8.2. Аналог алгоритма Диффи-Хеллмана обмена ключами

Обмен ключами с использованием *эллиптических кривых* может быть выполнен следующим образом. Сначала выбирается простое число $p \approx 2^{180}$ и параметры a и b для уравнения *эллиптической кривой*. Это задает множество точек E_p (a,b). Затем в E_p (a,b) выбирается генерирующая точка $G = (x_1,y_1)$. При выборе G важно, чтобы наименьшее значение n, при котором $n \times G = 0$, оказалось очень большим простым числом. Параметры E_p (a,b) и G криптосистемы являются параметрами, известными всем участникам.

Обмен ключами между пользователями A и B производится по следующей схеме.

1. Участник A выбирает целое число n_A, меньшее n. Это число является закрытым ключом участника A. Затем участник A вычисляет открытый ключ $P_A = n_A \times G$, который представляет собой некоторую точку на E_p (a,b).
2. Точно так же участник B выбирает закрытый ключ n_B и вычисляет открытый ключ P_B.
3. Участники обмениваются открытыми ключами, после чего вычисляют общий секретный ключ K

   Участник A: $K = n_A \times P_B$

   Участник B: $K = n_B \times P_A$

Следует заметить, что общий секретный ключ представляет собой пару чисел. Если данный ключ предполагается использовать в качестве сеансового ключа для алгоритма симметричного шифрования, то из этой пары необходимо создать одно значение.