3. Protokół Diffie-Hellmana w grupie E_k

(E_k, P)- inicjalizacja + q- rząd E_k

Ustalamy P є E_k (publiczny), dużego rzędu

A generuje losowe a<q B generuje nosowość b<q

1. A oblicza i wysyła do B wartość aP
2. B oblicza i wysyła do A wartość Bp
3. Klucz wymuszony, bo K_{AB}= abP obliczam dla A:a*Bp dla B: b*aP

Założenie:

Problem, Diffie-Helmana: znając aP i bP nie możemy znaleźć abP (trudno obliczeniowe)

Zatem, E_5: $y^2-(x^3-x)=0$

G_5={Θ,(0,0),(1,0),(2,1),(2,4),(3,3),(3,2),(4,0)}

P=(2,1) A-losuje a=2 B- losuje b=2

Obliczyć aP, Bp, abp

$$\lambda = \frac{3*4-1}{2} = \frac{11}{2} = \frac{1}{2} = 2^{-1} = 3$$

$$x_3 = 3^2 - 2*2 = 0$$

$$y_3 = 3(2-0) - 1 = 0$$

aP= 2*(2,1)=(0,0)

bP= 2*(2,1)=(0,0)

abp= a*bP= 2*(0,0)= Θ

to samo dla a=2 b=4 aP=(0,0)

bP= 4*(2,1)= 2*(2*(2,1))= Θ

przeciwny do (2,1) czyli (x,y)+(2,1)= Θ

odwrotny do (2,1) jest (2,4) $\lambda = \frac{y_2 - y_1}{x_2 - x_1} = \frac{3}{0}$

E_7: $y^2-(x^3-x)=0(\mathrm{mod}7)$

$G_7=\{\Theta,(0,0),(1,0),(4,2),(4,4),(5,1),(5,6),(6,0)\}$

P=(5,1) A-losuje a=2 B- losuje b=2

λ =2

x_3=1

y_3=0

2P=(1,0) czyli 4P=Θ