POLITECHNIKA BIAŁOSTOCKA
WYDZIAŁ INFORMATYKI
Techniki zapewniania poufności w internecie

PRACOWNIA SPECJALISTYCZNA 10-11
MGR INŻ. MACIEJ BRZOZOWSKI

TEMAT: KRYPTOGRAFIA KRZYWYCH ELIPTYCZNYCH.

$$y^2 = x^3 - px - q \; mod \; M$$
$$\Delta_E = 4p^3 + 27q^2 \; mod \; M \neq 0$$
$$P = (x_P, y_P), Q = (x_Q, y_Q)$$
$$P + \theta = P$$

Dodawanie punktów $R = P + Q = (x_R, y_R)$:

1. jeżeli $x_P \neq x_Q$

$$s = \frac{y_P - y_Q}{x_P - x_Q} mod \; M$$
$$x_R = s^2 - x_P - x_Q \; mod \; M, y_R = y_P + s(x_R - x_P) \; mod \; M$$

2. jeżeli $x_P = x_Q$

   (a) jeżeli $y_P = -y_Q$ lub $y_P = y_Q = 0$ wynik równy θ (punkt neutralny bądź w nieskończoności w zależności od tłumaczenia)

   (b) jeżeli $y_P = y_Q \neq 0 \; R = P + P = 2P = (x_R, -y_R)$ (podwajanie punktu)

$$s = \frac{3x_P^2 - p}{2y_P} \; mod \; M$$
$$x_R = s^2 - 2x_P, y_R = y_P + s(x_R - x_P) \; mod \; M$$

Wymiana kluczy:

1. Użytkownik A generuje klucz prywatny $n_A < M$ oraz na jego podstawie klucz publiczny $P_A = n_A G$ gdzie G jest ustalonym punktem transmisji. Podobnie postępuje użytkownik B.

2. Użytkownik A na podstawie klucza publicznego użytkownika B wylicza $K = n_A P_B$ oraz użytkownik B wylicza $K = n_B P_A$.

Szyfrowanie wiadomości $P_m = (x, y)$

1. Użytkownik A generuje liczbę k
2. Użytkownik A wysyła dwa punkty $C_m = (kG, P_m + kP_B)$

Deszyfrowanie wiadomości:

1. Użytkownik B oblicza $P_k = n_B kG$
2. Użytkownik B wykonuje $P_m = (P_m + kP_B - P_k)$

Zadanie: Zaimplementuj system kryptograficzny bazujący na krzywych eliptycznych:

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