Лабораторная работа №7
«Криптография с использованием эллиптических кривых»

1. Цель работы:

Изучение алгоритмов ассиметричного шифрования данных с использованием эллиптических кривых.

2. Основные теоретические сведения:

Эллиптическая группа по модулю p обозначается через $E_p(a, b)$, где $4a^3+27b^2 (\text{mod } p) \neq 0$. Элементами эллиптической группы являются пары неотрицательных целых чисел (x, y), которые меньше p и удовлетворяют условию

$$y^2 \equiv x^3 + ax + b \ (\text{mod } p) \qquad (1)$$

вместе с точкой в бесконечности O.

Правила для сложения в $E_p(a, b)$ соответствуют геометрическим приемам (см. лекции). Формально эти приемы для всех точек $E_p(a, b)$ могут быть записаны следующим образом:

1. $P + O = P$.
2. Если $P = (x, y)$, *то* $P + (x, -y) = O$. Точка $(x, -y)$ является отрицательным значением точки P и обозначается $-P$.
3. Если $P = (x_1, y_1)$ и $Q = (x_2, y_2)$, то $P + Q = (x_3, y_3)$ определяется в соответствии с правилами

$$x_3 \equiv \lambda^2 - x_1 - x_2 (\text{mod } p)$$
$$y3 \equiv \lambda(x_1 - x_3) - y_1 (\text{mod } p)$$

где

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1}, \text{ если } P \neq Q \\ \dfrac{3x_1^2 + a}{2y_1}, \text{ если } P = Q \end{cases}$$

Рассмотрим два примера. Пусть $P = (3, 10)$ и $Q = (9, 7)$. Тогда

$$\lambda = \frac{7-10}{9-3} = \frac{-3}{6} = \frac{-1}{2} \equiv 11 \bmod 23$$
$$x_3 = 11^2 - 3 - 9 = 109 \equiv 17 \bmod 23$$
$$y_3 = 11(3-(-6)) - 10 = 89 \equiv 20 \bmod 23$$

Поэтому $P + Q = (17, 20)$.

Чтобы найти $2P$, найдем

$$\lambda = \frac{3(3^2)+1}{2 \times 10} = \frac{5}{20} = \frac{1}{4} \equiv 6 \bmod 23$$
$$x_3 = 6^2 - 3 - 3 = 30 \equiv 7 \bmod 23$$
$$y_3 = 6(3-7) - 10 = -34 \equiv 12 \bmod 23$$

и поэтому $2P = (7, 12)$.

Эллиптические кривые и криптография

Операция сложения в криптографии на основе эллиптических кривых является аналогом операции умножения по модулю простого числа в RSA, а многократное повторное сложение - аналогом возведения в степень. Чтобы построить криптографическую систему, используя эллиптические кривые, нужно найти "трудную проблему", соответствующую разложению на множители произведения двух простых чисел или дискретному логарифмированию.

Рассмотрим уравнение $Q = kP$, где $Q, P \in E_p(a, b)$ и $k < p$. Относительно легко вычислить Q по данным k и P, но относительно трудно определить k, имея Q и P.

Обмен ключами с использованием эллиптических кривых (аналог обмена по схеме Диффи-Хеллмана)

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 эллиптической кривой в уравнении (1). Это задает эллиптическую группу 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 $nG = O$, 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 можно провести по следующей схеме.

1. Сторона A выбирает целое число n_A, меньшее n. Это число будет личным ключом участника A., Затем участник A генерирует открытый ключ $P_A = n_A \times G$. Открытый ключ представляет собой некоторую точку из $E_p(a, b)$.
2. Точно так же участник B выбирает личный ключ n_B и вычисляет открытый ключ P_B.
3. Участник A генерирует секретный ключ $K = n_A \times P_B$, а участник B генерирует секретный ключ $K = n_B \times P_A$.

Две формулы в п. 3 дают один и тот же результат, поскольку

$$n_A \times P_B = n_A \times (n_B \times G) = n_B \times (n_A \times G) = n_B \times P_A.$$

Чтобы взломать эту схему, противник должен будет вычислить k по данным G и kG, что предполагается трудным делом.

В качестве примера возьмем $E_{211}(0, -4)$ (что соответствует кривой $y^2 = x^3-4$) и $G = (2, 2)$. Можно подсчитать, что

241$G = O$. Личным ключом пользователя А является $n_A = 121$, поэтому открытым ключом А будет $P_A = 121(2, 2) = (115, 48)$. Личным ключом пользователя В является $n_B = 203$, поэтому открытым ключом участника В будет $203(2, 2) = (130, 203)$. Общим секретным ключом является $121(130, 203) = 203(115, 48) = (161, 69)$.

Обратите внимание на то, что общий секретный ключ представляет собой пару чисел. Если этот ключ предполагается использовать в качестве сеансового ключа для традиционного шифрования, то из этой пары чисел необходимо генерировать одно подходящее значение. Можно, например, использовать просто координату x или некоторую простую функцию от x.

Шифрование/дешифрование с использованием эллиптических кривых

В специальной литературе можно найти анализ нескольких подходов к шифрованию/дешифрованию, предполагающих использование эллиптических кривых. Рассмотрим наиболее простой из этих подходов. Здесь точка P_m будет представлять шифрованный текст и впоследствии будет дешифроваться. Обратите внимание, что нельзя закодировать сообщение просто координатой x или y точки, так как не все такие координаты имеются в $E_p(a, b)$. Опять же, существует несколько подходов к кодированию, но мы их рассматривать не будем - для наших целей достаточно просто отметить, что имеются относительно прямые методы, которые могут быть здесь применены.

Как и в случае системы обмена ключами, в системе шифрования/дешифрования в качестве параметров тоже рассматривается точка G и эллиптическая группа $E_p(a, b)$. Пользователь А выбирает личный ключ n_A и генерирует открытый ключ $P_A = n_A \times G$. Чтобы зашифровать и послать сообщение P_m пользователю В, пользователь А выбирает случайное положительное целое число k и вычисляет шифрованный текст C_m состоящий из пары точек

$$C_m = \{kG, P_m + kP_B\}.$$

Заметим, что сторона А использует открытый ключ стороны В: P_B. Чтобы дешифровать этот шифрованный текст, В умножает первую точку в паре на секретный ключ В и вычитает результат из второй точки:

$$P_m + kP_B - n_B(kG) = P_m + k(n_BG) - n_B(kG) = P_m.$$

Пользователь A замаскировал сообщение P_m с помощью добавления к нему kP_B. Никто, кроме этого пользователя, не знает значения k, поэтому, хотя P_B и является открытым ключом, никто не сможет убрать маску kP_B. Однако пользователь А включает в сообщение и "подсказку", которой будет достаточно, чтобы убрать маску тому, кто имеет личный ключ n_B. Противнику для восстановления сообщения придется вычислить k по данным G и kG, что представляется трудной задачей.

В качестве примера подобного шифрования рассмотрим случай $p = 751$, $E_p(-1, 188)$ (что соответствует кривой $y^2 = x^3 - x + 188$) и $G = (0, 376)$. Предположим, что пользователь А собирается отправить пользователю В сообщение, которое кодируется эллиптической точкой $P_m = (562, 201)$, и что пользователь А выбирает случайное число $k = 386$. Открытым ключом В является $P_B = (201, 5)$. Мы имеем $386(0, 376) = (676, 558)$ и $(562, 201) + 386(201, 5) = (385, 328)$. Таким образом, пользователь А должен послать шифрованный текст $\{(676, 558), (385, 328)\}$.

3. Задание на лабораторную работу

1. В эллиптической группе $E_p(a, b)$ (см. таблицу) выбрать любую точку G.
2. Выбрать секретные $n_A>100$ и $n_B>100$.
3. Вычислить открытые P_A и P_B.
4. Вычислить общий ключ K по схеме обмена ключами.
5. Послать шифрованное сообщение P_m=(513, 167) от пользователя В пользователю А.

№ варианта	P	a	b
1	2089	5	889
2	2237	16	871
3	2347	27	853
4	2459	38	835
5	2617	49	817
6	2713	60	799
7	2837	71	781
8	2969	82	763
9	2027	93	745
10	2141	104	727
11	2281	115	709
12	2389	126	691
13	2539	137	673
14	2671	148	655
15	2767	159	637
16	2897	170	619
17	2081	181	601
18	2207	192	582
19	2333	203	565
20	2437	214	547
21	2591	225	529
22	2699	236	511
23	2803	247	493
24	2953	258	475
25	2003	269	457

№ варианта	P	a	b
26	2099	280	439
27	2239	291	421
28	2351	302	403
29	2467	313	385
30	2621	324	367
31	2719	335	349
32	2843	346	331
33	2971	357	313
34	2039	368	295
35	2153	379	277
36	2293	390	259
37	2399	401	241
38	2549	412	223
39	2683	423	205
40	2789	434	187
41	2909	445	169
42	2083	456	151
43	2213	467	133
44	2339	478	115
45	2441	489	97
46	2593	500	79
47	2707	511	61
48	2819	522	43
49	2957	533	25
50	2011	544	7