|  |  |
| --- | --- |
| **Politechnika Białostocka**  **Wydział Informatyki** | Data: 17.11.2016 |
| **Przedmiot:** Techniki zapewniania poufności w Internecie.  **Sprawozdanie nr:** 4  **Temat:** Krzywe eliptyczne. Podpis cyfrowy i wymiana kluczy.  **Autor:** Maciej Ziniewicz  **Studia:** stacjonarne II stopnia, semestr 2 | **Prowadzący:**  prof. dr hab. Vyacheslav Yarmolik  Ocena: |

Spis treści

[1. Treść zadania 2](#_Toc464143197)

[2. Część teoretyczna 2](#_Toc464143198)

[3. Rozwiązanie 3](#_Toc464143199)

# Treść zadania

1. Zaimplementuj wymianę kluczy w grupie krzywej eliptycznej.
2. Zaimplementuj algorytm podpisu cyfrowego.

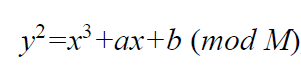
# Część teoretyczna

Do użycia krzywych eliptycznych w kryptografii, na początku należy stworzyć grupy eliptyczne. Do stworzenia takich grup krzywa eliptyczna musi spełniać określone warunki.

Jeżeli mamy dane dwie liczby a i b które są dodatnie, krzywa musi spełniać zależność:



gdzie M jest liczbą pierwszą i dane liczby dodatnie a i b są mniejsze od M (a<M,b<M). Krzywa spełniająca te warunki może być użyta do swtorzenia grup eliptycznych.

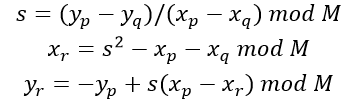
Taka grupa składa się z zestawu par liczb dodatnich (x,y) mniejszych od M, spełniających równanie:

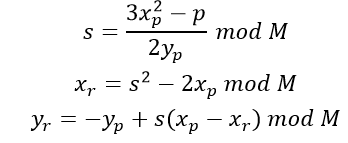
Jeżeli dwie liczby dodatnie (x,y) o wartośćiach od (0,0) do (M-1,M-1) spełniają powyższe równanie, mogą zostać użyte jako elementy(punkty) grupy eliptycznej. Aby wygenerować wszystkie punkty dla grupy eliptycznej należy:

* Dla każdej wartości x, 0≤x≤M, obliczyć wartość wyrażenia
* Dla każdej wartości uzyskanej po wykonaniu poprzedniego kroku należy z niej wyliczyć pierwiastek kwadratowy modulo M, którego wynikiem ma być liczba całkowita. Jeżeli nie uzyskamy takiej cyfry oznacza to że punkt nie należy do grupy eliptycznej, natomiast jeżeli uzyskamy taką liczbę to istnieją dwa elementy y w grupie y i –y.

Kolejnym krokiem do użycia krzywych eliptycznych do kryptografi jest obliczenie rzędu punktu aby to zrobić należy wykorzystać dwa podstawowe działania używanych do obliczania punktów.

Dodawanie dwóch punktów oraz :

* Punkty P i Q muszą być różne i P nie może się równać -Q, wtedy obliczamy P+Q=R gdzie współrzędne R są uzyskiwane w operacji dodawania:
* Jeżeli P jest równe –Q czyli Px jest równe Qx i Py=-Qy lub Py=Qy=wynik jest równy θ (punkt w nieskończoności)

W przypadku niespełnienia powyższych warunków(punkty nie są różne) wykonywania jest operacja podwajania punktu P+P=R:

 Aby określić generację punktu i jego rząd należy sprawdzić która jego wielokrotność jest punktem nieskończoności, numer tej wielokrotności będzie rzędem punktu, a wielokrotności czyli punkty obliczane w wyniku powyższych działań arytmetycznych stanowią generację punktu. Matematycznie rząd punktu wyrażony jest to wzorem:

Gdzie δ(delta) oznacza pierwszą wielokrotność P a kolejna oznaczona jest przez ß(beta). Obie wielokrotności spełniają warunek równości δP=ßP gdzie ß> δ wtedy rząd stanowi róznice

# Rozwiązanie

