8.4. Шифрование/дешифрование с использованием эллиптических кривых

Рассмотрим самый простой подход к шифрованию/дешифрованию с использованием *эллиптических кривых*. Задача состоит в том, чтобы зашифровать сообщение M, которое может быть представлено в виде точки на эллиптической кривой P_m (x,y).

Как и в случае обмена ключом, в системе шифрования/дешифрования в качестве параметров рассматривается *эллиптическая кривая* E_p (a,b) и точка G на ней. Участник B выбирает закрытый ключ n_B и вычисляет открытый ключ $P_B = n_B \times G$. Чтобы зашифровать сообщение P_m используется открытый ключ получателя B P_B. Участник A выбирает случайное целое положительное число k и вычисляет зашифрованное сообщение C_m, являющееся точкой на *эллиптической кривой*.

$$C_m = \{k \times G, P_m + k \times P_B\}$$

Чтобы дешифровать сообщение, участник B умножает первую координату точки на свой закрытый ключ и вычитает результат из второй координаты:

$$P_m + k \times P_B - n_B \times (k \times G) = P_m + k \times (n_B \times G) - n_B \times (k \times G) = P_m$$

Участник A зашифровал сообщение P_m добавлением к нему kxP_B. Никто не знает значения k, поэтому, хотя P_B и является открытым ключом, никто не знает $k \times P_B$. Противнику для восстановления сообщения придется вычислить k, зная G и $k \times G$. Сделать это будет нелегко.

Получатель также не знает k, но ему в качестве подсказки посылается $k \times G$. Умножив $k \times G$ на свой закрытый ключ, получатель получит значение, которое было добавлено отправителем к незашифрованному сообщению. Тем самым получатель, не зная k, но имея свой закрытый ключ, может восстановить незашифрованное сообщение.