|  |  |
| --- | --- |
| **Politechnika Białostocka**  **Wydział Informatyki** | Data: 17.11.2016 |
| **Przedmiot:** Techniki zapewniania poufności w Internecie.  **Sprawozdanie nr:** 5  **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 wymiany kluczy potrzebna jest poprzednia część zadania a konkretnie liczba pierwsza M oraz paramtery a i b, stworzona grupa eliptyczna (a,b) , oraz wybrany punkt generujący G oraz jego rząd c. Grupa eliptyczna i punkt generujący wraz z rzędem jest dostępny publicznie.

Przy wymianie kluczy mamy dwóch użytkownikó A i B.

* Użytkownik A wybiera liczbę taką że <c, liczba ta jest kluczem prywatnym użytkownika A, następnie użytkownik a generuje klucz publiczny(punkt) Pa = .
* Użytkownik B wykonuje te same czynności wybierając i generując Pb
* Następnie użytkownik A wysyła swój klucz publiczny Pa użytkownikowi B, użytkownik B wysyła klucz publiczny Pb użytkownikowi A.
* Użytkownik A generuje klucz prywatny(punkt) używając klucza publicznego użytkownika B oraz swojego wybranego klucza prywatnego K=
* Użytkownik B generuje klucz prywatny(punkt) używając klucza publicznego użytkownika A oraz swojego wybranego klucza prywatnego K=

# Rozwiązanie









