|  |  |
| --- | --- |
| Vitali Karpinski  Robert Zagórski | prowadzący: mgr inż. Mariusz Sepczuk semestr: 14L (2013/2014) |

**Protokół DH na krzywej eliptycznej nad ciałem binarnym**

Zadanie projektowe polega na stworzeniu aplikacji, która pozwoli użytkownikom wygenerować wspólny klucz sesji z wykorzystaniem algorytmu ECDH.

Przed rozpoczęciem działania algorytmu muszą być zdefiniowane pewne stałe niezbędne w celu jego realizacji. Przede wszystkim użytkownik aplikacji powinien podać parametry krzywej eliptycznej oraz zdefiniować ciało binarne. Krzywa eliptyczna wykorzystywana do realizacji ECDH nad ciałem binarnym jest opisana następującym równaniem[1]:

, gdzie *b ≠ 0*

Użytkownik powinien podać wartość parametrów *a* i *b* oraz parametru *m*. Parametr *m* definiuje ciało binarne F2m. Ciało F2m zawiera *2m* elementów, każdy z których jest ciągiem bitów o długości *m*. Parametry *a* i *b* są elementami ciała F2m.

Innymi parametrami potrzebnymi do zaimplementowania algorytmu ECDH są: *G (gx, gy),* *n* oraz *h*.

*G* – generator grupy punktów na krzywej. Jest to losowo wybrany punkt na krzywej eliptycznej.

*n* – rząd punktu *G*, *n* jest dużą liczbą pierwszą.

*h* – liczba warstw podgrupy, czyli liczba punktów na krzywej eliptycznej jest równa *h·n*.

Pierwszym krokiem wygenerowania wspólnego klucza sesji jest generacja kluczy prywatnych[2]. Kluczem prywatnym *d* jest liczba pierwsza wybrana losowo z zakresu [1, *n*-1]. Następnie muszą być stworzone klucze publiczne, które będą wymieniane między uczestnikami sesji. Klucz publiczny jest obliczany jako iloczyn klucza prywatnego oraz punktu *G, Q = [d]G*. Operacja iloczynu punktu na krzywej eliptycznej jest definiowana jako suma punktu *G* z samym sobą *d* razy. Każdy z uczestników sesji ma własny klucz prywatny i publiczny.

Kolejnym krokiem następuje wymiana kluczy publicznych między uczestnikami sesji.

Ostatecznie każdy uczestnik oblicza wartość wspólnego tajnego klucza. Jeżeli nazwiemy uczestników sesji A i B, to wartość tajnego klucza jest obliczana jako *dAQB = dBQA*. Warunkiem poprawności algorytmu, jest równość niezależnie obliczonych kluczy publicznych.

Bibliografia:

1. Blake, I., Seroussi, G., Smart, N., *Krzywe eliptyczne w kryptografii*, WNT,   
   Warszawa, 2004
2. Andrzej Chmielowiec, *Wydajne metody generowania bezpiecznych parametrów algorytmów klucza publicznego*, Instytut Podstawowych Problemów Techniki PAN, Warszawa, 2012