Ciało binarne , gdzie , n- duże mniejsze niż 200

Krzywa eliptyczna w notacji afinicznej nad ciałem charakterystyki dwa ( ):  
 , gdzie:  
(grupa multiplikatywna dla ciała ),   
ustalony element , dla którego (przyjmuje wartości 0 lub 1)

Dodawanie punktów na krzywej:

Niech   
𝒪 oraz   
Suma :

1. (podwajanie punktu:), to

Obliczanie wielokrotności punktu: (strony 72-91 *„Krzywe eliptyczne w kryptografii”*):

1. Metoda binarna
2. Metoda m-arna
3. Metoda przesuwających się okienek oparta na znakowanym rozwinięciu m-arnym

Zastosować Rozwinięcie Frobeniusa (?)

Protokół wymiany klucza metodą Diffiego-Hellmana zakłada, że strony A

i B mają uzgodnioną pewną publicznie znaną grupę cykliczną G, która spełnia

następujące warunki:

1. ,

2. ,

3. rozwiązanie równania jest obliczeniowo trudne,

4. istnieje funkcja KDFG : , która pozwala przekształcić dowolny element grupy w ciąg bitów o zadanej długości.

Aby uzgodnić klucz sesyjny strony A i B realizują następujący protokół.

1. Strona A wybiera losową liczbę całkowitą i przesyła stronie B element

.

2. Strona B wybiera losową liczbę całkowitą i przesyła stronie A element

.

3. Strona A po otrzymaniu elementu hB wyznacza element

i oblicza wspólny klucz .

4. Strona B po otrzymaniu elementu hA wyznacza element

i oblicza wspólny klucz .

Podczas realizacji protokołu Diffiego-Hellmana w kanale publicznym pojawiają się jedynie takie wartości, jak . Aby złamać protokół należałoby wyznaczyć wartość:

Czy należy generować własną krzywą eliptyczną (i sprawdzać ją z procedurą sprawdzania zawartą w normie ANSI X9.62) czy zaimplementować krzywą uznawaną za bezpieczną (np.: Curve B-163 z *„The Elliptic Curve Digital Signature Algorithm (ECDSA)”*)?

Czy wygenerować generator grupy G, czy wziąć gotowy? (ECDSA-cert 5.3)