha - 1\}$ i obliczamy wartość prawej strony równania E dla takiej liczby x. Wartość tę oznaczamy przez $f(x)$. Powstaje pytanie jak dobrać y całkowite, aby $y^2 = f(x) \,(mod\, 7)$. Wystarczy w tym celu obliczyć pierwiastek kwadratowy z $f(x)$ i przyjąć go jako y. W ten sposób dostajemy punkt $D(x, y)$, który odpowiada liczbie m. Ewentualne trudności z obliczeniem tego pierwiastka pokonujemy przez dobór liczby j. Jeżeli $j = 0$, to ze znajomości punktu $P(x, y)$ wartość m dostajemy ze wzoru $m = \dfrac{m\alpha}{\alpha}$.

Przykład 9
Zakodujemy jako wiadomość literę B z odpowiednikiem liczbowym $m = 1$. Niech $\alpha = 2$, $j = 0$, $p = 7$, $y^2 = x^3 - x + 12$.
Wówczas $f(x) = x^3 - x + 12$. Obliczamy $f(x\alpha) = f(2) = 8 - x + 12 = 18 = 4 \,(mod\, 7)$.
Zatem $y^2 = 18 = 4 \,(mod\, 7)$. Zachodzą równości
$4^4 = (4^{7+1})^{\frac{1}{2}} = (4^{7-1+2})^{\frac{1}{2}} = (4^{7-1})^{\frac{1}{2}} 4 = 4 \,(mod\, 7)$.
Zatem $(4^2)^2 = 4 \,(mod\, 7)$ stąd $y = 4^2 = 16 = 2 \,(mod\, 7)$

Punkt $P(x,y)$ odpowiadający liczbie $m = 1$ ma współrzędne $P(2,2)$. Zauważmy więc, że wzór $m = \frac{m\alpha}{\alpha}$ daje w naszym przypadku $m = 1$.

Ogólne objaśnienie pojęcia krzywej eliptycznej przedstawimy w przypadku, gdy krzywa ta jest położona na płaszczyźnie $\Re^2 = \Re \times \Re$ i jest przedstawiona równaniem

$$y^2 = x^3 + ax + b \tag{29}$$

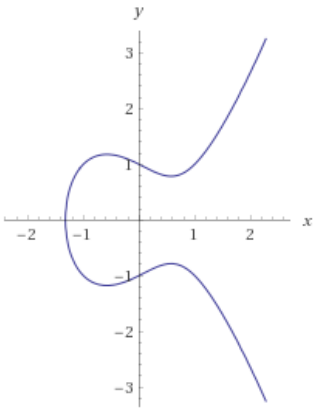
Mówimy wtedy, że rozważamy krzywą eliptyczną nad ciałem liczb rzeczywistych. Para zmiennych (x,y) należy do $\Re^2$, liczby a i $b \in R$ są dane. Wprowadzamy oznaczenie

$$E(\Re) = (x,y) \in \Re^2 : y^2 = x^3 + ax + b \tag{30}$$

Do zbioru $E(\Re)$ zaliczamy również tzw. „punkt w nieskończoności". Oznaczamy go literą O. Punkt ten objaśnimy później. Zakładamy, że dla liczb a i b zachodzi nierówność

$$4a^3 + 27b^2 \neq 0 \tag{31}$$

Warunek (31) gwarantuje, że wielomian po prawej stronie (29) nie ma pierwiastków wielokrotnych. W przypadku $a = -1$, $b = 1$ równanie (B) ma postać $y^2 = x^3 - x + 1$ i określa ono zbiór.



Rysunek 1: $y^2 = x^3 - x + 1$

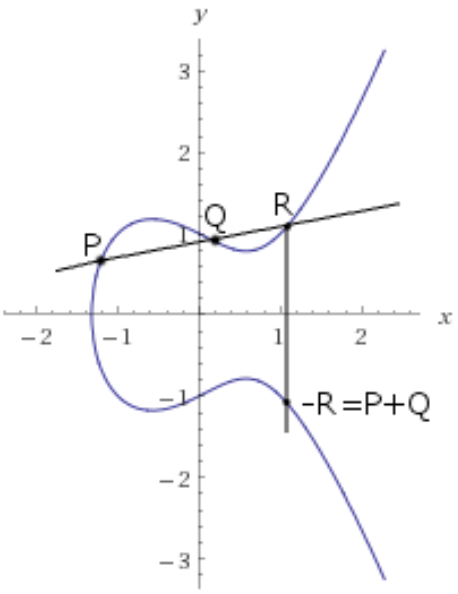
Punkt w nieskończoności wyobrażamy sobie jako graniczne położenie punktu $P(0,y)$, gdy y dąży do nieskończoności. Zauważmy, że dla dużych x krzywa zachowuje się w przybliżeniu tak jak krzywa o równaniu $y = x^{\frac{3}{2}}$.

Krzywa (25) ma bardzo cenną dla kryptografii własność. Pokazuje się ([6], str. 157), że zbiór punktów krzywej tworzy grupę abelową z dodawaniem. Trzeba wskazać element neutralny i element przeciwny. Zajmiemy się teraz definicją dodawania punktów krzywej. Podamy dwie wersje tej definicji: wersję geometryczną i algebraiczną.
Najpierw wersja geometryczna. Definicja składa się z kilku części.
Niech P i O będą dwoma punktami krzywej.

1. Jeżeli $P = O$ (punkt w nieskończoności), to definiujemy punkt przeciwny do P. Oznaczamy go przez $-P$. Z definicji $-P = O$ oraz $P+O = O$. Ostatnia równość oznacza, że punkt O jest elementem neutralnym w zbiorze punktów krzywej.

2. Element przeciwny do $P \neq O$ oznaczamy również przez $-P$. Jeżeli P ma współrzędne (x, y) to $-P$ ma współrzędne $(x, -y)$, czyli $-(x, y) = (x, -y)$. Z równania (3) wynika, że jeżeli punkt (x, y) leży na krzywej (3), to również $(x, -y)$ leży na tej samej krzywej.

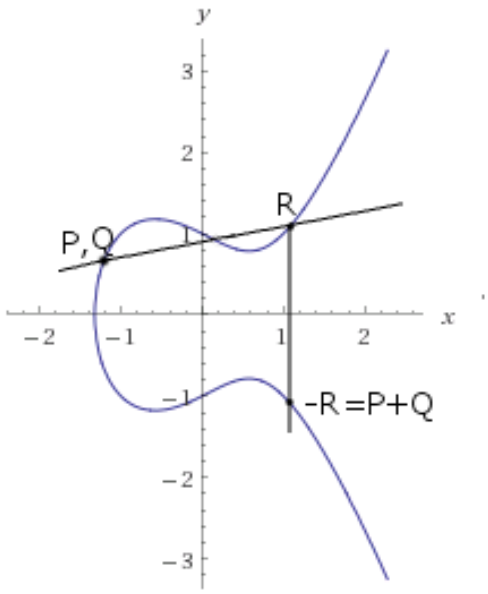
3. Jeżeli punkty P i O mają różne współrzędne x, to rozważamy sieczną PQ. Przecina ona krzywą w pewnym punkcie R (jedynym, różnym od P i Q). Sumę $P + Q$ definiujemy jako $-R$. Jeżeli ta prosta jest styczna do krzywej P, to $R = P$. Jeżeli ta prosta jest styczna do krzywej w punkcie Q, to $R = Q$ (Rysunek 2).



Rysunek 2: Dodawanie punktów należących do krzywej eliptycznej

4. Jeżeli $Q = -P$ to z definicji $P + Q = O$.

5. Jeżeli $P = Q$ wówczas rozważamy prostą l styczną do krzywej w punkcie P i punkt R przecięcia tej prostej z krzywą. Sumę P+Q definiujemy jako $P + Q = -R$. Jeżeli punkt P jest punktem przecięcia krzywej, wówczas $R = P$ (Rysunek 3).



Rysunek 3: Dodawanie punktów krzywej eliptycznej, gdy P=Q

Stwierdziliśmy już wcześniej, że symbolem kP, $k \in Z$, oznaczamy punkt otrzymany przez dodanie do siebie punktu P k razy.

Zajmijmy się teraz algebraiczną wersją dodawania punktów krzywej (3). Niech punkty P i Q będą dane, jak w przypadku 3 definicji geometrycznej dodawania, przy pomocy współrzędnych $P(x_1, y_1)$, $Q(x_2, y_2)$. Zakładamy, że $x_1 \neq x_2, y_1 \neq y_2$. Wyrazimy współrzędne sumy $R(x_3, y_3)$ przy pomocy współrzędnych $(x_1, y_1)(x_2, y_2)$. Równanie prostej przechodzącej przez punkty P i Q ma postać

$$y = \alpha x + \beta \tag{32}$$

Z faktu, że punkty P i Q spełniają to równanie wynika, że
$\alpha = \dfrac{y_2 - y_1}{x_2 - x_1}$ oraz $\beta = y_1 - \alpha x_1$
bo $y_1 = \alpha x_1 + \beta$, $y_2 = \alpha x_2 + \beta$
Zatem $\alpha(x_2 - x_1) = y_2 - y_1$, czyli $\alpha = \dfrac{y_2 - y_1}{x_2 - x_1}$ oraz $y_1 = \alpha x_1 + \beta$ stąd $\beta = y_1 - \alpha x_1$

Jeżeli punkt (x, y) prostej (32) leży na krzywej (29) to spełnia równanie

$$(\alpha x + \beta)^2 = x^3 + ax + b \; czyli \; x^3 - \alpha^2 x^2 + (a - 2\alpha\beta)x + (b - \beta^2) = 0 \tag{33}$$

Jest to równanie stopnia trzeciego ze względu na x. Ma ono trzy rozwiązania. Dwa z nich to liczby x_1, x_2. Są to pierwsze współrzędne punktów P i Q leżących na krzywej (29) i na prostej (32). Trzecim rozwiązaniem równania (33) jest liczba x_3 wyrażona wzorem

$$x_3 = \alpha^2 - x_1 - x_2 \tag{34}$$

Aby uzasadnić wzór (34) skorzystamy z twierdzenia mówiącego, że suma $x_1 + x_2 + x_3$ rozwiązań równania (33) równa jest współczynnikowi przy x^2 z przeciwnym znakiem. Twierdzenie to wynika z porównania współczynników przy odpowiednich potęgach x w tożsamości

$x^2 + a_2x^2 + a_1x + a_0 = (x - x_1)(x - x_2)(x - x_3) = x^3 - (x_1 + x_2 + x_3)x^2 + (x_2x_3 + x_1x_3 + x_1x_2 - x_1x_2x_3)$

Z wzoru (34) dostajemy współrzędne punktu $R = (x_3, \alpha x_3 + \beta)$ w postaci

$$\begin{aligned} x_3 &= (\frac{y_2 - y_1}{x_2 - x_1})^2 - x_1 - x_2 \\ y_3 &= -y_1 + (\frac{y_2 - y_1}{x_2 - x_1})(x_1 - x_3) \end{aligned} \tag{35}$$

Zauważmy, że współrzędne (x_3, y_3) przedstawione we wzorach (35) wyrażają się wyłącznie przy pomocy współrzędnych punktów $(x_1, y_1)(x_2, y_2)$. Dodajmy, że we wzorze (35) na y_3 w miejsce x_3 należy wstawić wyrażenie występujące o jeden wiersz wyżej.

W przypadku 5 definicji geometrycznej, gdy $P = Q$ zamiast siecznej używamy stycznej w punkcie P i zamiast α w postaci ilorazu $\frac{y_2 - y_1}{x_2 - x_1}$ używamy pochodnej funkcji $y(x)$ określonej w sposób uwikłany przy pomocy równania krzywej. Otrzymujemy wówczas dla α wyrażenie

$\alpha = \frac{3x_1^2 + a}{2y_1}$

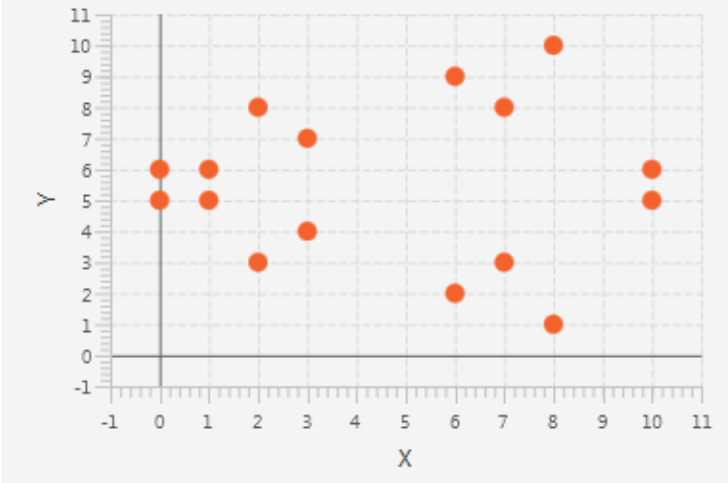
Otrzymujemy stąd wzory na współrzędne punktu $2P$ w postaci

$$\begin{aligned} x_3 &= (\frac{3x_1^2 + a}{2y_1})^2 - 2x_1 \\ y_3 &= -y_1 + \frac{3x_1^2 + a}{2y_1}(x_1 - x_3) \end{aligned} \tag{36}$$

Korzystając ze wzorów (35) i (36) otrzymujemy współrzędne sumy $P+Q$ oraz kP, jeżeli współrzędne punktów P i Q oraz liczba k są dane.

Dotychczas rozważaliśmy krzywe eliptyczne nad ciałem liczb rzeczywistych. Wykres krzywej otrzymywaliśmy przez wstawienie do równania (29)

punktów $(x, y) \in \Re^2$. Ponieważ po lewej stronie równania (29) występuje y^2, to wykres krzywej przebiega symetrycznie do osi x. Wartość y otrzymuje się jedynie dla tych wartości x, dla których strona równania (29) jest dodatnia. Dla zastosowań kryptografii będziemy rozważać obecnie krzywe eliptyczne nad ciałem skończonym $F_p = \{1, 2, ..., p-1\}$. Aby F_p było ciałem zakładamy, że p jest liczbą i $p > 2$.
Wykres krzywej (29) nie będzie teraz krzywą ciągłą lecz będzie składał się z izolowanych punktów położonych na płaszczyźnie $\Re^2$. Dla przykładu wykres krzywej $y^2 = x^3+x+3$ przedstawimy na rysunku 4 w przypadku $F_{11}(p = 11)$.



Rysunek 4: $E(F_{11})$

Badać będziemy też pary liczb

$$\{(1,1)(1,2)...(1,p-1)$$
$$.$$
$$. \qquad (37)$$
$$.$$
$$(p-1,1)(p-1,2)...(p-1,p-1)\}$$

które równanie (29) spełniają modulo p. Ważne będą dla nas liczby ze zbioru F_p, dla których prawa strona równania (29) jest kwadratem modulo p. Nie wszystkie punkty (37) spełniają równanie (29). Na temat liczby punktów (37), które należą do krzywej eliptycznej (modulo p) prawdziwe jest twierdzenie Hassego ([9], str. 138)

Twierdzenie 11 (twierdzenie Hassego)
Niech N będzie liczbą F_p-punktów na krzywej eliptycznej zdefiniowanej nad ciałem F_p. Wtedy zachodzi nierówność $|N - (p+1)| \leqslant 2\sqrt{p}$.

Dla bezpieczeństwa systemów kryptograficznych ważny jest wybór liczby p tak dużej, by punktów na krzywej eliptycznej było bardzo dużo. Twierdzenie Hassego nie dostarcza efektywnego algorytmu dla wyliczenia liczby punktów krzywej w F_p ([9], str. 139). Dostarcza jedynie oszacowania wielkości tej liczby. Ale w szczególnych przypadkach, korzystając z tego twierdzenia można liczbę punktów krzywej w F_p obliczyć dokładnie.

Przykład 10
Niech dana będzie krzywa $y^2 = x^3 - x$ nad ciałem F_{71}.
Liczbę punktów tej krzywej można wyrazić wzorem ([7], str. 214)

$1 + \sum_{x \in F_p} (1 + X(x^3 - x)) = 1 + p + \sum_{x \in F_p} X(x^3 - x)$

gdzie funkcja X jest tzw. symbolem Legendre'a ([7], str. 64) określonym wzorem:

$X(x) = \frac{x}{p} = \{x$, gdy $p|x$ 1, gdy x jest resztą kwadratową modulo p
-1, gdy x jest nieresztą modulo p $\}$

Wyrażenie $x^3 - x$ jest równe 0 względem x w każdej rozważanej sytuacji. Zatem liczba punktów krzywej $y^2 = x^3 - x$ w F_{71} wynosi 1+71 =72.

3.5 Szyfrowanie w systemie ElGamala z wykorzystaniem krzywych eliptycznych

Rozważmy system, który jest odpowiednikiem, na gruncie krzywych eliptycznych, systemu ElGamala przedstawionego w punkcie poprzednim w oparciu o grupę multiplikatywną ciała F_p*. Rozpoczynamy, jak wcześniej, od ustalenia liczby pierwszej $p > 2$ i ciała liczbowego $F_p* = \{1, 2, ..., p-1\}$. Następnie ustalamy krzywą eliptyczną $E(F_p*)$ w postaci

$$y^2 = x^3 + ax + b, \text{ gdzie } a, b, x, y \in F_p* \tag{38}$$

Aby bezpiecznie przesłać zaszyfrowaną wiadomość musimy ją najpierw zakodować. Dla prostoty prezentacji niech wiadomość będzie liczbą W. Chodzi zatem o przyporządkowanie wiadomości W pewnego punktu na krzywej eliptycznej (38). Oznaczmy ten punkt przez $P \in E(F_p*)$. Nadawca N, pragnący użyć systemu ElGamala do przesyłania wiadomości W odbiorcy O, wybierze dowolnie punkt $B \in E(F_p*)$ i ujawnia go. Odbiorca wybiera tajną liczbę k, której nie ujawnia, ale ujawnia punkt kB. Nadawca ma więc do dyspozycji dwa punkty: B i kB. Dysponuje też punktem P, który oznacza zakodowaną wiadomość W. Wówczas nadawca wybiera losowo liczbę $r \in F_p*$ i przekazuje odbiorcy zaszyfrowaną wiadomość W w formie pary punktów $(rB, P + r(kB))$. Po otrzymaniu tej pary punktów odbiorca mnoży punkt

rB przez tajne k i wynik tego działania odejmuje od drugiego punktu. Zna punkty B i kB, bo są one ujawnione. Nie zna liczby k mimo, że zna punkt kB. Potraktujmy więc punkty B i kB jako dane na krzywej. Dla pełnej jasności użyjmy nawet innej litery na kB. Niech $kB = B_p$. Widzimy stąd, że trzecia osoba może odszyfrować wiadomość, jeśli znajdzie liczbę $k \in Z$ taką, że $kB = B_p$. A więc odszyfrowuje wiadomość wtedy, kiedy znajdzie rozwiązanie logarytmu dyskretnego na krzywej eliptycznej.

$$P + r(kB) - k(rB) = P \tag{39}$$

W ten sposób punkt (39) daje wiadomość P. Powstaje teraz bardzo ważne pytanie. Czy oraz w jaki sposób osoba trzecia może odszyfrować przesłaną wiadomość? Przedstawmy aktualną sytuację. Osoba trzecia ma dostęp do dwóch punktów krzywej związanych z przesyłaną wiadomością.

Ogólne metody rozwiązania tego problemu nie są znane. Bezpieczeństwo systemów kryptograficznych opartych na problemie logarytmu dyskretnego opiera się na dotychczasowych niepowodzeniach w próbach rozwiązania tego problemu. Zauważmy na koniec, że w systemie ElGamala liczba punktów na krzywej nie jest potrzebna.

4 Część programistyczna

W części programistycznej pracy został przedstawiony program komputerowy mojego autorstwa, który implementuje algorytm szyfrowania i odszyfrowania metodą ElGamala przy wykorzystaniu krzywych eliptycznych. Dodatkowymi funkcjonalnościami są: rysowanie wykresu $E(F_p)$, losowy wybór parametrów krzywej eliptycznej i ciała F_p oraz kalkulator punktów. Program zawiera również funkcję demonstracji, która w sposób automatyczny prezentuje po kolei wszystkie etapy użycia algorytmu ElGamala na krzywej eliptycznej, od wyboru krzywej eliptycznej i ciała, przez szyfrowanie i odszyfrowanie punktu należącego do $E(F_p)$.

Program zawiera graficzny interfejs użytkownika.

4.1 Architektura programu

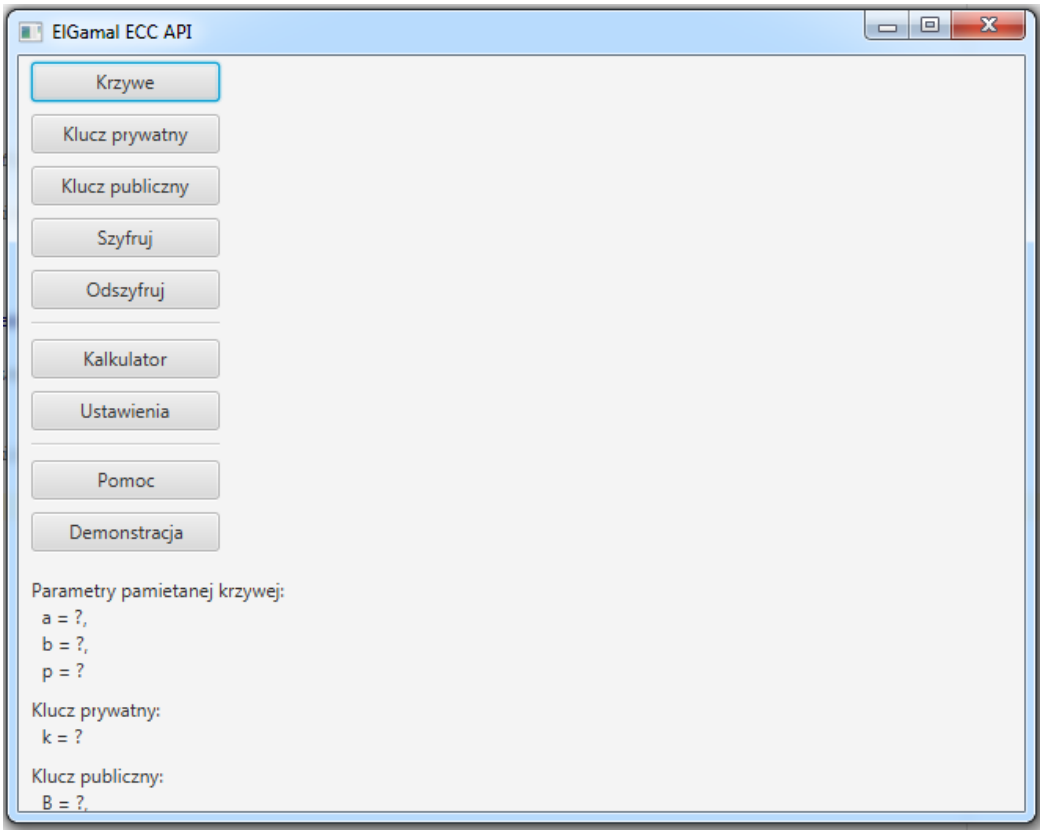
Program napisany został w języku Java z wykorzystaniem pakietu do tworzenia graficznego interfejsu użytkownika -*JavaFX*.

4.2 Opis głównych funkcjonalności programu

Działanie programu koncentruje się na pięciu głównych funkcjonalnościach:

1. Rysowanie wykresu $E(F_p)$.
2. Szyfrowanie punktu w systemie ElGamala opartym o krzywe eliptyczne.
3. Odszyfrowanie punktu w systemie ElGamala opartym o krzywe eliptyczne.
4. Kalkulator punktów wybranej krzywej eliptycznej nad ciałem F_p.
5. Demonstracja szyfrowania i odszyforwywania punktów $E(F_p)$ algorytmem ElGamala opartym o krzywe eliptyczne.

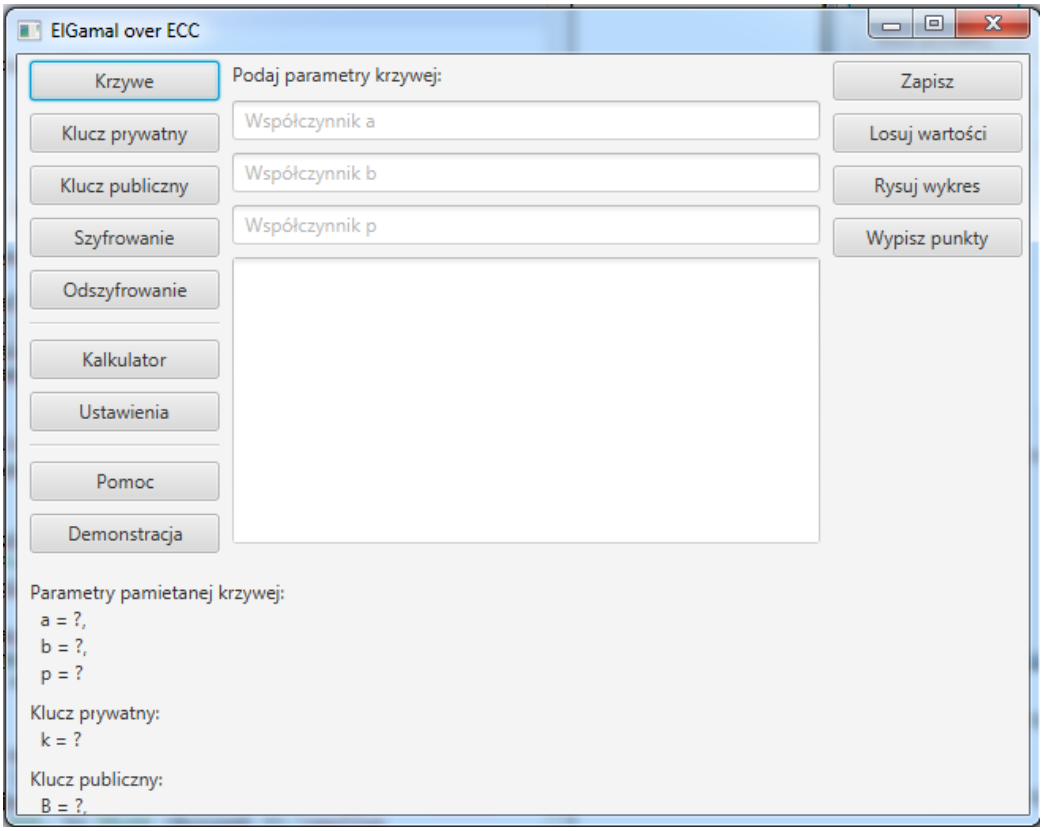
Po uruchomieniu programu pojawia się okno główne (Rysunek 5) z menu głównym oraz znajdującą się pod nim informacją o zapisanych wartościach parametrów *Parametry pamiętanej krzywej, Klucz prywatny, Klucz publiczny*, które są wykorzystywane do działania funkcjonalności programu. Znak *?* oznacza, że dany parametr nie został jeszcze wybrany i zapisany.
Po wyborze z menu głównego jednego z przycisków: *Krzywe, Klucz prywatny, Klucz publiczny, Szyfruj, Odszyfruj, Kalkulator, Ustawienia* w centralnej części programu pojawia się formularz wejścia, konsola, na której wypisywane są wyniki działania programu oraz submenu dla danej funkcjonalności (Rysunek 6). Dla każdej funkcjonalności pola formularza oraz zawartość submenu mogą się różnić między sobą.



Rysunek 5: Okno główne programu. Zawiera menu główne oraz pole z informacjami o zapisanych parametrach.

Program działa w jednym oknie, gdyż ma on charakter demonstracyjny i dydaktyczny. Należy pamiętać jednak, że szyfrowanie i odszyfrowanie może zachodzić na kontach dwóch różnych użytkowników, a co za tym idzie na różnych fizycznych urządzeniach.

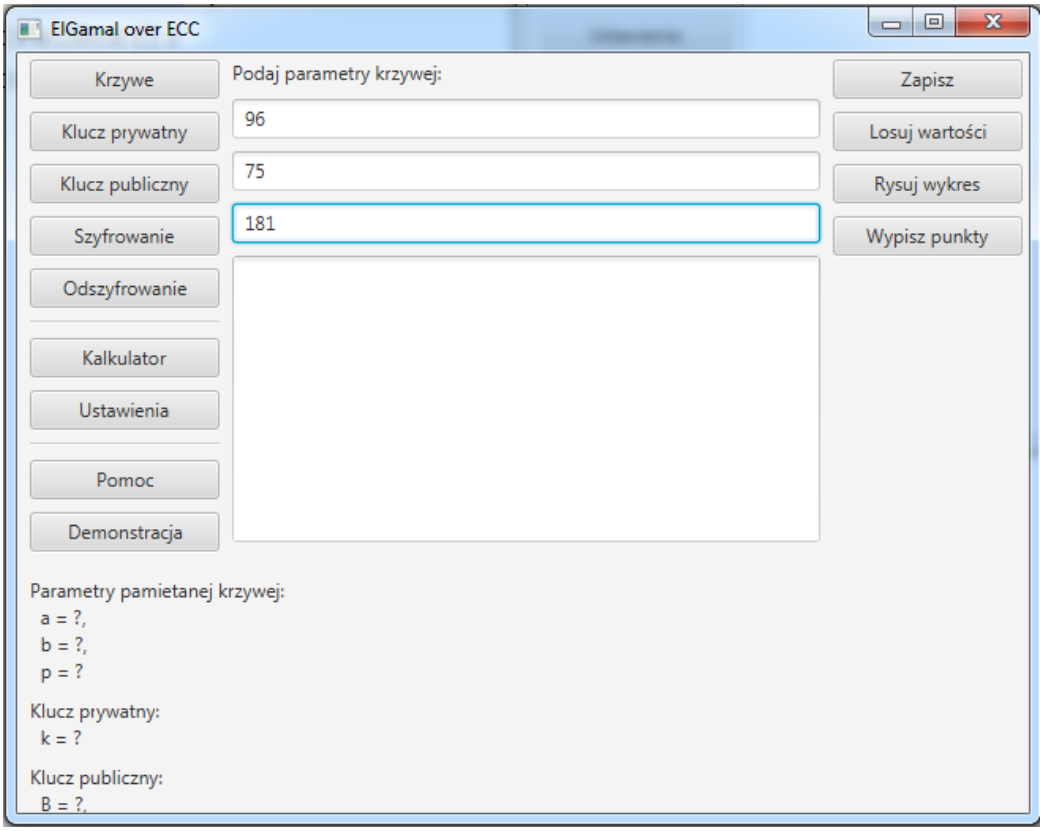
Funkcjonalność rysowanie wykresu *E(Fp)*. Z menu głównego należy wybrać przycisk *Krzywe* (Rysunek 6). Następnie należy wybrać parametry, na podstawie których zostanie wygenerowany wykres. Te parametry to a, b, które odnoszą się do współczynników w równaniu krzywej $y^2 = x^3 + ax + b$ oraz p, który odnosi się do parametru p w ciele F_p.



Rysunek 6: Formularz wyboru współczynników krzywej eliptycznej a, b oraz p dla ciała F_p

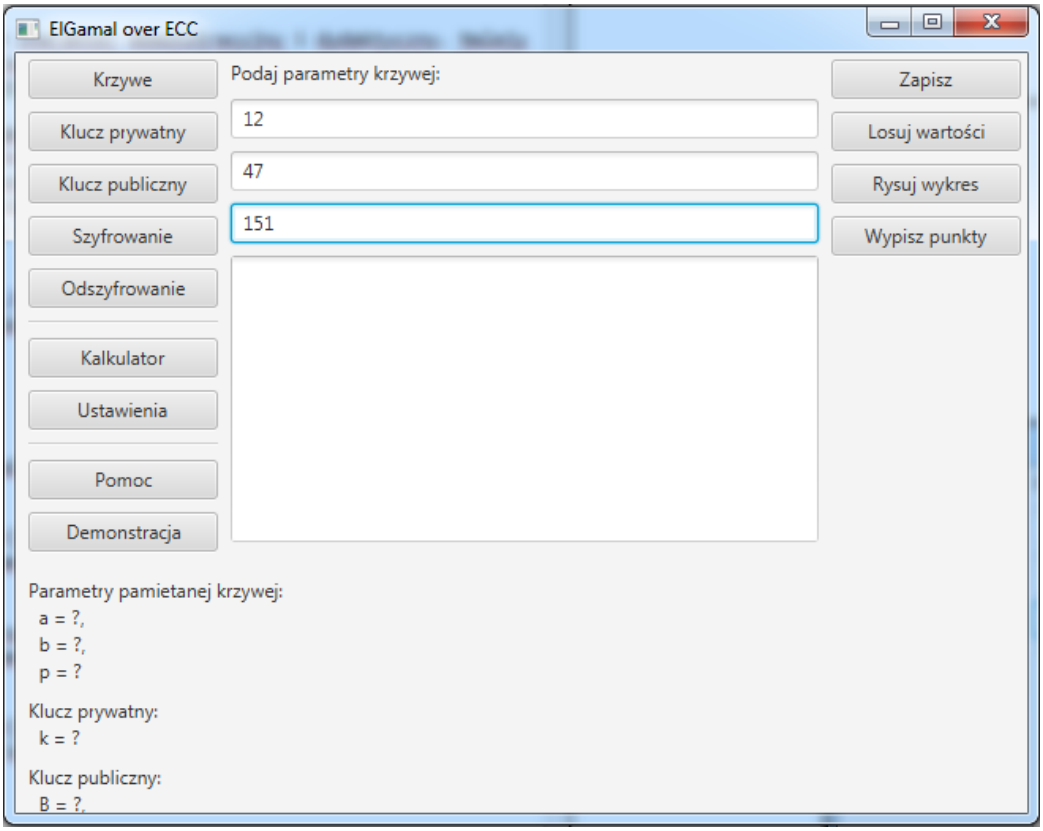
Istnieją dwa sposoby wyboru parametrów:

1. Ręczne wpisanie parametrów do pól formularza programu (Rysunek 7).



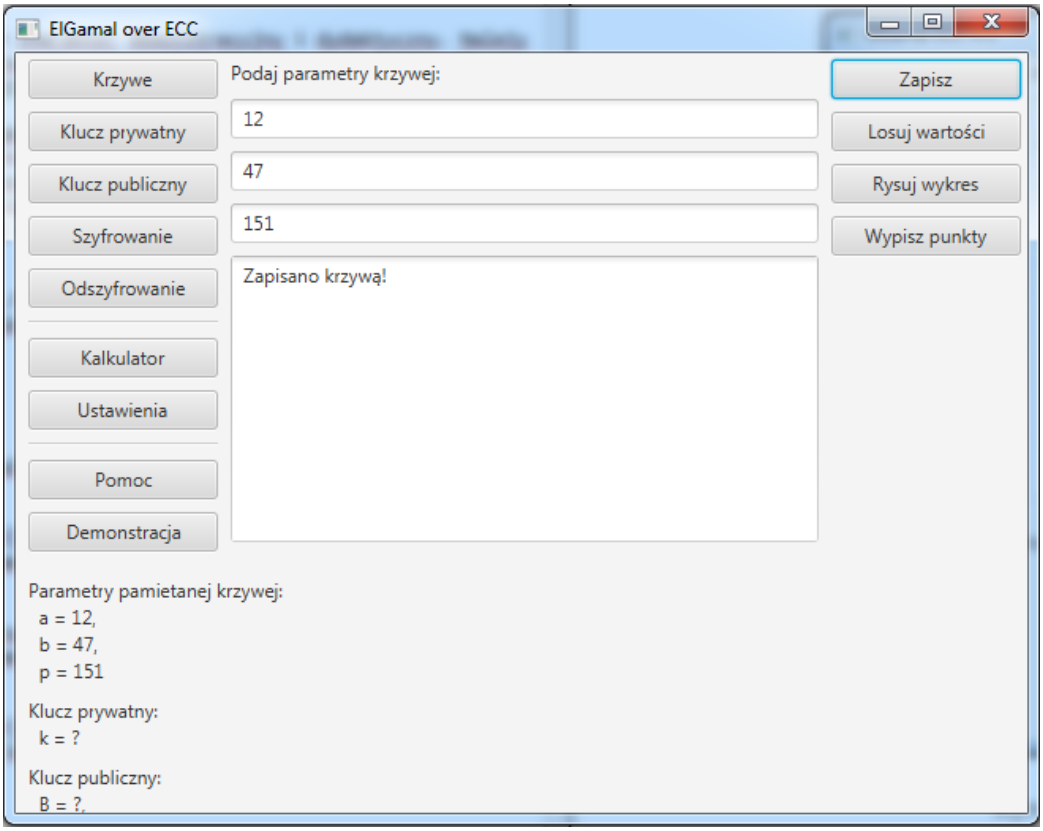
Rysunek 7: Ręczne uzupełnienie parametrów krzywej eliptycznej i ciała F_p

2. Wylosowanie parametrów przez program. W tym celu należy wybrać przycisk *Losuj wartości* z prawego submenu (Rysunek 8).



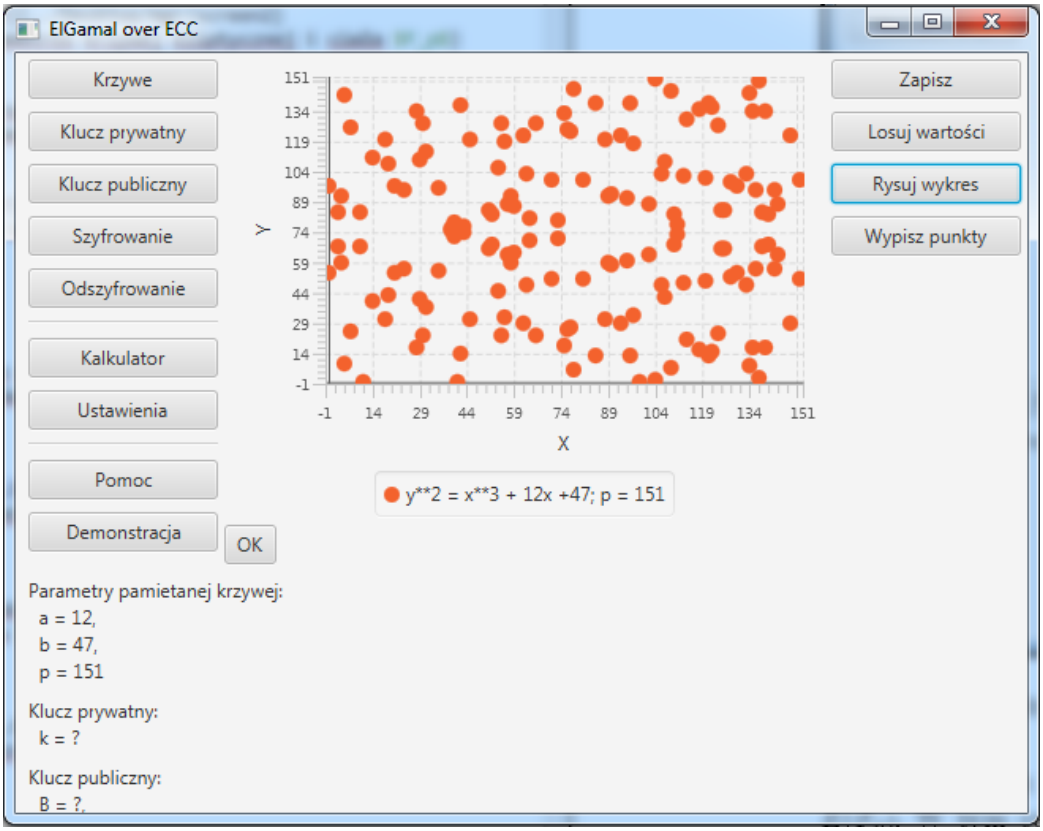
Rysunek 8: Losowy wybór parametrów krzywej eliptycznej i ciała F_p przez program

Gdy pola a, b, p są już uzupełnione należy wybrać przycisk *Zapisz* (Rysunek 9).Zapisane wartości zostaną wyświetlone pod menu głównym w *Parametry pamiętanej krzywej* (Rysunek 9).



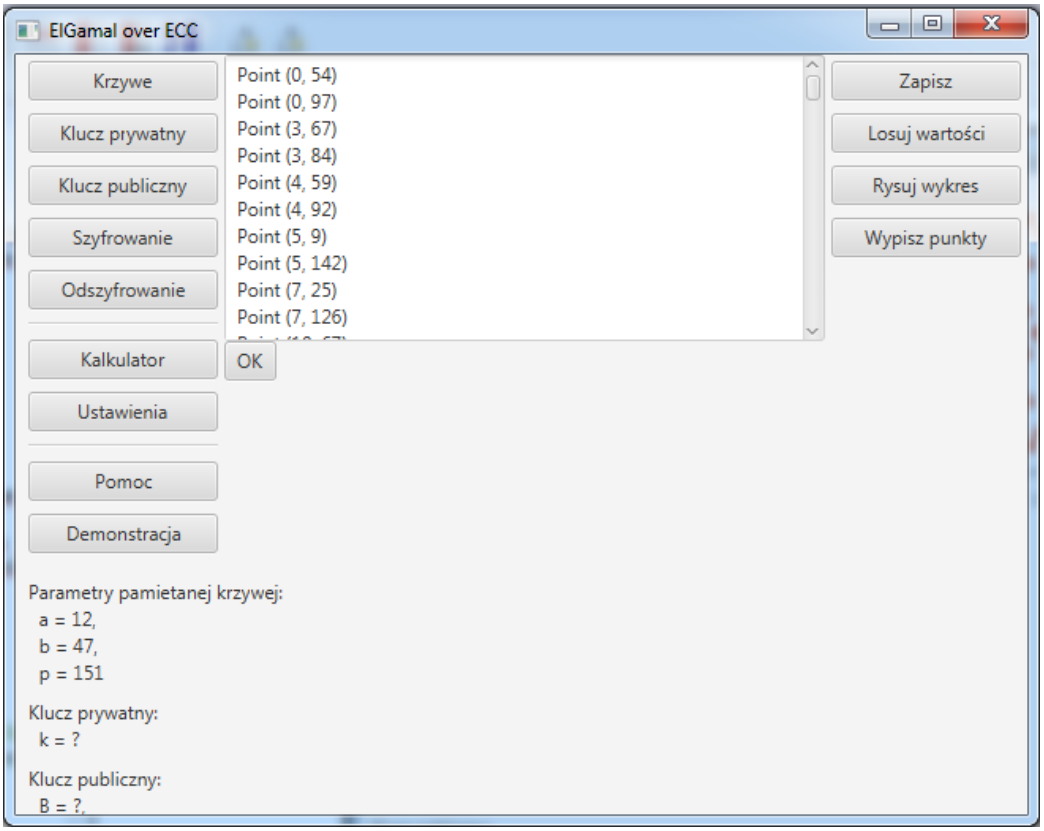
Rysunek 9: Zapisywanie wybranych parametrów

Następnie należy wybrać w submenu przycisk *Rysuj wykres* (Rysunek 10). Efektem działania programu jest zwrócenie wykresu $E(F_p)$ z parametrami konkretnie zadanych we wcześniejszym kroku (Rysunek 10).



Rysunek 10: Wykres $E(F_p)$ dla wybranych wartości parametrów

Dostępna jest również opcja przeglądania listy punktów, które należą do $E(F_p)$. W tym celu należy wybrać przycisk *Wypisz punkty* (Rysunek 11). Program zwróci listę tych punktów (Rysunek 11).



Rysunek 11: Wypisanie listy punktów należących do $E(F_p)$ dla wybranych wartości parametrów

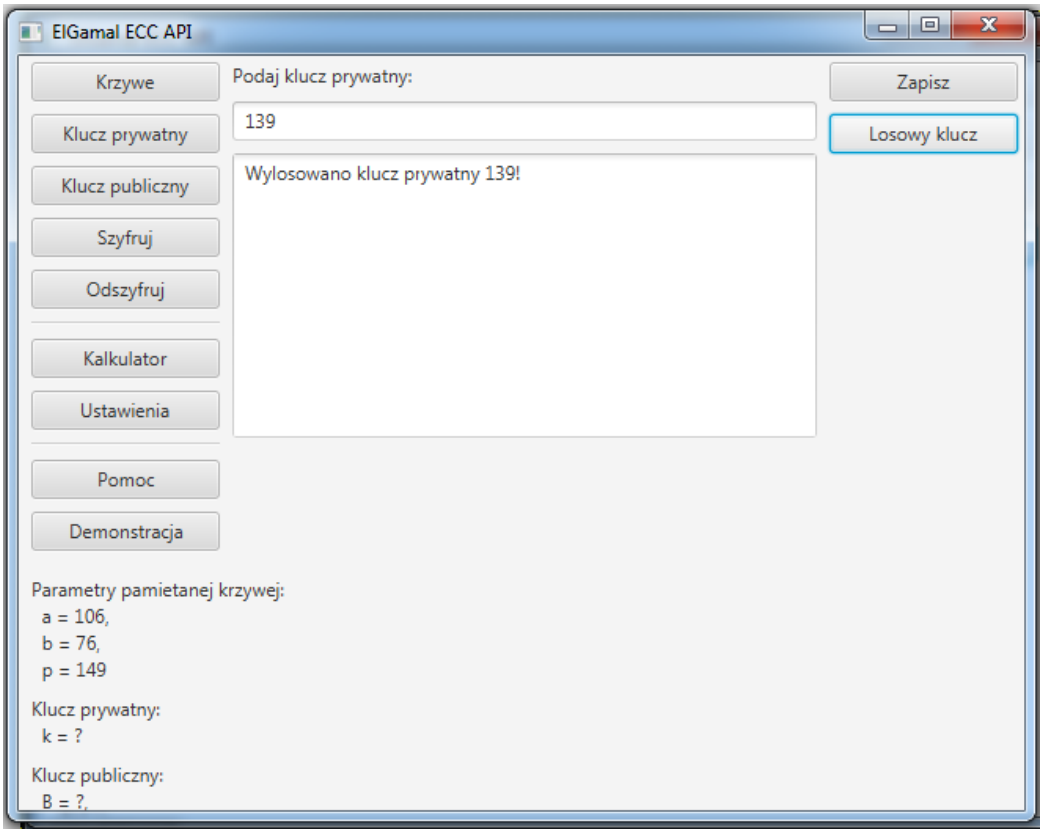
Funkcjonalność szyfrowanie punktów w systemie ElGamala opartym o krzywe eliptyczne. W systemie ElGamala opartym o krzywe eliptyczne wiadomość, która ma być zaszyfrowana najpierw podawana jest kodowaniu. Kodowanie polega na przypisaniu konkretnej wiadomości tekstowej określonej reprezentacji w zbiorze punktów $E(F_p)$. Problem ten nie jest jednak szerzej poruszany w niniejszej pracy więc program pomija etap kodowania i szyfruje jedynie sam wybrany punkt należący do $E(F_p)$.

W celu zaszyfrowania punktu należy wykonać kolejno następujące kroki:

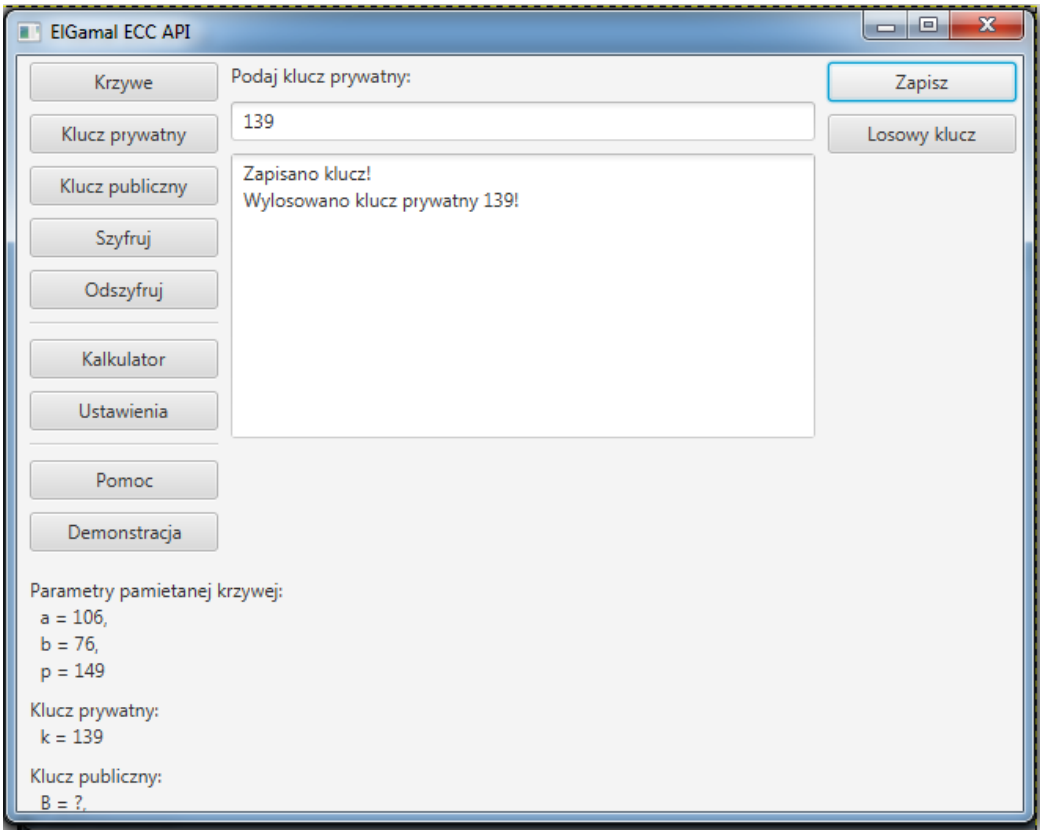
1. **Wybór parametrów** a, b odnoszących się do krzywej eliptycznej i p odnoszący się do ciała F_p. Należy to zrobić w ten sam sposób, jak w pokazano w opisie poprzedniej funkcjonalności **Funkcjonalność rysowanie wykresu** $E(F_p)$.

2. **Wybór klucza prywatnego.** Z menu głównego należy wybrać przy-

cisk *Klucz prywatny* (Rysunek 12), a następnie wpisać ręcznie do formularza wartość, która będzie kluczem prywatnym. Można również programowo wylosować tą wartość przez wybranie z submenu funkcji *Losuj klucz*. Następnie należy wybrać przycisk *Zapisz*(Rysunek 13). Informacja o zapisanych parametrach pojawi się w polu pod menu głównym w sekcji *Klucz prywatny*(Rysunek 13)

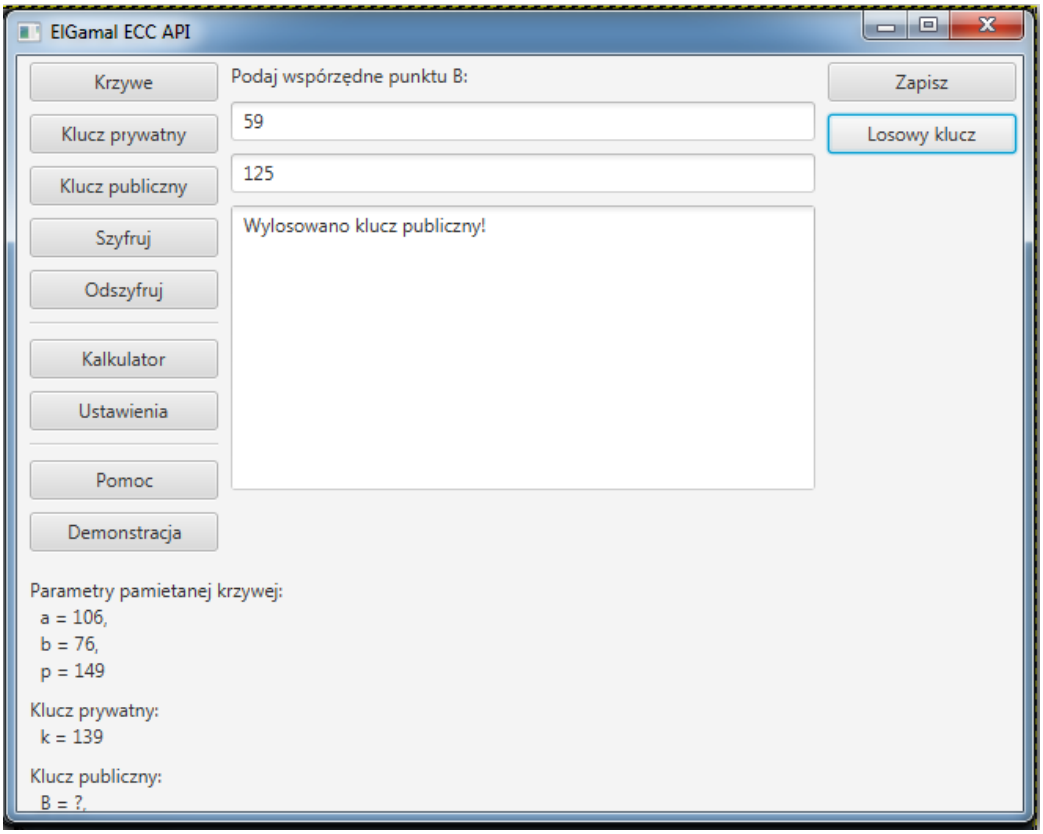


Rysunek 12: Wybór wartości klucza prywatnego

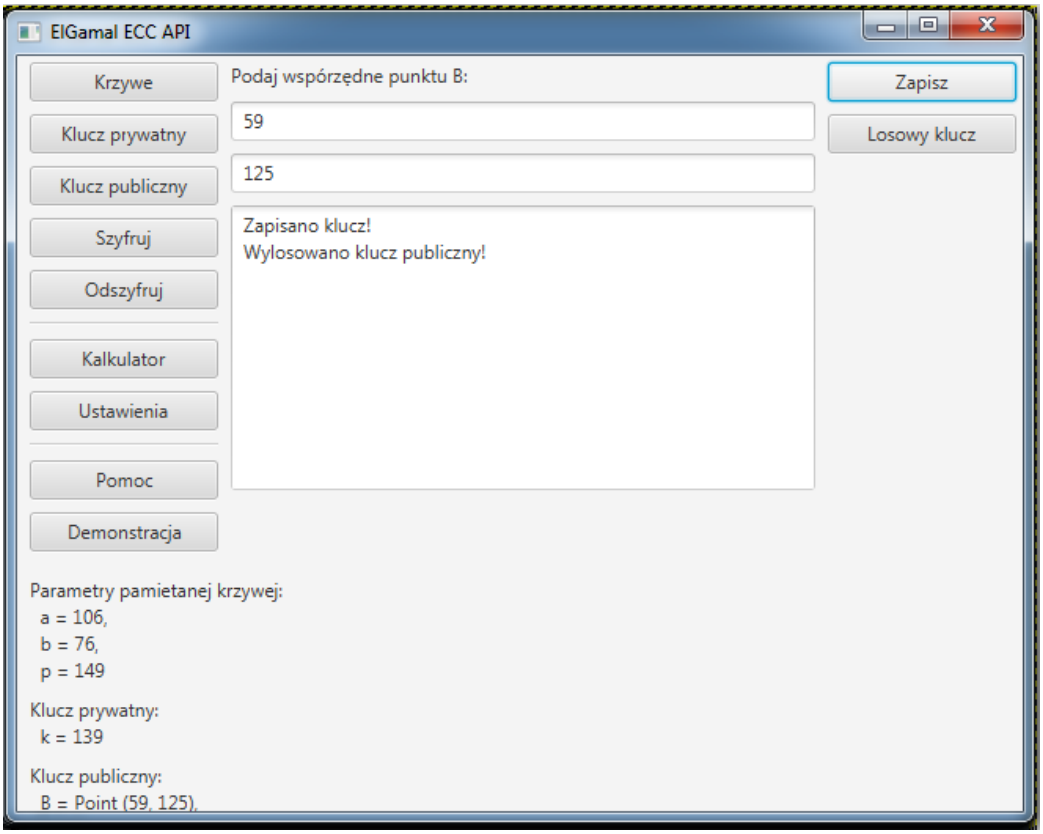


Rysunek 13: Zapisywanie wartości klucza prywatnego

3. **Wybór klucza publicznego.** Z menu głównego należy wybrać przycisk *Klucz publiczny* (Rysunek 14). Do wygenerowania klucza publicznego konieczne jest wcześniejsze ustawienie wartości klucza prywatnego (punkt 2) w przeciwnym wypadku program zwróci błąd. Klucz publiczny generowany jest z klucza prywatnego k i punktu B należącego do $E(F_p)$. W formularzu należy wpisać ręcznie współrzędne x, y punktu B lub wylosować je (poprzez wybór przycisku w submenu *Losowy klucz* (Rysunek 14)), a następnie zapisać przez kliknięcie przycisku *Zapisz*(Rysunek 15). Zapisana wartość klucza publicznego pojawi się w polu pod menu głównym w sekcji *Klucz publiczny*(Rysunek 15).

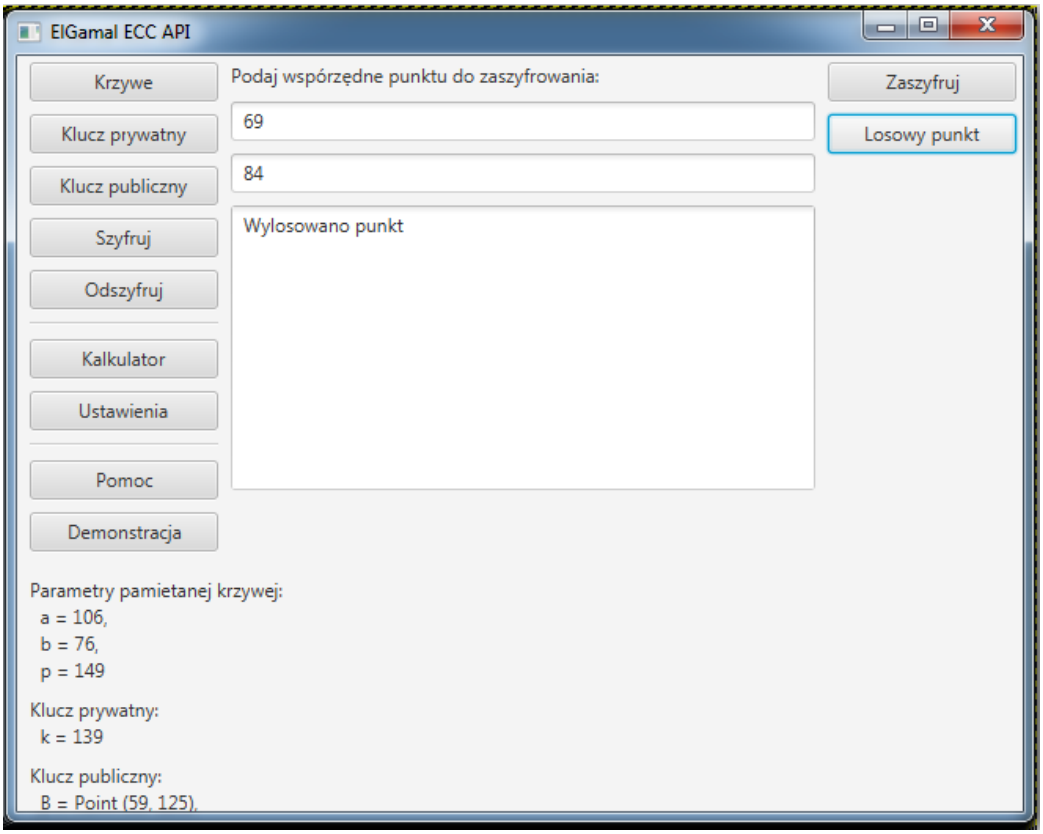


Rysunek 14: Losowanie klucza publicznego



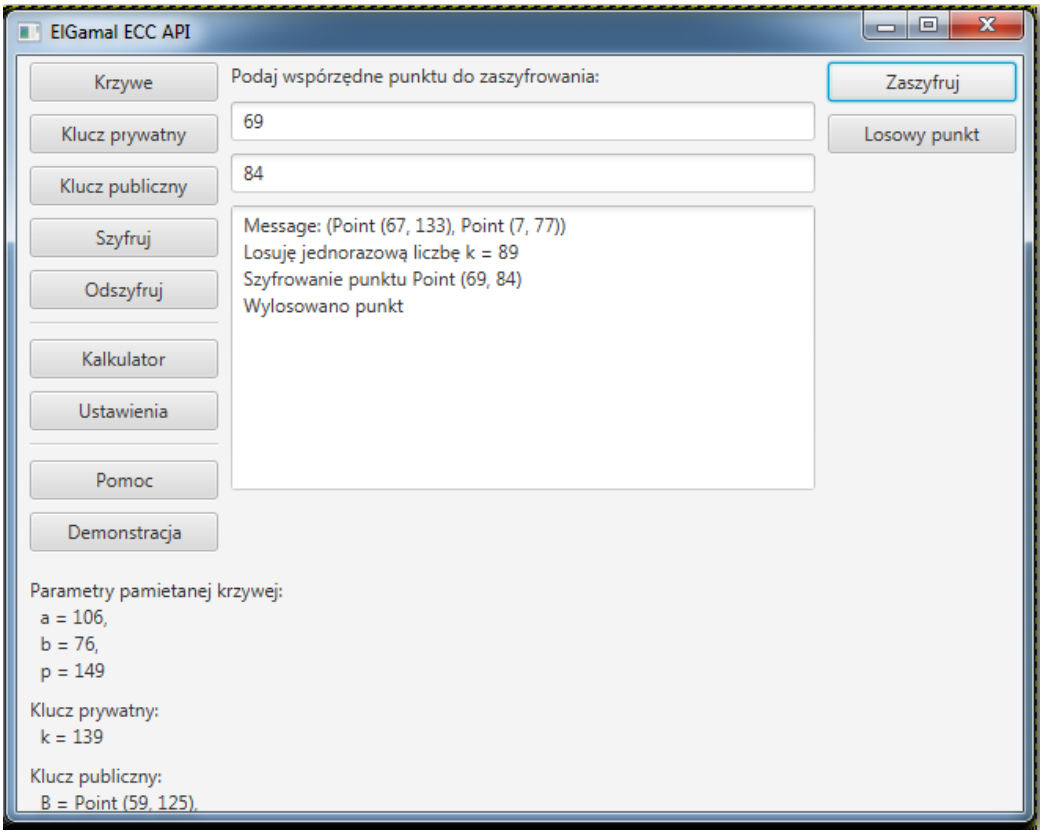
Rysunek 15: Zapisywanie klucza publicznego

Gdy powyższe trzy kroki są już wykonane i w polu pod menu głównym w sekcjach *Parametry pamiętanej krzywej, Klucz prywatny, Klucz publiczny* wszystkie wartości są wypełnione, to z menu głównego należy wybrać *Szyfruj*, a następnie wpisać ręcznie do formularza lub wylosować poprzez wybranie w sumbemu przycisku *Losowy punkt* współrzędne x, y punktu do zaszyfrowania (Rysunek 16). Punkt ten musi należeć do zbioru $E(F_p)$.



Rysunek 16: Wybór punktu należącego do $E(F_p)$ do zaszyfrowania

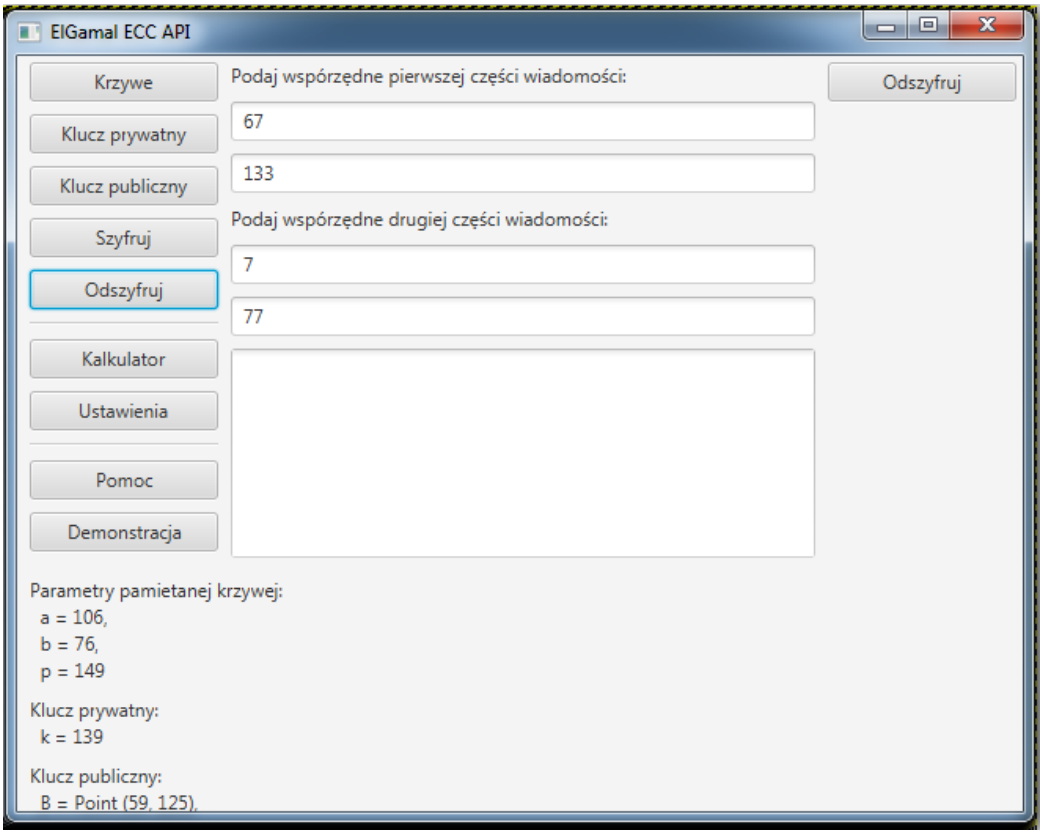
Następnie w submenu wybieramy przycisk *Szyfruj*.



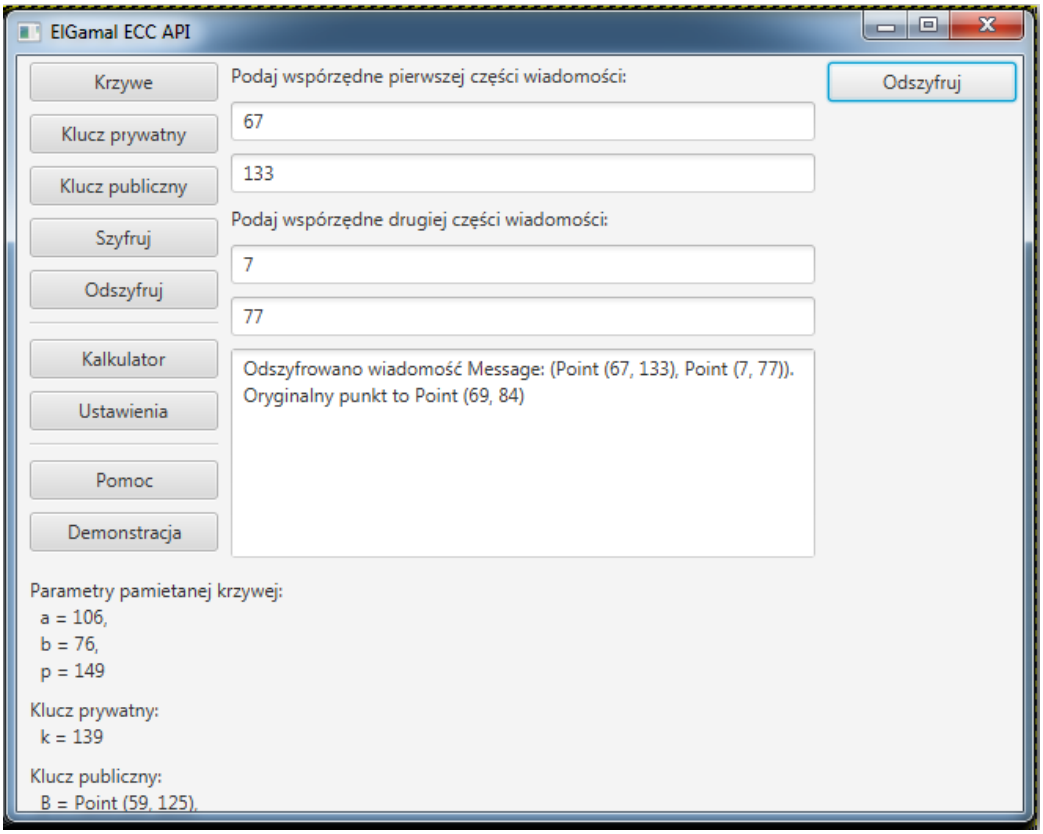
Rysunek 17: Szyfrowanie punktu

W wyniku działania funkcji szyfrowania program zwraca dwa punkty, które stanowią szyfrogram (wiadomość, która została zaszyfrowana). Są one wypisane w konsoli pod formularzem (Rysunek 17).

Funkcjonalność odszyfrowanie punktów w systemie ElGamala opartym o krzywe eliptyczne. W celu odszyfrowania zaszyfrowanego wcześniej punktu wybieramy z menu głównego przycisk *Odszyfruj*. Jeśli w *Ustawienia* jest zaznaczona opcja *Autouzupełnianie szyfrogramu przy odszyfrowaniu* to pola formularza same automatycznie zostaną uzupełnione przez współrzędne szyfrogramu uzyskanego w poprzednim kroku (Rysunek 18), jeśli nie, należy je wpisać ręcznie do pól formularza. Następnie należy wybrać z submenu przycisk *Odszyfruj*. W wyniku działania odszyfrowywania program zwraca współrzędne punktu, który został zaszyfrowany i wyświetla je w konsoli pod formularzem (Rysunek 19).



Rysunek 18: Wprowadzanie szyfrogramu do odszyfrowania



Rysunek 19: Rozszyfrowanie punktu

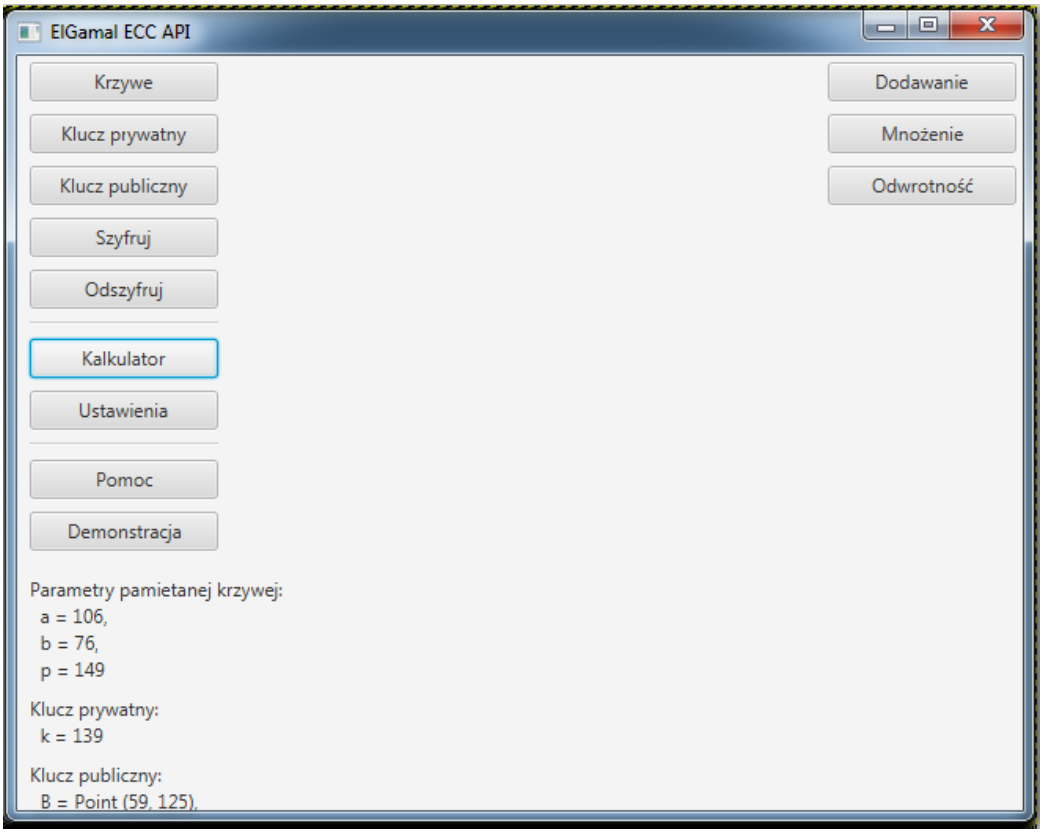
Funkcjonalność kalkulator punktów wybranej krzywej eliptycznej nad ciałem Fp. Z menu głównego należy wybrać przycisk *Kalkulator*. Do korzystania z tej funkcjonalności konieczne jest wcześniejsze ustawienie parametrów krzywej eliptycznej i ciała F_p. Należy to zrobić tak jak pokazano w opisie funkcjonalności **Funkcjonalność rysowanie wykresu *E(Fp)*.** Funkcjonalność kalkulator umożliwia wykonywanie trzech typów działań (Rysunek 20):

1. **Dodawanie do siebie dwóch punktów należących do *E(Fp)*.** Z submenu należy wybrać przycisk *Dodawanie* (Rysunek 21), a następnie uzupełnić pola formularza współrzędnymi x, y punktów A i B, które mają być do siebie dodane (Rysunek 22). Aby otrzymać wynik, należy wybrać przycisk *Oblicz wynik*. Suma pojawi się w polach formularza i jest to punkt o współrzędnych x, y (Rysunek 23).

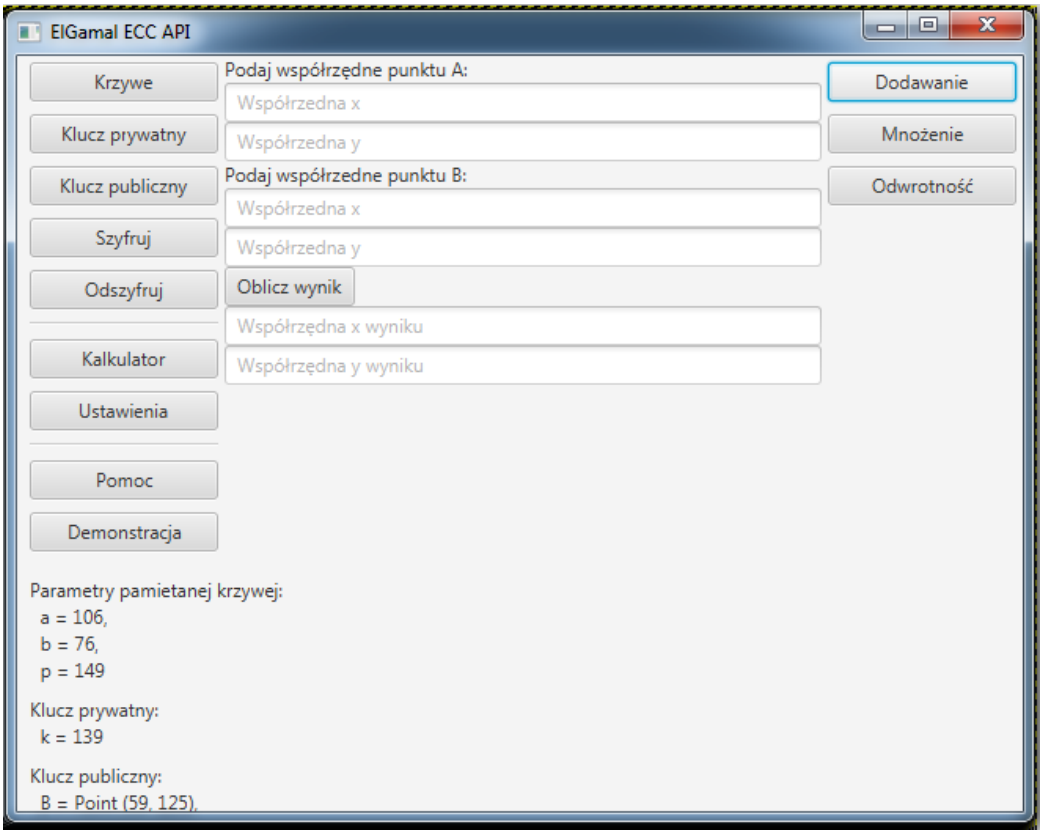
2. **Mnożenie punktu przez liczbę.** Z submenu należy wybrać przycisk *Mnożenie*, a następnie uzupełnić pola formularza współrzędnymi

x, y punktu A oraz liczbę całkowitą k, przez którą ma być pomnożony punkt A (*Czynnik liczbowy*)(Rysunek 24). Aby otrzymać wynik, należy wybrać przycisk *Oblicz wynik*. Iloczyn pojawi się w polach formularza i jest to punkt o współrzędnych x, y (Rysunek 25).

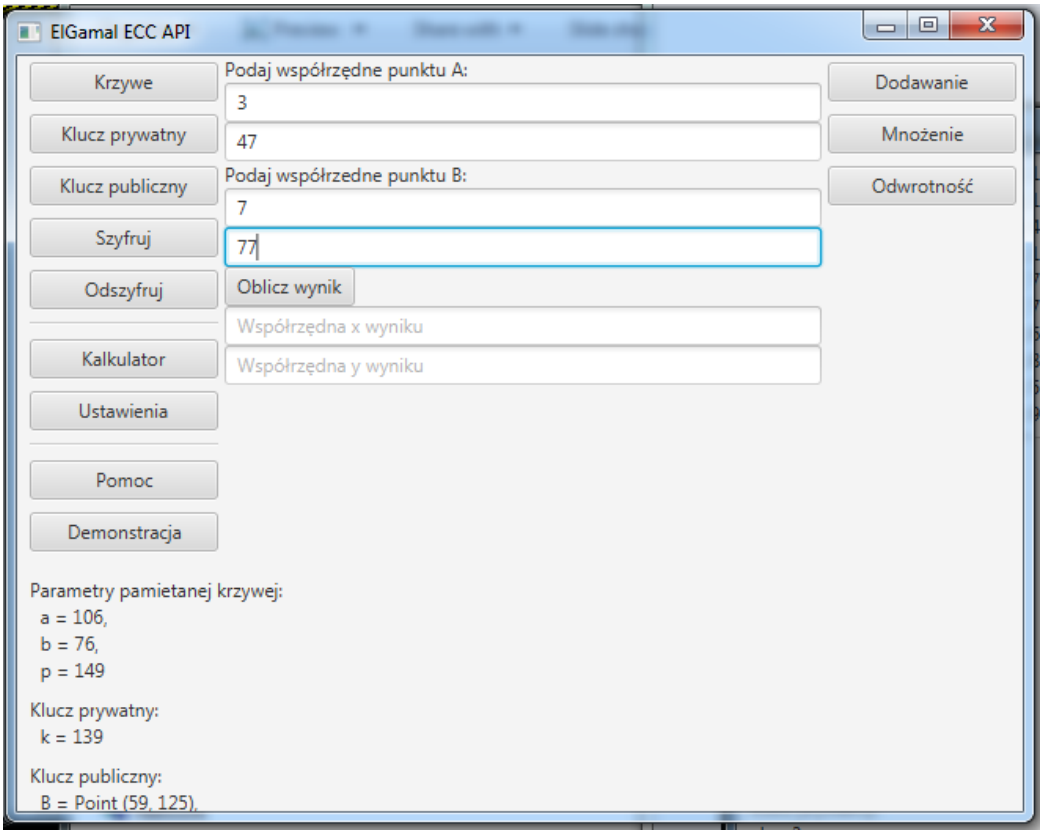
3. **Wyliczanie punktu odwrotnego.** Z submenu należy wybrać przycisk *Odwrotność*, a następnie uzupełnić pola formularza współrzędnymi x, y punktu A, którego odwrotność ma być obliczona (Rysunek 26). Aby otrzymać wynik należy wybrać przycisk *Oblicz wynik*. Współrzędne punktu odwrotnego pojawią się w formularzu (Rysunek 27).



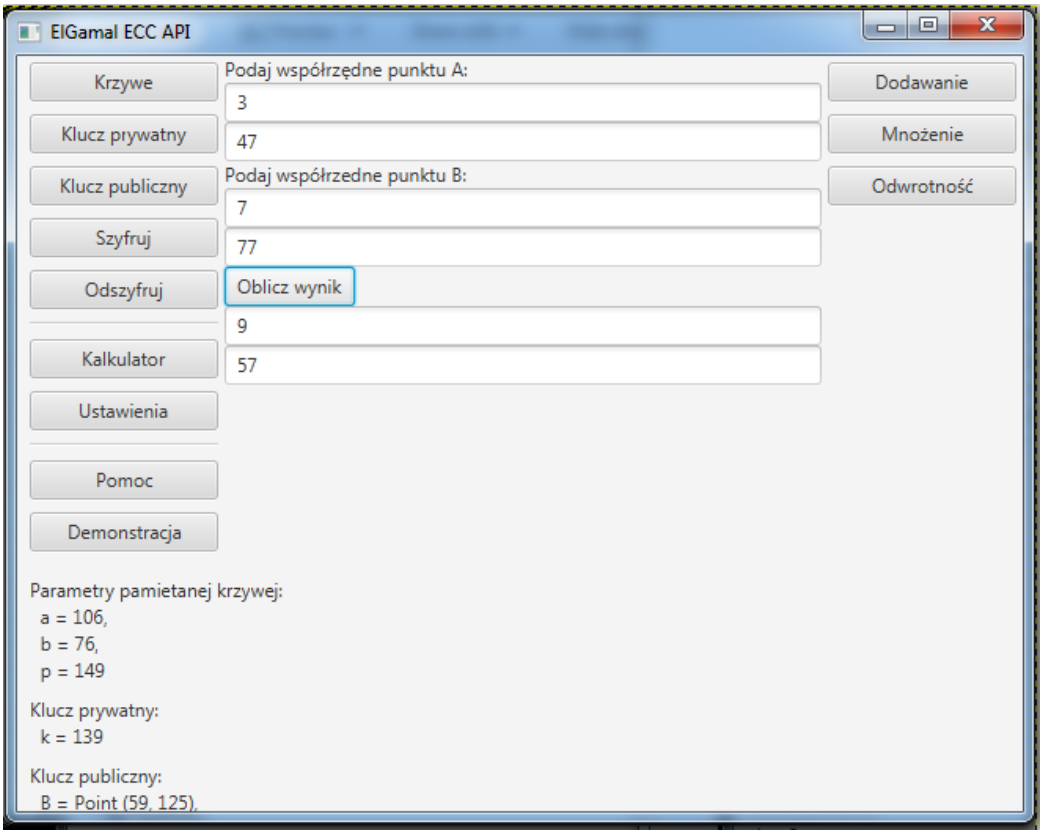
Rysunek 20: Kalkulator punktów $E(F_p)$



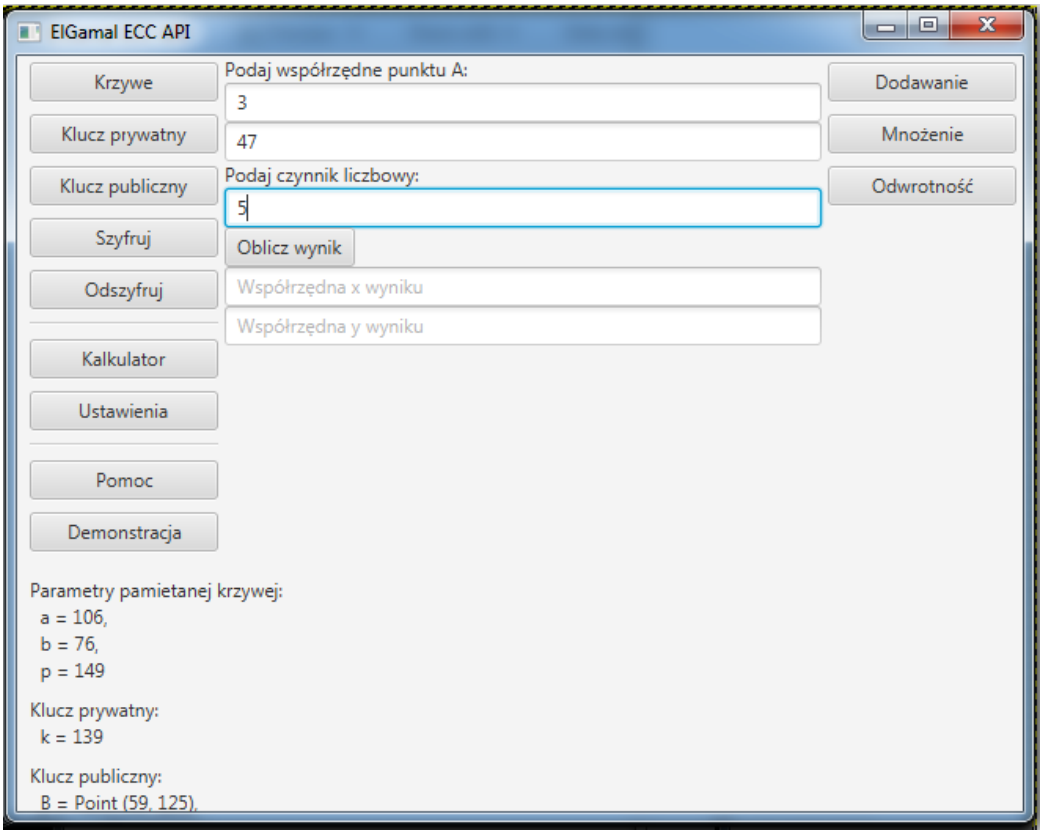
Rysunek 21: Kalkulator: dodawanie dwóch punktów



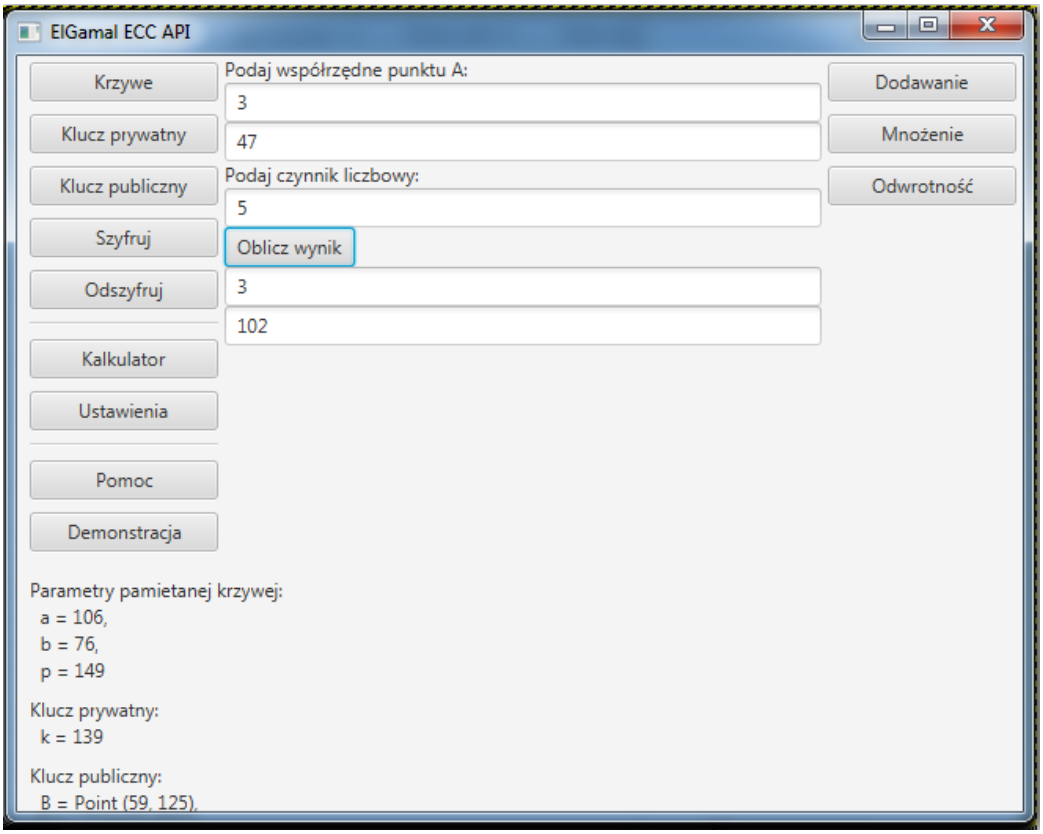
Rysunek 22: Wprowadzanie współrzędnych punktów, które mają być dodane



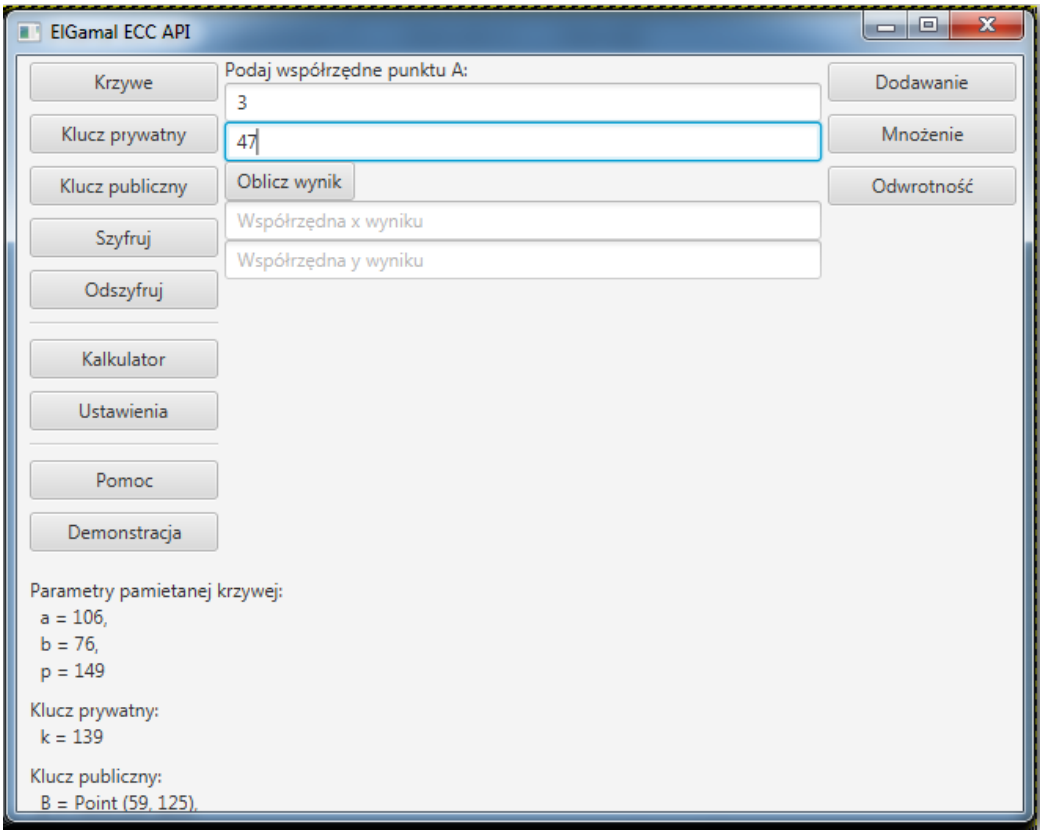
Rysunek 23: Obliczanie wyniku dodawania punktów



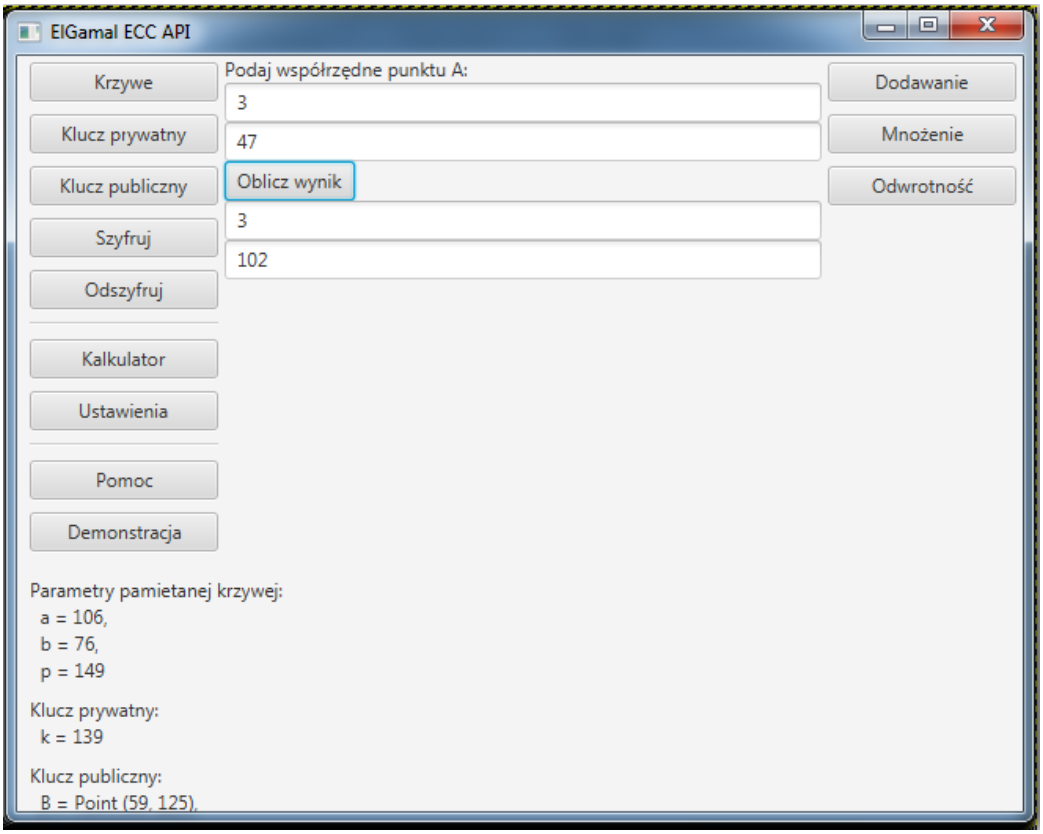
Rysunek 24: Wprowadzanie współrzędnych punktu oraz liczby, które mają być pomnożone



Rysunek 25: Obliczanie wyniku mnożenia

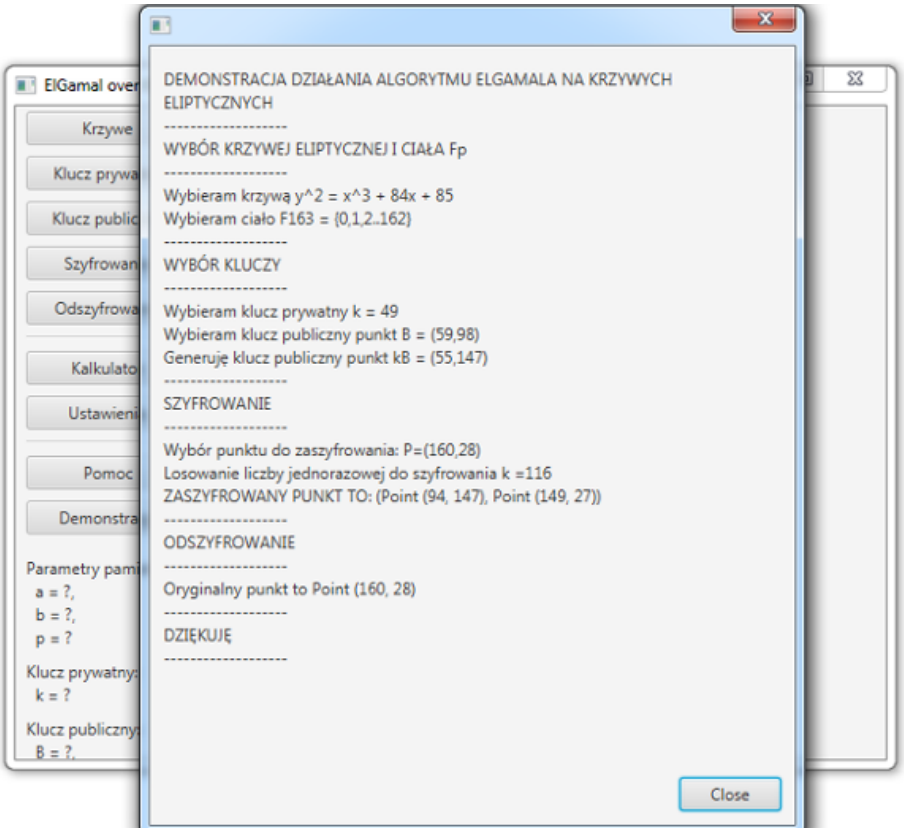


Rysunek 26: Wprowadzanie współrzędnych punktu, dla którego wyliczona ma być odwrotność



Rysunek 27: Obliczanie wartości punktu odwrotnego

Demonstracja działania programu Po wybraniu z menu głównego przycisku *Demonstracja* pojawia się okienko, w którym krok po kroku program sam wypisuje przebieg szyfrowania i odszyfrowania punktu metodą ElGamala (Rysunek 28).



Rysunek 28: Demonstracja szyforwania i odszyfrowania punktu algorytmem ElGamala

Opis dodatkowych funkcjonalności:

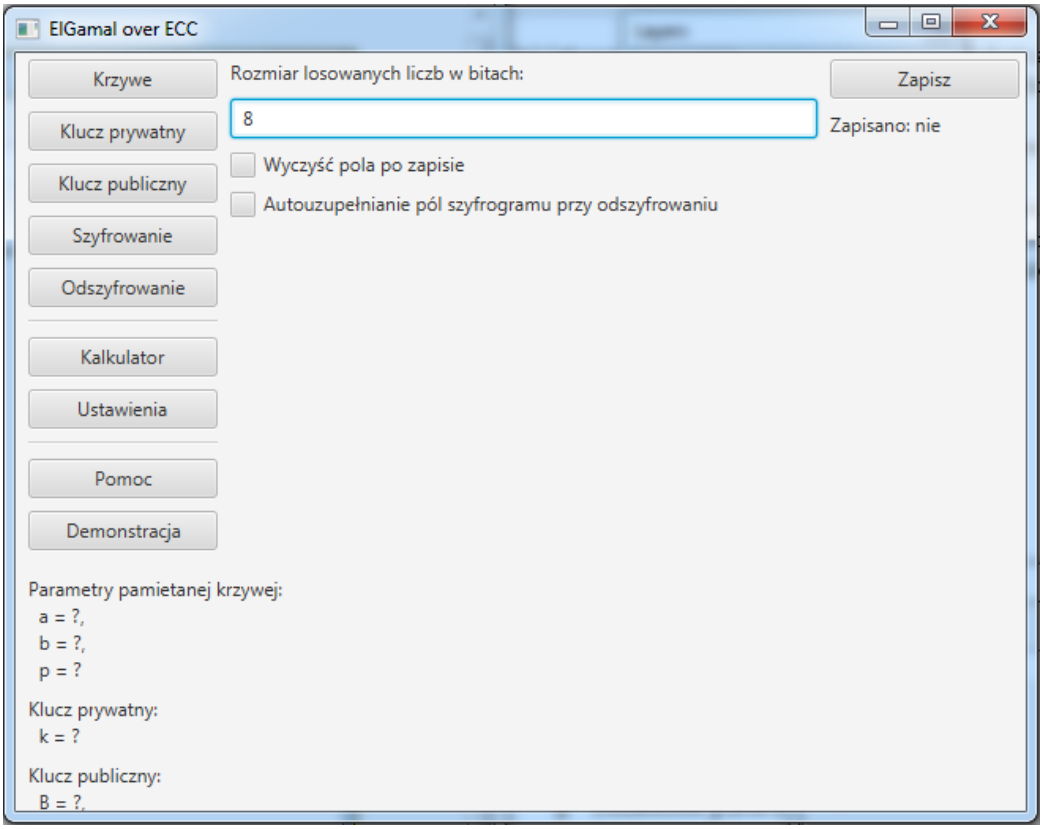
Ustawienia

1. **Rozmiar losowanych liczb w bitach.** Wszystkie parametry odnoszące się do działania programu takie jak: a, b, p, k oraz współrzędne punktów A, B można wpisać ręcznie bezpośrednio do formularza. Należy jednak wtedy pamiętać o relacjach pomiędzy konkretnymi parametrami. Aby to uprościć, można również posłużyć się parametrami automatycznie wygenerowanym przez program. W tym celu należy wybrać przycisk losowania znajdujący się w submenu w określonej funkcjonalności.

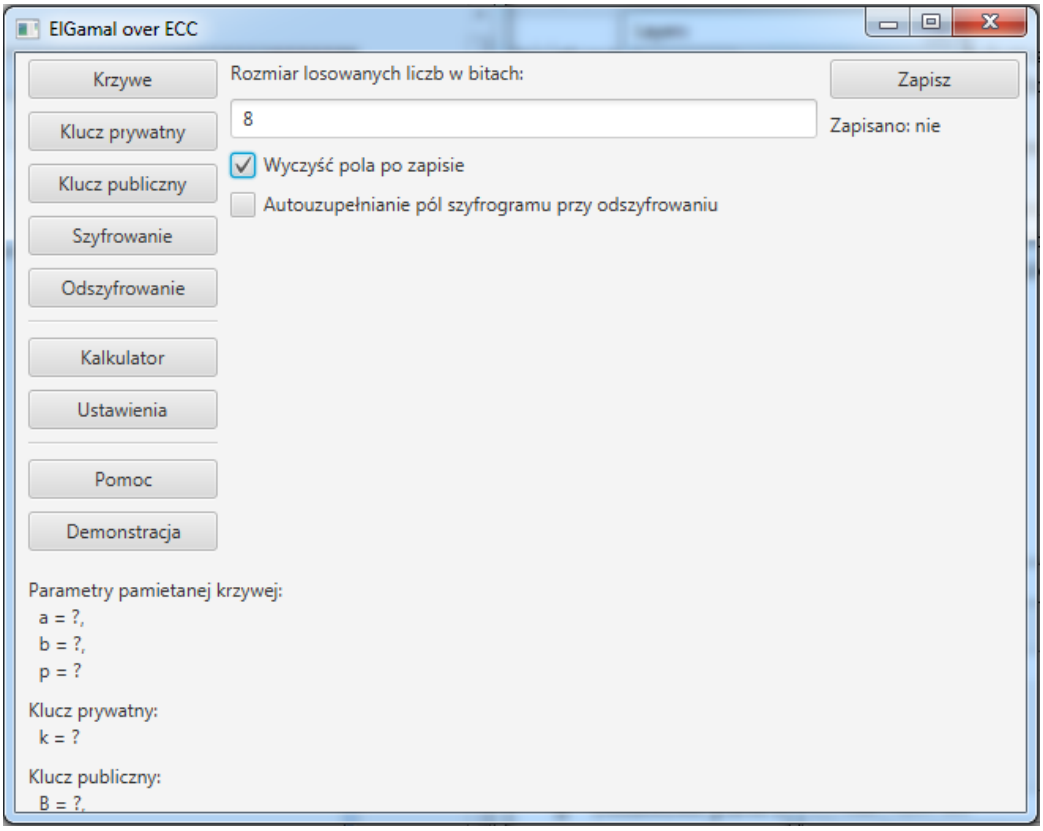
   Liczbę bitów losowanej wartości można regulować w zakładce *Ustawienia* poprzez wpisanie w polu formularza *Rozmiar losowanych liczb w bitach* określonej liczby (Rysunek 29).

2. **Wyczyść pola po zapisie.** Zaznaczenie tej opcji powoduje automatyczne czyszczenie pól formularza zaraz po zapisaniu znajdujących się w nich wartości (Rysunek 30).

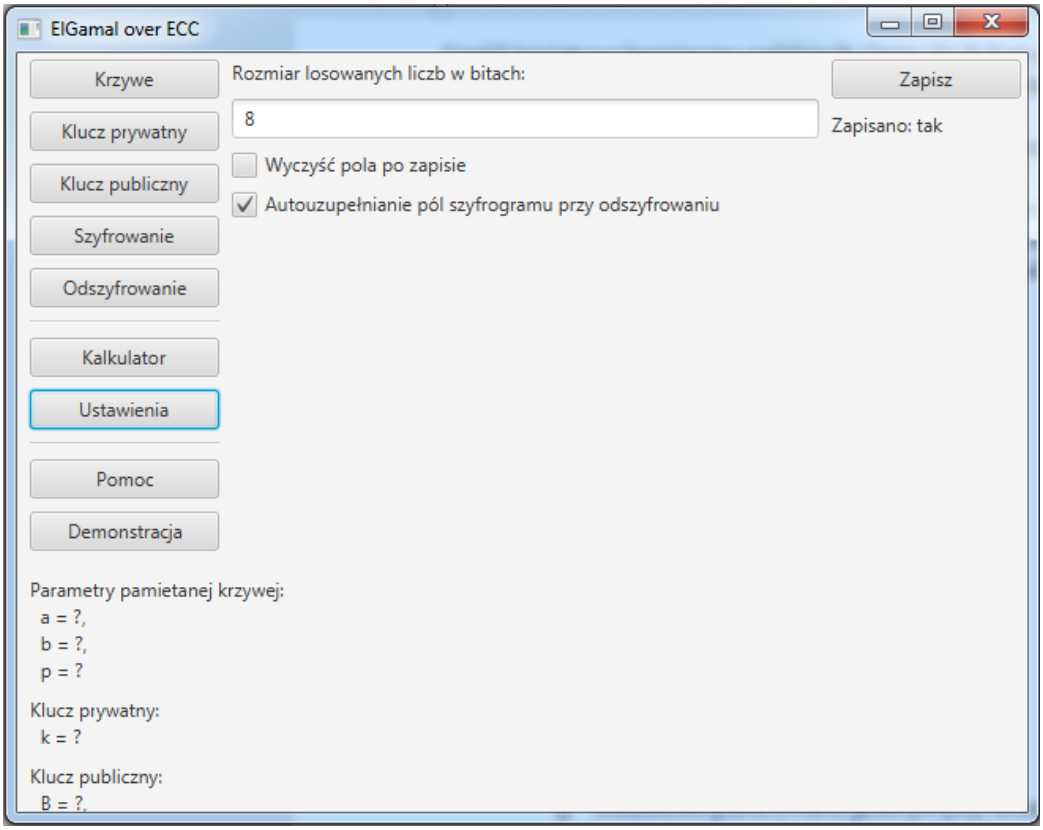
3. **Autouzupełnianie pól szyfrogramu przy odszyfrowaniu.** Zaznaczenie tej opcji powoduje, że w funkcjonalności z menu głównego *Odszyfruj* pola formularza automatycznie zostaną wypełnione przez wartość szyfrogramu, jeśli w poprzednim kroku taki powstał, przez wywołanie funkcjonalności *Szyfruj* (Rysunek 31). Jest to ułatwienie mające na celu skrócenie czasu związanego z wpisywaniem ręcznie wartości.



Rysunek 29: Ustawienia: zmiana rozmiaru losowanego parametru

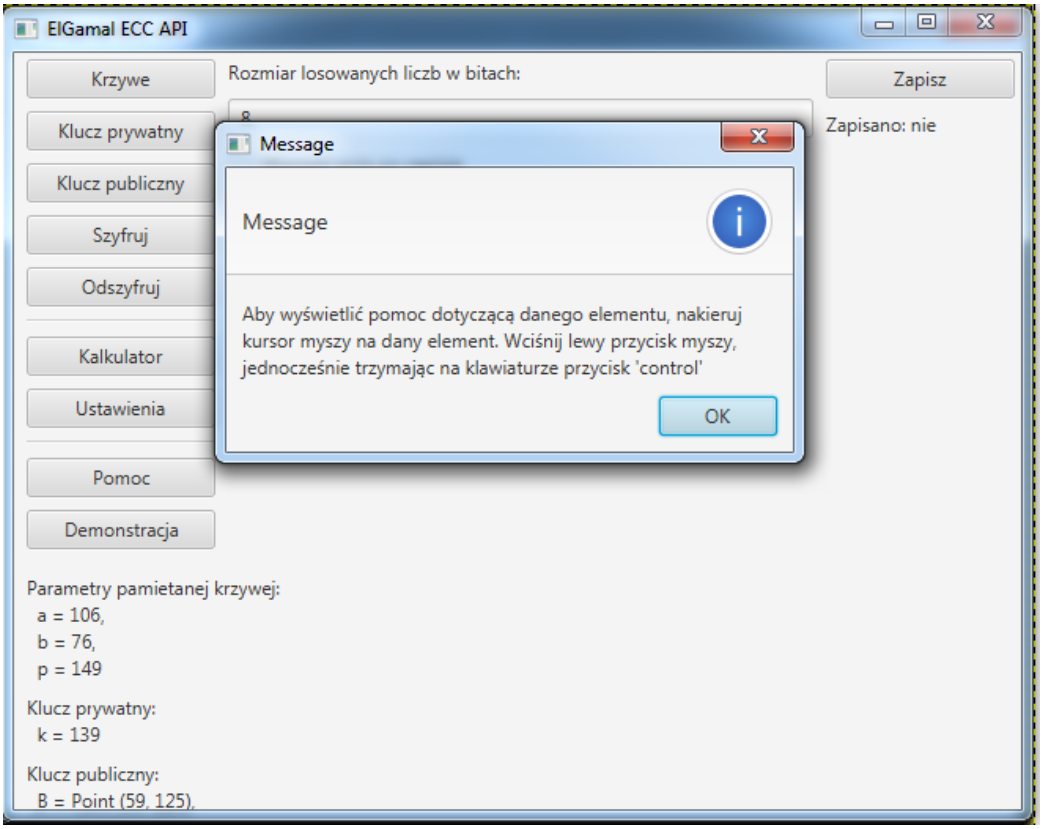


Rysunek 30: Ustawienia: włączanie/wyłączanie czyszczenia pola po zapisie



Rysunek 31: Ustawienia: włączanie/wyłączanie autouzupełniania pola w funkcjonalności odszyfrowanie

Pomoc Pomoc zawiera wskazówki na temat korzystania z programu. Aby z niej skorzystać należy wybrać przycisk z menu głównego *Pomoc* (Rysunek 32).



Rysunek 32: Pomoc

5 Podsumowanie i wnioski

Przedstawiona powyżej praca miała za zadanie przybliżyć zagadnienia teoretyczne związane z krzywymi eliptycznymi. Możemy zaobserwować pewną analogię między tradycyjnym systemem ElGamala, a tym opartym o krzywe eliptyczne. Istota działania kryptosystemu opartego na logarytmie dyskretnym w F_p* polega na tym, aby dla danych liczb g, h oraz p znaleźć liczbę x, która spełni kongruencję

$$h = g^x \,(mod\, p) \tag{40}$$

Innymi słowy chodzi o to, ile razy g musi być pomnożone przez siebie aby otrzymać $h\,(mod\, p)$. Podobny pomysł został zastosowany do otrzymania kryptosystemu opartego na krzywych eliptycznych nad ciałem F_p. Ze zbioru $E(F_p)$ wybieramy dwa punkty P i Q. Istota tego systemu polega na tym aby znaleźć liczbę naturalną taką, by była spełniona równość

$$P + P + P + ... + P = nP = Q \tag{41}$$

Sposób zdefiniowania sumy jest jednak taki, by operacja dodawania w (39) była dużo trudniejsza niż operacja mnożenia modulo w (40). Dzięki temu rozwiązaniu kryptosystemy oparte o krzywe eliptyczne w F_p są dużo bezpieczniejsze niż kryptosystemy oparte o problem logarytmu dyskretnego przy tej samej długości klucza.
Krzywe eliptyczne należą do bardzo efektywnych narzędzi, które są stosowane w ciągu ostatnich lat w systemach kryptograficznych. Wynika to z faktu, że umożliwiają one stosowanie krótszych kluczy kryptograficznych przy zachowaniu takiego samego poziomu bezpieczeństwa danych jak w tradycyjnych systemach. Kryptosystemy oparte o krzywe eliptyczne są dzięki temu bardzo szybkie w działaniu i konsumują mniejszą ilość pamięci. Jest to szczególnie istotne, zwłaszcza w systemach o ograniczonych zasobach, takich jak systemy radiokomunikacji ruchomej, sieci sensorowe, karty elektroniczne czy systemy wbudowane. Kryptografia oparta o krzywe eliptyczne jest łatwa w implementacji, nawet przy użyciu programowalnych układów FPGA (ang. field-programmable gate array). Praca ta potwierdziła przydatność krzywych eliptycznych dla zastosowania w systemach kryptograficznych. Napisany program może być zastosowany z powodzeniem do zajęć dydaktycznych z zakresu kryptografii.
Zarówno praca jak i napisany program komputerowy mogą stanowić podstawę do dalszych badań nad zagadnieniem zastosowania krzywych eliptycznych w kryptografii w takich systemach jak na przykład Masseya-Omury.

6 Bibliografia

Literatura

[1] Blake, I.; Seroussi, G.; Smart. N.: *Krzywe eliptyczne w kryptografii.* Warszawa: WNT, 2004. Pozycja nie cytowana w pracy.

[2] Chrzęszczyk, A.: *Algorytmy teorii liczb i kryptografii w przykładach.* Legionowo: Wydawnictwo BTC, 2010.

[3] Chmielowiec, A.: *Wydajne metody generowania bezpiecznych parametrów algorytmów klucza publicznego, Rozprawa doktorska wykonana pod kierunkiem dr hab. Janusza Szczepańskiego prof. IPPT PAN Instytut Podstawowych Problemów Techniki Polskiej Akademii Nauk* . Warszawa: Instytut Podstawowych Problemów Techniki Polska Akademia Nauk, 2012.

[4] Jost, Ch.; Mattsson, J.; Näslund, M.; and Smeets, B.: *Cryptography in an all encrypted world*. Ericsson Technology Review, 2015. Pozycja nie cytowana w pracy.

[5] Karbowski, M.: *Podstawy kryptografii. Wydanie III*. Gliwice: Helion, 2015. Pozycja nie cytowana w pracy.

[6] Koblitz, N.: *Algebraiczne aspekty kryptografii*. Warszawa: WNT, 2000.

[7] Koblitz, N.: *Wykład z teorii liczb i kryptografii*. Warszawa: WNT, 1995.

[8] Pieprzyk, J.; Hardjono, T.; Seberry J.: *Teoria bezpieczeństwa systemów komputerowych*. Gliwice: Helion, 2005.

[9] Silverman, J. H.: *The Arithmetic of Elliptic Curves*. Springer- Verlag, 1986.

[10] Stallings, W.: *Kryptografia i bezpieczeństwo sieci komputerowych. Matematyka szyfrów i techniki kryptologii*. Gliwice: Helion, 2011. Pozycja nie cytowana w pracy.