Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
Поволжский государственный университет телекоммуникаций и информатики

Кафедра ИБ

Методические указания и контрольные задания по дисциплине

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ИНФОКОММУНИКАЦИОННЫХ СЕТЕЙ И СИСТЕМ

часть 1

для студентов всех специальностей

Самара 2021

Задание №1

1. Зашифровать сообщение одним из следующих методов:

Последняя цифра студенческого билета										
	1	2	3	4	5	6	7	8	9	0
Сообщение	1	2	3	4	5	5	4	3	2	1
Метод	1	2	3	4	5	1	2	5	4	3
Предпоследняя цифра студенческого билета										
	1	2	3	4	5	6	7	8	9	0
Ключевое слово/ магический квадрат/ размер блока	-	Следующий	-	4x4	Самоучитель	-	Волшебный	Конвертация	4x4	-

Варианты сообщений

1. Под информационной безопасностью следует понимать защиту интересов субъектов информационных отношений
2. Под доступом к информации понимается ознакомление модификация и уничтожение информации
3. Правила разграничения доступа служат для регламентации права доступа субъекта доступа к объекту доступа
4. Доступность это возможность за приемлемое время получить требуемую информационную услугу
5. Конфиденциальность данных это статус предоставляемый данным и определяющий требуемую степень их защиты

Варианты методов

а) Метод простой перестановки
б) Метод одиночной перестановки по ключу
в) Метод двойной перестановки сообщения
г) Шифрование магическими квадратами
д) Биграммный шифр Плейфера

Задание №2

2.1. Используя метод перестановок на основе маршрутов Гамильтона зашифровать сообщение из предыдущего задания:

Последняя цифра студенческого билета										
	1	2	3	4	5	6	7	8	9	0
L	4	5	6	2	5	6	4	5	6	7
Предпоследняя цифра студенческого билета										
	1	2	3	4	5	6	7	8	9	0
K	1,1,1,1,1,1,2,2,2,2,2,2,2	1,1,2,2,1,1,2,2,1,1,2	1,1,1,2,2,2,1,1,1,2,2,2,1	1,2,1,2,1,2,1,2,1,2,1	2,1,1,2,2,1,1,2,2,1,1,2,2	1,2,2,1,1,2,2,1,1,2,2,1,1	2,1,2,1,2,1,2,1,2,1,2	2,2,2,1,1,1,2,2,2,1,1,1,2	2,2,1,1,2,2,1,1,2,2,1	2,2,2,2,2,2,2,1,1,1,1,1,1

Задание №3

3. Пусть выбраны простые числа p и q, а также открытый ключ e. Требуется выполнить шифрование и дешифрование в ассиметричной криптосистеме RSA сообщения:

Последняя цифра студенческого билета										
	1	2	3	4	5	6	7	8	9	0
p	31	37	41	43	47	53	59	61	67	71
q	89	83	79	73	101	107	97	103	109	89
Предпоследняя цифра студенческого билета										
	1	2	3	4	5	6	7	8	9	0
e	101	97	89	83	79	73	79	83	89	97
Сообщение	1	2	3	4	5	1	2	3	4	5

1. 5764996751347925346
2. 98754783459345986
3. 634923499192345193

4. 234616141136234616748
5. 663487195324672817

Задание №4

4. Сформировать и проверить ЭЦП Эль Гамаля при следующих начальных условиях:

Последняя цифра студенческого билета										
	1	2	3	4	5	6	7	8	9	0
P	13	17	19	23	29	31	37	31	29	23
G	2	3	4	5	4	3	5	2	5	3
Предпоследняя цифра студенческого билета										
	1	2	3	4	5	6	7	8	9	0
X	7	8	9	10	11	10	9	8	7	6

Задание №5

5. Реализовать алгоритм открытого распределения ключей Диффи-Хеллмана при следующих начальных условиях: модуль N, примитивный элемент g, секретные ключи пользователей $К_а$ и $К_в$:

Последняя цифра студенческого билета										
	1	2	3	4	5	6	7	8	9	0
N	79	73	71	67	61	59	53	59	61	59
g	23	29	31	37	41	37	31	26	23	17
Предпоследняя цифра студенческого билета										
	1	2	3	4	5	6	7	8	9	0
K_a	13	14	17	15	21	23	25	23	21	19
K_b	41	30	36	21	38	37	42	43	32	31

Пояснение к заданию 4

Алгоритмы электронной цифровой подписи

4. Алгоритм цифровой подписи Эль Гамаля (EGSA)

Название EGSA происходит от слов El Gamal Signature Algorithm (алгоритм цифровой подписи Эль Гамаля). Идея EGSA основана на том, что для обоснования практической невозможности фальсификации цифровой подписи может быть использована более сложная вычислительная задача, чем разложение на множители большого целого числа,– задача дискретного логарифмирования. Кроме того, Эль Гамалю удалось избежать явной слабости алгоритма цифровой подписи RSA, связанной с возможностью подделки цифровой подписи под некоторыми сообщениями без определения секретного ключа.

Для того чтобы сгенерировать пару ключей (открытый ключ – секретный ключ), сначала выбирают некоторое большое простое целое число P и большое целое число G, причем $G < P$. Отправитель и получатель подписанного документа используют при вычислениях одинаковые большие целые числа P ($\sim 10^{308}$ или $\sim 2^{1024}$) и G ($\sim 10^{154}$ или $\sim 2^{512}$), которые не являются секретными.

Отправитель выбирает случайное целое число X, $1 < X \le (P-1)$, и вычисляет

$$Y = G^X \bmod P.$$

Число Y является открытым ключом, используемым для проверки подписи отправителя. Число Y открыто передается всем потенциальным получателям документов.

Число X является секретным ключом отправителя для подписывания документов и должно храниться в секрете.

Для того чтобы подписать сообщение M, сначала отправитель хэширует его с помощью хэш-функции $h(\cdot)$ в целое число m:

$$m = h(M), \quad 1 < m < (P-1),$$

и генерирует случайное целое число K, $1< K< (P-1)$, такое, что K и $(P-1)$ являются взаимно простыми. Затем отправитель вычисляет целое число a:

$$a = G^K \bmod P$$

и, применяя расширенный алгоритм Евклида, вычисляет с помощью секретного ключа X целое число b из уравнения

$$m =(X* a + K * b) (\text{mod } (P-1)).$$

Пара чисел (a,b) образует цифровую подпись S:

$$S = (a,b),$$

проставляемую под документом M.

Тройка чисел (M,a,b) передается получателю, в то время как пара чисел (X,K) держится в секрете.

После приема подписанного сообщения (M,a,b) получатель должен проверить, соответствует ли подпись S = (a,b) сообщению M. Для этого получатель сначала вычисляет по принятому сообщению M число

$$m = h(M),$$

т.е. хэширует принятое сообщение M.

Затем получатель вычисляет значение

$$A = Y^a a^b \text{ (mod P)}$$

и признает сообщение M подлинным, если, и только если

$$A = G^m \text{ (mod P)}.$$

Иначе говоря, получатель проверяет справедливость соотношения

$$Y^a a^b \text{ (mod P)} = G^m \text{ (mod P)}.$$

Можно строго математически доказать, что последнее равенство будет выполняться тогда, и только тогда, когда подпись S=(a,b) под документом M получена с помощью именно того секретного ключа X, из которого был получен открытый ключ Y. Таким образом, можно надежно удостовериться, что отправителем сообщения M был обладатель именно данного секретного ключа X, не раскрывая при этом сам ключ, и что отправитель подписал именно этот конкретный документ M.

Выполнение каждой подписи по методу Эль Гамаля требует нового значения K, причем это значение должно выбираться

случайным образом. Если нарушитель раскроет значение K, повторно используемое отправителем, то он сможет раскрыть секретный ключ X отправителя.

Задача 1

Сформировать и проверить ЭЦП Эль Гамаля при следующих начальных условиях: P=11, G=2, секретный ключ X=8.

Решение. Вычисляем значение открытого ключа:

$$Y = G^X \bmod P = Y = 2^8 \bmod 11 = 3.$$

Предположим, что исходному сообщению M соответствует хэш-значение m = 5.

Для того,чтобы вычислить цифровую подпись под сообщением M, имеющем хэш-значение m = 5, сначала выберем случайное целое число K = 9. Убедимся, что числа K и (P – 1) являются взаимно простыми. Действительно,

$$\text{НОД}\ (9, 10) = 1.$$

Далее вычисляем элементы a и b подписи:

$$a = G^K \bmod P = 2^9 \bmod 11 = 6,$$

элемент b определяем, используя расширенный алгоритм Евклида:

$$m = (X * a + K * b)\ (\text{mod}\ (P - 1)).$$

При m = 5, a = 6, X = 8, K = 9, P = 11 получаем

$$5 = (6 * 8 + 9 * b)(\text{mod}\ 10)$$

или

$$9 * b \equiv -43\ (\text{mod}\ 10).$$

Решая сравнение, получаем b = 3. Цифровая подпись представляет собой пару: a = 6, b = 3.

Далее отправитель передает подписанное сообщение. Приняв подписанное сообщение и открытый ключ Y = 3, получатель вычисляет хэш-значение для сообщения M : m = 5, а затем вычисляет два числа:

1) $Y^a a^b\ (\text{mod}\ P) = 3^6 * 6^3\ (\text{mod}\ 11) = 10$;

2) $G^m\ (\text{mod}\ P) = 2^5\ (\text{mod}\ 11) = 10$.

Так как эти два целых числа равны, принятое получателем сообщение признается подлинным.

Следует отметить, что схема Эль Гамаля является характерным примером подхода, который допускает пересылку сообщения M в открытой форме вместе с присоединенным аутентификатором (a,b). В таких случаях процедура установления подлинности принятого сообщения состоит в проверке соответствия аутентификатора сообщению.

Схема цифровой подписи Эль Гамаля имеет ряд преимуществ по сравнению со схемой цифровой подписи RSA.

1. При заданном уровне стойкости алгоритма цифровой подписи целые числа, участвующие в вычислениях, имеют запись на 25% короче, что уменьшает сложность вычислений почти в два раза и позволяет заметно сократить объем используемой памяти.
2. При выборе модуля P достаточно проверить, что это число является простым и что у числа (P –1) имеется большой простой множитель (т.е. всего два достаточно просто проверяемых условия).
3. Процедура формирования подписи по схеме Эль Гамаля не позволяет вычислять цифровые подписи под новыми сообщениями без знания секретного ключа (как в RSA).

Однако алгоритм цифровой подписи Эль Гамаля имеет и некоторые недостатки по сравнению со схемой подписи RSA. В частности, длина цифровой подписи получается в 1,5 раза больше, что, в свою очередь, увеличивает время ее вычисления.

Пояснение к заданию 5

Распределение ключей в компьютерной сети

При использовании для информационного обмена криптосистемы с симметричным секретным ключом два пользователя, желающие обменяться криптографически защищенной информацией, должны обладать общим секретным ключом. Пользователи должны обменяться общим ключом по каналу связи безопасным образом. Если пользователи меняют ключ достаточно часто, то доставка ключа превращается в серьезную проблему.

Для решения этой проблем можно применить два способа:
1) использование криптосистемы с открытым ключом для шифрования и передачи секретного ключа симметричной криптосистемы;
2) использование системы открытого распределения ключей Диффи–Хеллмана.

5.1. Алгоритм открытого распределения ключей Диффи–Хеллмана

Алгоритм Диффи–Хеллмана был первым алгоритмом с открытыми ключами (предложен в 1976 г.). Его безопасность обусловлена трудностью вычисления дискретных логарифмов в конечном поле, в отличие от легкости дискретного возведения в степень в том же конечном поле.

Предположим, что два пользователя A и B хотят организовать защищенный коммуникационный канал.
1. Обе стороны заранее уславливаются о модуле N (N должен быть простым числом) и примитивном элементе g, ($1 \le g \le N - 1$).
Эти два целых числа N и g могут не храниться в секрете. Как правило, эти значения являются общими для всех пользователей системы.
2. Затем пользователи A и B независимо друг от друга выбирают собственные секретные ключи k_A и k_B (k_A и k_B – слу-

чайные большие целые числа, которые хранятся пользователями A и B в секрете).

3. Далее пользователь A вычисляет открытый ключ

$$y_A = g^{k_A} \pmod N,$$

а пользователь B – открытый ключ

$$y_B = g^{k_B} \pmod N.$$

4. Затем стороны A и B обмениваются вычисленными значениями открытых ключей y_A и y_B по незащищенному каналу.

5. Далее пользователи A и B вычисляют общий секретный ключ, используя следующие выражения:

пользователь A: $K = (y_B)^{k_A} = (g^{k_B})^{k_A} \pmod N$;

пользователь B: $K' = (y_A)^{k_B} = (g^{k_A})^{k_B} \pmod N$.

При этом $K = K'$, так как $(g^{k_B})^{k_A} = (g^{k_A})^{k_B} \pmod N$.

Схема реализации алгоритма Диффи–Хеллмана показана на рис. 6.1.

Ключ K может использоваться в качестве общего секретного ключа (ключа шифрования ключей) в симметричной криптосистеме. Кроме того, обе стороны A и B могут шифровать сообщения, используя следующее преобразование шифрования (типа RSA): $C = E_K(M) = M^K \pmod N$.

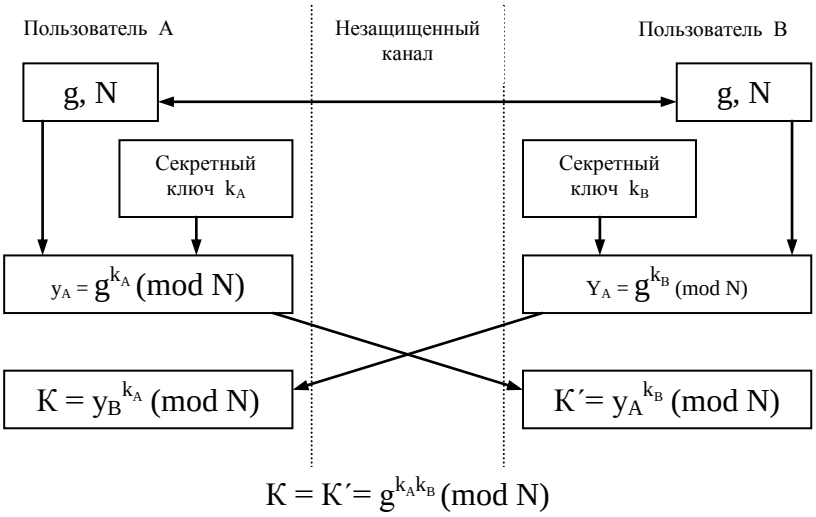

Рис. 6.1- Схема реализации алгоритма Диффи–Хеллмана

Для выполнения расшифрования получатель сначала находит ключ расшифрования K* с помощью сравнения

$$K * K^* \equiv 1 \pmod{N-1},$$

а затем восстанавливает сообщение

$$M = D_K(C) = C^{K^*} \pmod{N}.$$

Задача 1

Реализовать алгоритм открытого распределения ключей Диффи-Хеллмана при следующих начальных условиях: модуль N=47, примитивный элемент g=23, секретные ключи пользователей A и B: K_A=12, K_B=33 соответственно.

Решение. Для того, чтобы иметь общий секретный ключ K, пользователи A и B сначала вычисляют значения частных открытых ключей:

$$y_A = g^{k_A} \pmod{N} = 23^{12} \pmod{47} = 27,$$

$$y_B = g^{k_B} \pmod{N} = 23^{33} \pmod{47} = 33$$

После того, как пользователи A и B обменяются своими значениями y_A и y_B, они вычисляют общий секретный ключ $K = (y_B)^{k_A} \pmod{N} = (y_A)^{k_B} \pmod{N} = 33^{12} \pmod{47} = 27^{33} \pmod{47} = 23^{12*33} \pmod{47} = 25$.

Кроме того, они находят секретный ключ расшифрования, решая следующее сравнение:

$$K * K^* \equiv 1 \pmod{N-1},$$

откуда K* = 35.

Если сообщение M =16, то криптограмма:

$$C = M^K = 16^{25} \pmod{47} = 21.$$

Получатель восстанавливает сообщение :

$$M = C^{K^*} = 21^{35} \pmod{47} = 16.$$

Злоумышленник, перехватив значения N, g, y_A и y_B, тоже хотел бы определить значение ключа K. Очевидный путь для решения этой задачи состоит в вычислении такого значения k_A по N, g, y_A, что $g^{k_A} \bmod N = y_A$ (поскольку в этом случае, вычислив k_A, можно найти $K = (y_B)^{k_A} \bmod N$). Однако нахождение

k_A по N, g и y_A – задача нахождения дискретного логарифма в конечном поле, которая считается неразрешимой.

Выбор значений N и g может иметь существенное влияние на безопасность этой системы. Модуль N должен быть большим и простым числом. Число $(N-1)/2$ также должно быть простым числом. Число g желательно выбирать таким, чтобы оно было примитивным элементом множества Z_N.

Алгоритм открытого распределения ключей ДиффиХеллмана позволяет обойтись без защищенного канала для передачи ключей. Однако, работая с этим алгоритмом, необходимо иметь гарантию того, что пользователь A получил открытый ключ именно от пользователя B, и наоборот. Эта проблема решается с помощью электронной подписи, которой подписываются сообщения об открытом ключе.