

WYDZIAŁ INFORMATYKI

Katedra Systemów Informacyjnych i Sieci Komputerowych

**Techniki Zapewniania Poufności w Internecie**

Kryptografia krzywych eliptycznych

Arkadiusz Rutkowski

20.04.2013 r

*prof. dr hab. Vyacheslav Yarmolik*

***Opis zadania***

Zaimplementuj system kryptograficzny bazujący na krzywych eliptycznych:

1. Generowanie wszystkich punktów krzywej eliptycznej dla podanych parametrów.
2. Dokonaj wymiany klucza.
3. Szyfrowanie oraz deszyfrowanie punktów przy pomocy kluczy z poprzedniego zadania.

***Teoria***

Równanie krzywej eliptycznej:

Wymiana kluczy:

1. Użytkownik *A* generuje klucz prywatny *nA < M* oraz na jego podstawie klucz publiczny *PA* = *nAG* gdzie *G* jest ustalonym punktem transmisji. Podobnie postępuje użytkownik *B*.
2. Użytkownik *A* na podstawie klucza publicznego użytkownika *B* wylicza *K* = *nAPB* oraz użytkownik *B* wylicza *K* = *nBPA*.

Szyfrowanie:

1. Ustalana jest wiadomość *Pm = (xP, yP)*.
2. Użytkownik *A* generuje liczbę *k*, gdzie *k < c*.
3. Użytkownik *A* wysyła dwa punkty *Cm* = (*kG, Pm* + *kPB*).

Deszyfrowanie:

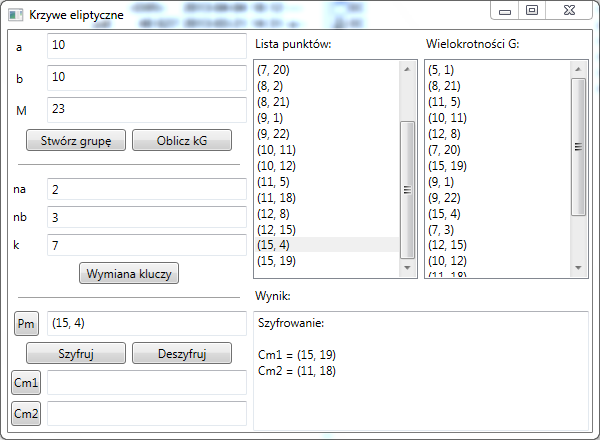
1. Użytkownik *B* oblicza *Pk* = *nBkG.*
2. Użytkownik *B* wykonuje *Pm* = (*Pm* + *kPB − Pk*).

***Użyta technologia***

* Język C# oraz .NET Framework 4.5
* Środowisko Visual Studio 2012 Premium

***Instrukcja obsługi***

Interfejs graficzny aplikacji:



Generowanie krzywej eliptycznej:

1. Najpierw ustalamy parametry krzywej (*a, b, M*) i klikamy przycisk *„Stwórz grupę”*.
2. Wybieramy punkt transmisyjny *G* z listy punktów i wciskamy *„Oblicz kG”*.

Wymiana kluczy:

1. Wprowadzamy *nA*, *nB* (muszą być mniejsze od *M*).
2. Następnie podajemy *k* (mniejsze od *c*, czyli liczby wielokrotności *G*).
3. Wciskamy *„Wymiana kluczy”*,

Szyfrowanie:

1. Wybieramy punkt z listy i wciskamy *Pm*, a następnie *„Szyfrowanie”*.
2. Wybieramy kolejno 2 punkty z listy i wciskamy *Cm1* oraz *Cm2*, a następnie *„Deszyfrowanie”*.