Лабораторна робота 2.4

КРИПТОГРАФІЧНІ СИСТЕМИ ЯКІ ЗАСНОВАНІ БАЗІ ЕЛІПТИЧНИХ КРИВИХ

Мета: отримати навички у створенні програмної реалізації криптографічної системи яка заснована базі еліптичних кривих.

Основні завдання:

1. Розробити об'єктно-орієнтованою мовою програмування консольний або віконний додаток, що реалізує шифрування та дешифрування вмісту текстового або виконуваного файлу з використанням апарату еліптичних кривих. Програма повинна запитувати ім'я вхідного і вихідного файлів, тип шифру та вхідні параметри для проведення криптографічних перетворень. В якості вхідних параметрів виступають: еліптична крива: p=751; a= -1; b=1; $E_{751}(-1,1)$; $y^2 = x^3-x+1(\text{mod}751)$; генеруюча точка: G = (0, 1).
2. Представити блок структурну схему своєї програмної реалізації.
3. Зробити висновки на підставі проведених теоретичних та практичних досліджень. У висновках слід зазначити, які навички та знання отримано під час виконання завдань.

Основні теоретичні відомості

Криптосистеми на еліптичних кривих відносяться до класу криптосистем із відкритим ключем. Їхня безпека, як правило, заснована на труднощі вирішення задачі дискретного логарифмування в групі точок еліптичної кривої над кінцевим полем. Розглянемо найпростіший підхід до шифрування та дешифрування з використанням еліптичних кривих. Завдання полягає в тому, щоб зашифрувати повідомлення M, яке може бути представлено у вигляді точки на еліптичній кривій $P_M(x;y)$ $P_M(x;y)$.

Як і в разі обміну ключем, в системі шифрування / дешифрування в якості параметрів розглядається еліптична крива $E_p(a,b)$ $E_p(a,b)$ і точка G G на ній. Учасник B вибирає закритий ключ $n_б$ n_B і обчислює відкритий ключ $P_B = n_B \times G$ $P_б = n_б \times G$. Щоб зашифрувати повідомлення P_M $P_M(x;y)$ використовується відкритий ключ одержувача B – $P_б$ P_B. Учасник A вибирає

випадкове ціле позитивне число k k і обчислює зашифроване повідомлення C_M C_M, що є точкою на еліптичній кривій:

$$C_M = \{k \cdot G; P_M + k \cdot P_B\}$$

Щоб дешифрувати повідомлення, учасник *B* примножує першу координату точки на свій закритий ключ і віднімає результат з другої координати:

$$P_M + kP_B - n_B(kG) = P_M + k(n_B G) - n_B(kG) = P_M$$

Учасник *A* зашифрував повідомлення P_M P_M додаванням до нього kP_B kP_B. Ніхто не знає значення k k, тому, хоча P_B P_B і є відкритим ключем, ніхто не знає kP_B kP_B. Противнику для відновлення повідомлення доведеться обчислити k k, знаючи G G і kG kG. Зробити це буде нелегко.

Одержувач також не знає k k але йому в якості підказки надсилається kG kG. Помноживши kG kG на свій закритий ключ, одержувач отримає значення, яке було додано відправником до незашифрованого повідомлення. Тим самим одержувач, не знаючи k k, але маючи свій закритий ключ, може відновити незашифроване повідомлення [21].

Шифр Ель-Гамаля на еліптичній кривій. Для користувачів вибираються загальна еліптична крива $E_p(a,b)$ $E_p(a,b)$ і точка G G на ній такі, що $G,2G,3G,...,qG$ $G, 2G, 3G, \ldots, qG$ – різні точки і $q \times G = 0$ $q \times G = 0$ для деякого простого числа q q. Кожен користувач мережі вибирає число k, $0 < k < q$ $k, 0 < k < q$, яке зберігає як свій секретний ключ, і обчислює точку на кривій $Y = kG$ $Y = kG$, яка буде його відкритим ключем. Параметри кривої і список відкритих ключів передаються всім користувачам мережі.

Припустимо, користувач *A* хоче передати повідомлення користувачу *B*. Будемо вважати, що повідомлення представлено у вигляді числа $M < p$ $M < p$.

Користувач А виконує наступні дії:

1. вибирає випадкове число r, $0 < r < q$ $r, 0 < r < q$;
2. обчислює $R = rG$, $P = rY_b = (x; y)$ $R = rG$ $P = rY_b = (x; y)$;
3. зашифровує $C = (Mx) \bmod p$ $C = (Mx) mod\ p$;
4. посилає користувачеві *B* шифртекст (R, C) (R, C).

Користувач *B*, після отримання (R, C) (R, C) виконує наступні дії:

1. обчислює $Q = Rk_b = (x; y)$ $Q = Rk_b = (x; y)$;
2. розшифровує $M = (Cx^{-1}) \bmod p$ $M = (Cx^{-1}) mod\ p$.

Для обгрунтування протоколу достатньо показати, що $k_b R = k_b (rG) = r(k_b G) = rY_b$ $k_b R = k_b (rG) = r(k_b G) = rY_b$, тобто $Q = P$ $Q = P$.

Координата x x точки Q Q залишається секретною для криптоаналітика, так як він не знає числа r r. Криптоаналітик може спробувати обчислити r r з точки P P, але для цього йому потрібно вирішити проблему дискретного логарифмування на кривій, що вважається складним завданням. Найбільш імовірним варіантом використання розглянутого алгоритму буде передача в якості числа M M секретного ключа для блочного або поточного шифру. В цьому випадку краще вибирати параметри кривої так, щоб $\log q$ $\log q$ приблизно вдвічі перевищував довжину ключа шифру.

Запитання для самоперевірки

1. Поясність основні напрями використання криптографічних

систем, які засновані на базі еліптичних кривих.

2. Що таке еліптична крива?

3. Поясніть основні етапи проведення процедури шифрування з використанням еліптичних криптосистем.

4. Охарактеризуйте переваги та недоліки використання еліптичних криптосистем.

5. Перелічіть відкриті та закриті параметри еліптичної кривої при здійсненні шифрування та дешифрування.