**Лабораторная работа №3**
**«Задачи дискретного логарифмирования»**

**Цели**: Научиться шифровать сообщения по алгоритмам: Диффи-Хелмана и Эль-Гамаля.

## ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

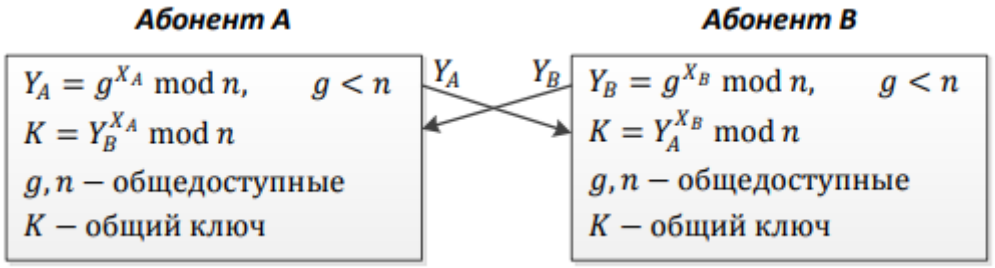
### Алгоритм обмена ключами по схеме Диффи-Хеллмана

В 1976 году была опубликована работа молодых американских математиков У. Диффи и М.Э. Хеллмана «Новые направления в криптографии». В ней они предложили конкретную конструкцию так называемого «открытого распределения ключей» [2, 3].

Цель алгоритма состоит в том, чтобы два участника могли безопасно обменяться ключом, который в дальнейшем может использоваться в каком-либо алгоритме симметричного шифрования. Сам алгоритм Диффи-Хеллмана может применяться только для обмена ключами. Алгоритм основан на трудности вычислений дискретных логарифмов.

Безопасность обмена ключами в алгоритме Диффи-Хеллмана вытекает из того факта, что, хотя относительно легко вычислить экспоненты по модулю простого числа, но очень трудно вычислить дискретные логарифмы. Для больших простых чисел задача считается неразрешимой.

Предположим, что двум абонентам необходимо провести конфиденциальную переписку, а в их распоряжении нет первоначально оговоренного секретного ключа. Однако между ними существует канал, защищённый от модификации, т.е. данные, передаваемые по нему, могут быть прослушаны, но не изменены (такие условия имеют место довольно часто). В этом случае две стороны могут создать одинаковый секретный ключ, ни разу не передав его по сети, по следующему алгоритму:




*Алгоритм заключается в следующем:*

1. Задаются глобальные открытые элементы:
    1) n – случайное большое простое число;
    2) $g$ – первообразный корень n.
2. Вычисляется ключ абонентом $A$:
    1) выбирается большое секретное число $X_A$ ($X_A <$ n);
    2) вычисление открытого значения $Y_A$: $Y_A = g^{X_A} \ mod \ n.$
3. Вычисляется ключ абонентом $B$:
    1) выбирается большое секретное число $X_B$ ($X_B <$ n);
    2) вычисление открытого значения $Y_B$ : $Y_B = g^{X_B} \ mod \ n.$
4. Вычисляется секретный ключ абонентом $A$: $K = Y_B^{X_A} \ mod \ n.$
5. Вычисляется секретный ключ абонентом $B$: $K = Y_A^{X_B} \ mod \ n.$

Необходимо ещё раз отметить, что алгоритм Диффи-Хеллмана работает только на линиях связи, надёжно защищённых от модификации. Если бы он был применим на любых открытых каналах, то давно снял бы проблему распространения ключей и, возможно, заменил бы собой всю асимметричную криптографию

**Пример.** Пусть и n = 97 и $g$ = 5. Абонент $A$ сгенерировал случайное число $X_A$ = 36. Абонент $B$ сгенерировал случайное число $X_B$ = 58. Эти элементы они держат в секрете. Далее каждый из них вычисляет новый элемент:

$$Y_A = 5^{36} \ mod 97 = 50, \qquad Y_B = 5^{58} \ mod 97 = 44.$$

Затем они обмениваются этими элементами по каналу связи. Теперь абонент $A$, получив $Y_{\text{B}}$ и зная свой секретный элемент $X_{\text{A}}$, вычисляет общий ключ: $K_A = 44^{36} \ mod 97 = 75$. Аналогично поступает абонент $B$: $K_B = 50^{58} \ mod 97 = 75$.

**Алгоритм шифрования Эль – Гамаля**

Генерация ключей:

1. Генерируется случайное простое число p.

2. Выбирается целое число $g$ - первообразный корень p.

3. Выбирается случайное целое число x такое, что 1 < x < p .

4. Вычисляется $y = g^x \ mod \ p$.

5. Открытым ключом является тройка (p, g, y), закрытым ключом - число x.

*Шифрование:*

Сообщение M должно быть меньше числа P. Сообщение шифруется следующим образом:

Выбирается сессионный ключ - случайное целое число k такое, что 1 < k < p-1.

Вычисляются числа $a = g^k \ mod \ p$ и $b = y^k M \ mod \ p$.

Пара чисел (a, b) является шифротекстом.

Нетрудно видеть, что длина шифротекста в схеме Эль-Гамаля длиннее исходного сообщения M вдвое.

*Расшифровывание:*

Зная закрытый ключ x, исходное сообщение можно вычислить из шифротекста (a, b) по формуле:

$$M = \frac{b}{a^x} \ mod \ p.$$

При этом нетрудно проверить, что $\frac{1}{a^x} \equiv \frac{1}{g^{kx}} \ mod\, p$ и поэтому $\frac{b}{a^x} \equiv \frac{y^k M}{g^{kx}} = \frac{g^{kx} M}{g^{kx}} \equiv \mathrm{M} \ mod\, p.$

Для практических вычислений больше подходит следующая формула: $M = \frac{b}{a^x} \ mod\, p = ba^{(p-1-x)} \ mod\, p.$

**Пример:**

*Шифрование*

Допустим, что нужно зашифровать сообщение M **=** 5.

Произведем генерацию ключей: Пусть p = 11, $g = 2$. Выберем x **=** 8 - случайное целое число x такое, что 1**<** x **<** p .

Вычислим $y = g^x mod\, p = 2^8 \ mod\, 11 = 3.$

Итак, открытым ключом является тройка ( p,g, y ) = (11, 2, 3), а закрытым ключом - число x **=** 8.

Выбираем случайное целое число k такое, что 1 < k < (p-1). Пусть k **=** 9.

Вычисляем число $a = g^k \ mod\, p = 2^9 \ mod\, 11 = 512 \ mod\, 11 = 6.$

Вычисляем число $b = y^k M \ mod\, p = 3^9 5 \ mod\, 11 = 19683 * 5 \ mod\, 11 = 9.$ Полученная пара (a, b) = (6, 9) является шифротекстом.

*Расшифрование*

Необходимо получить сообщение M **=** 5 по известному шифротексту (a, b) = (6, 9) и закрытому ключу x **=** 8.

Вычисляем M по формуле: $M = \frac{b}{a^x} \ mod\, p = \frac{9}{6^8} \ mod\, 11 = 5.$

Получили исходное сообщение M **=** 5.

Так как в схему Эль-Гамаля вводится случайная величина k, то шифр Эль-Гамаля можно назвать шифром многозначной замены. Из-за случайности выбора числа k такую схему еще называют схемой вероятностного шифрования. Вероятностный характер шифрования является преимуществом для схемы ЭльГамаля, так как у схем вероятностного шифрования

наблюдается большая стойкость по сравнению со схемами с определенным процессом шифрования. Недостатком схемы шифрования Эль-Гамаля является удвоение длины зашифрованного текста по сравнению с начальным текстом. Для схемы вероятностного шифрования само сообщение M и ключ не определяют шифротекст однозначно. В схеме Эль-Гамаля необходимо использовать различные значения случайной величины для шифровки различных сообщений M и M’. Если использовать одинаковые k, то для соответствующих шифротекстов (a, b) и (a', b') выполняется соотношение $\frac{b}{b'} = \frac{M}{M'}$. Из этого выражения можно легко вычислить M ', если известно M.

## ПРАКТИЧЕСКАЯ ЧАСТЬ

**Задание 1:** Разбиться на пары. Выбрать числа n и $g$ согласно алгоритму Диффи-Хеллмана. Вычислить открытые и закрытые ключи, произвести обмен, далее вычислить переданные ключи, после проверить правильность расчёта друг друга.

**Задание 2:** Зашифровать и расшифровать сообщение t = 174 с помощью схемы шифрования Эль Гамаля. Даны простое число p = 659 и число g = 409. Секретный ключ X и случайное число K требуется выбрать исходя из таблицы:

| № | X | K |
|---|---|---|
| **1** | 5 | 11 |
| **2** | 8 | 10 |
| **3** | 9 | 5 |
| **4** | 6 | 9 |
| **5** | 3 | 6 |

**Задание 3:** Зашифровать сообщение, согласно своему варианту, при помощи алгоритма Эль-Гамаля. Числа p, $g$, x и k выбрать самостоятельно.

| № Варианта | Исходный текст |
|---|---|
| 1. | Шумит дубравушка к непогодушке |
| 2. | Утром вороны каркают к дождю |

| | |
|---|---|
| 3. | Сорока на хвосте принесла |
| 4. | Снег холодный, а от мороза укрывает |
| 5. | Сирень или берёза, а всё дерево |
| 6. | Сегодня не тает, а завтра кто знает |
| 7. | Розы без шипов не бывает |
| 8. | Не высок лесок, а от ветра защищает |
| 9. | На всех и солнышко не светит |
| 10. | Красна ягодка, да на вкус горька |
| 11. | В осеннее ненастье семь погод на дворе |
| 12. | Ветром ветра не смеряешь |
| 13. | Пропущенный час годом не нагонишь |
| 14. | Счастливые часов не наблюдают |
| 15. | Друг неиспытанный, как орех не расколотый |
| 16. | Дружи с теми, кто лучше тебя самого |
| 17. | Крепкую дружбу и топором не разрубишь |
| 18. | Кто друг прямой, тот брат родной |
| 19. | лучше выслушать упрёки друга, чем потерять его |
| 20. | Одна пчела много мёду не принесёт |
| 21. | С тем не ужиться, кто любит браниться |
| 22. | Старый друг лучше новых двух |
| 23. | На чужой сторонушке рад родной воробушке |
| 24. | Народы нашей страны дружбой сильны |
| 25. | Поднявший меч от меча и погибнет |
| 26. | При солнце тепло, при Родине добро |
| 27. | Старая слава новую любит |
| 28. | Любишь кататься - люби и саночки возить |
| 29. | Кто пахать не ленится, у того хлеб родится |
| 30. | На печи не храбрись, а в поле не трусь |

**Задание 4:** Найти функцию Эйлера $\varphi(288)$, $\varphi(100)$, $\varphi(3125)$, $\varphi(97)$