7.ПРАКТИКАЛЫҚ ЖҰМЫСТАР

Практикалық жұмыс №1. Пәнге қатысты соңғы 5 жыл ішінде басылып шыққан әдебиеттер туралы деректерді кестеге енгізу керек. Егерде .pdf форматта әдебиет табылса, кестеге енгізуге болады. Электронды нұсқасын кестемен бірге оқытушыға поштаға салып жібересіз. Кем дегенде 5-10 атаудан тұратын болсын кесте.

«Ақпаратты қорғаудың криптографиялық әдістері» пәнінің қамтылуы

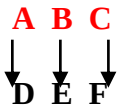
№	Әдебиет атауы	Автор (лар)	Басылым түрі (оқулық, оқу құралы, әдістемелік нұсқаулар т.с.с.)	Шыққан жылы	Баспана атауы	Беттер саны	Шифр (кітапх.)	УДК	№ абонемента (№ корпуса)
1.									
2.									

Практикалық жұмыс №2. Дәстүрлі шифрлеу жүйелерінде жұмыс жасау.

Ағымдық жүйелер

Әр шифрге мысал келтірілген, сосын төменде тапсырма берілген, жауабын тауып толтыру керек

1. Цезарь шифры (жылжыту). Цезарь шифры (50 г. до н.э.) негізінде әріптер 3 әріпке жылжыту арқылы жүргізіледі (жалпы жағдайда **к** әріпке):



Тогда:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z → *pt*

Д E F G H I J K L M N O P Q R S T U V W X Y Z A B C → *ct*

Пример 1:

pt_L=PROCESSOR

ct_L=SURFHVVRU

pt_r=ПРОЦЕССОР

ct_r=?

ct_r=НСПТЯБХЗУ

pt_r=?

Пример 2:

pt_r=ПРОГРАММИРОВАНИЕ

ct_r=ТУСЁУГПП ЛУСЕ ГРЛ З

pt_r=СИСТЕМНЫЙ БЛОК

ct_r=?

pt_k=БАҒДА РЛАМАЛАУ

ct_k=?

Пример 3:

pt = IBM

ct = ?

Пример 4:

k = 25

ct = BNLOTSDQ

pt = ?

2. Трисемус шифры (немецкий аббат, 1508г.) (алмастыру шифры).

Задается ключевое слово. Оставшиеся буквы, не входящее в это слово дописываются в таблицу. Шифрование заключается в том, что каждой букве соответствует символ, находящийся под этой буквой.

д	**о**	**к**	**у**	**м**	**е**	**н**	**т**
А	Б	В	Г	**Ж**	З	И	Й
Л	П	Р	С	**Ф**	Х	Ц	Ч
Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я

Пример 1 (в рассматриваемом примере пропущена буква «ё» для использования таблицы меньшей размерности):

pt_r=МОДЕМ

ct_r=ЖБАЗЖ

Задание
pt_r=ФАЙЛ
ct_r=?
ct_r=ЗШМ
pt_r=?

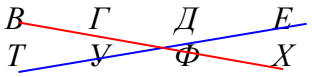
3. Шифр Плейфейера (без ключа)

Шифр Плейфейра, изобретенный в 1854г., является наиболее известным биграммным шифром замены. Основой шифра Плейфейра является шифрующая таблица со случайно расположенными буквами алфавита исходных сообщений. Для удобства запоминания шифрующей таблицы отправителем и получателем сообщений можно использовать ключевое слово при заполнении начальных строк таблицы.

Шифр Плейфейера заключается в том, что каждой паре букв соответствуют символы из таблицы:

А	Б	**В**	Г	Д	**Е**	Ж	З
И	Й	К	Л	М	Н	О	П
Р	С	**Т**	У	Ф	**Х**	Ц	Ч
Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я

а) Если обе буквы биграммы открытого текста не попадают на одну строку или столбец
Например: ЕТ



ВХ (буквы на пересечении и наоборот)

б) Если обе буквы биграммы открытого текста принадлежат одному столбцу таблицы, то буквами шифротекста считаются буквы, которые лежат под ними
Например:

Е
Н
Х
Э

***ЕХ*->НЭ**

в) Если обе буквы биграммы открытого текста принадлежат одной строке таблицы, то буквами шифртекста считаются буквы, которые лежат справа от них.
*Например: **МО* -> НП**

Пример 1:
pt_r=ДИСК
ct_r=АМТЙ.

Задание:
ct_r=ХВЭХПМЛЖПШ
pt_r=?

4. Шифр Плейфейера (с ключом).

Шифрование происходит так же, как предыдущее, только задается ключевое слово.

д	**о**	**к**	**у**	**м**	**е**	**н**	**т**
А	Б	В	Г	Ж	З	И	Й
Л	П	Р	С	Ф	Х	Ц	Ч
Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я

Пример 1:
pt_r=ТУРБО ПАСКАЛЬ
ct_r=ДМПВБЩГЛДВФШ

Задание
ct_r=ЦГЧУНЕУЫЦЙФПНТЙЮ
pt_r=?

Шифр перестановки на основе магических квадратов

Дан магический квадрат. Слово, которое нужно зашифровать нумеруем и вписываем символы в квадрат, сопоставляя цифры магического квадрата и номера шифруемого слова. Для примера взят магический квадрат 4x4.

16	3	2	13
5	10	11	8
9	6	7	12
4	15	14	1

Известно, что ∃ 1 маг 3*3
880 4*4
250000 5*5

Пример 1:
pt_r=КОМПЬЮТЕРИЗАЦИЯ!
Ct_r=!МОЦЬИЗЕРЮТАПЯИК

!	М	О	Ц
Ь	И	З	Е
Р	Ю	Т	А
П	Я	И	К

Задание:
ct_r=ИМОСЬНЫЕРЮТЕПТЕК
pt_r=?

Шифр Уитстона (19в.)

При шифровании исходного текста нужно построить 2 таблицы. Буквы и символы в этих таблицах могут располагаться произвольно. Таблицы построены следующим образом:

Таблица №1

Ж	Щ	Н	Ю	Р
И	Т	Ь	Ц	Б
Я	М	Е	.	С
В	Ы	П	Ч	
:	Д	У	О	К
З	Э	Ф	Г	Ш
Х	А	,	Л	Ъ

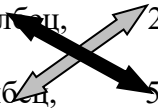
Таблица №2

И	Ч	Г	Я	Т
,	Ж	Ь	М	О
З	Ю	Р	В	Щ
Ц	:	П	Е	Л
Ъ	А	Н	.	Х
Э	К	С	Ш	Д
Б	Ф	У	Ы	

Процедуру шифрования рассмотрим на примере. Исходное слово: Информация.
Необходимо разделить данное слово следующим образом: ИН ФО РМ АЦ ИЯ.
Для того, чтобы зашифровать первые две буквы (ИН): берем первую букву (И) смотрим в 1-ю таблицу, выписываем местоположение данной буквы, то есть (1-ый столбец, 2-я строка); далее,

берем вторую букву (Н), смотрим во 2-й таблице ее местонахождение, то есть (3-й столбец, 5-я строка). Теперь составим пропорцию следующего вида:

1-ый столбец, 2-я строка (И)



3-й столбец, 5-я строка (Н)

Теперь, чтобы зашифровать букву (И), из данной пропорции берем ту часть, которая выделена серым цветом, т.е.: 3-й столбец, 2-я строка, и смотрим на вторую таблицу. Во второй таблице на пересечении (3-го столбца, 2-й строки) стоит буква (Ь). Здесь с помощью второй таблицы мы зашифровали букву (И). Таким образом получили: исходная буква (И) заменилась на (Ь).

Теперь, чтобы зашифровать букву (Н), из данной пропорции берем ту часть, которая выделена черным цветом, т.е.: 1-й столбец, 5-я строка, и смотрим на первую таблицу. В первой таблице на пересечении (1-го столбца, 5-й строки) стоит символ (:). Здесь с помощью первой таблицы мы зашифровали букву (Н). Таким образом получили: исходная буква (Н) заменилась на (:).

В результате исходные первые 2 буквы (ИН) зашифровались как (Ь:).

Точно таким же образом шифруются и другие парные буквы исходного слова, в результате получаем следующее:

(исходное слово) (зашифрованное слово)

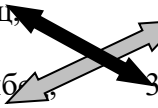
ИН ФО РМ АЦ ИЯ = Ь: ДЬ ЯБ БЫ МЖ

Следующий пример. Исходное зашифрованное слово: ПЕ ОВ ЩН ФМ. Необходимо расшифровать данное слово.

Для начала, берем первые 2 буквы (ПЕ): Здесь первая исходная буква (П), чтобы расшифровать эту букву смотрим во вторую таблицу и записываем его месторасположение, т.е. (3-й столбец, 4-я строка). Таким же способом исходную букву (Е) смотрим в первой таблице, т.е. (3-й столбец, 3-я строка).

Теперь составим пропорцию следующего вида:

3-й столбец, 4-я строка (П)



3-й столбец, 3-я строка (Е)

Теперь, чтобы расшифровать букву (П), из данной пропорции берем ту часть, которая выделена серым цветом, т.е.: 3-й столбец, 4-я строка, и смотрим на первую таблицу. В первой таблице на пересечении (3-го столбца, 4-й строки) стоит буква (П). Здесь с помощью первой таблицы мы расшифровали букву (П). Таким образом получили: исходная буква (П) расшифровалась как (П).

Теперь, чтобы расшифровать букву (Е), из данной пропорции берем ту часть, которая выделена черным цветом, т.е.: 3-й столбец, 3-я строка, и смотрим на вторую таблицу. Во - второй таблице на пересечении (3-го столбца, 3-й строки) стоит буква (Р). Здесь с помощью второй таблицы мы расшифровали букву (Е). Таким образом получили: исходная буква (Е) расшифровалась как (Р).

В результате исходные первые 2 буквы (ПЕ) расшифровались как (ПР).

Точно таким же образом расшифровываются и другие парные буквы исходного слова, в результате получаем следующее:

(исходное зашифрованное слово) (расшифрованное слово)

ПЕ ОВ ЩН ФМ = ПР ИЛ ЕТ АЮ.

Задание. Дана таблица

ж	щ	н	ю	р
и	т	ь	ц	б
я	м	е	.	с
в	ы	п	г	
:	д	у	о	к
з	э	ф	ч	ш
х	а	,	л	ъ

и	ч	а	я	т
,	ж	ь	м	о
з	ю	р	в	ц
ц	:	п	е	л
ъ	э	н	.	х
ғ	қ	с	ш	д
б	ф	у	ы	ш

Расшифруйте следующие криптограммы
ct_r=Ь:МЫАКЦН
ct_r=ЬРСЖНЩАУЛД

Задания по теме «Магические квадраты и криптография»

1 Составьте магический квадрат размерности 3х3
Пользуясь составленным квадратом, расшифруйте закрытый текст
Ct = ПРОМЬТЕКЮ

2 Дан магический квадрат 5х5

11	9	22	5	18
19	12	10	23	1
2	20	13	6	24
25	3	16	14	7
8	21	4	17	15

Зашифруйте открытый текст Pt = «информационная культура»

3 Воспользовавшись таблицей следующей таблицей Уитстона

ж	щ	н	ю	р
и	т	ь	ц	б
я	м	е	.	с
в	ы	п	г	
:	д	у	о	к
з	э	ф	ч	ш
х	а	,	л	ъ

и	ч	а	я	т
,	ж	ь	м	о
з	ю	р	в	ц
э	:	п	е	л
ъ	а	н	.	х
г	қ	с	Щ	д
б	ф	у	ы	ш

Расшифруйте криптограмму:
Ct = гншццбгнв:

Практикалық жұмыс №3. Шифрлеу стандарттарына сипаттама беру. Сипаттама критерийлері кесте түрінде берілген. Кестеде кем дегенде 3 стандарт сипатталу тиіс. Соңғы бағандағы сызбаны бөлек келтіруге болады

Шифрлеу стандарттарының сипаттамасы

№	Стандарт атауы	Қысқаша мазмұны	Шыққан жылы	Қолдану аймағы	Сызбасы
1					

Нәтиже тексеруге оқытушының поштасына жіберіледі

Практикалық жұмыс №4. Қалдықтар класындағы есептеулерді жасау. Салыстырмалар шешу. Есептерге нұсқаулықтар, шығару жолдары берілген

Қалдықтар класындағы есептеулер.

Примеры:

a mod n
a-произвольное целое число
n- модуль, целое число
a,n – заданные числа
7 mod23=7, a=7 n=23
25 mod23=2
47 mod23=1
23 mod23=0
22 mod23=22
-4 mod23=19
-45 mod23=1

Анализ вычислений в модулярной арифметике:

1) результаты не выходят за пределы модуля (нет ошибок переполнения при вычислении на ЭВМ);
2) все операции производятся с целыми числами (не бывает ошибок округления).

Келесі есептерді шешу керек:
Модуль бойынша есептеу:
5 mod13
11mod71
56mod17
-3mod7
-53mod19
88mod88
0mod14
18mod19

Дәреже алу алгоритмі

$$5^5 \bmod 9 = (5^2)^2 \cdot 5 \bmod 9 = (25 \bmod 9)^2 \cdot 5 \bmod 9 = 7^2 \bmod 9 \cdot 5 \bmod 9 = 4 \cdot 5 \bmod 9 = 20 \bmod$$

Таким образом $5^5 \bmod 9 = 2$

3^{15}mod7=(3*3^{14})mod7=(3*3^6*3^8)mod7=3*(3^2*3)^2*((3^2)^2)^{2}mod7=((((3^2*3)^2)^2*3^2*3)mod7= 6.
3^{15}≡6(mod 7)

Келесі өрнектерді есептеңіз:

(1) $3^{19} \bmod 17$ (ответ 10)
(2) $2^{30} \bmod 5$ (ответ 4)
(3) $5^{16} \bmod 13$ (ответ 1)
(4) $5^{35} \bmod 33$
(5) $7^{23} \bmod 13$
(6) $4^{37} \bmod 26$

Кері мәнді табу

Пусть дано сравнение вида $ax \equiv 1 \bmod n$ (1),

где a, n - известные числа. Требуется найти x: $x = a^{-1} \bmod n$, где a^{-1} - есть обратное значение числа a. Неизвестное x можно найти тремя способами:

- методом прямого перебора;
- с помощью функции Эйлера;
- через расширенный алгоритм Евклида.

Пример:

Пусть дано сравнение вида $ax \equiv 1 \bmod n$: $4x \equiv 1 \bmod 13$.

Тура іріктеу әдісі

x	ax	$ax \bmod n$
x	$4x$	$4x \bmod 13$
1	4	4
2	8	8
3	12	12
4	16	3
5	20	7
6	24	11
7	28	2
8	32	6
9	36	10
10	40	**1**

Ответ: $x = 10$.

Проверка $4*10 \bmod 13 \equiv 40 \bmod 13 \equiv 1 \bmod 13$

Тура іріктеу әдісімен х-ті табыңыз.

27x=1 mod 17
6x=1 mod 19
2x=1 mod 17
3x= 1 mod 7
3x=1mod 11
4x=1 mod 13
7x=1 mod 33
6x=1 mod 11
11x=1 mod 6
4x=1 mod 33

Вычисление обратных величин с помощью функции Эйлера. Расширенный алгоритм Евклида.

С помощью функции Эйлера. $\varphi(n)$ называется функцией Эйлера, ее значение равно количеству чисел меньших n и взаимно простых с n. В криптографии наибольший интерес представляют 3 случая:

Если n - простое число $\Rightarrow \varphi(n) = n - 1$.

$n = 7$

$1 \quad 2 \quad 3 \quad 4 \quad 5 \quad 6 \Rightarrow \varphi(7) = 6$

Если $n = p \cdot q$, где p, q - простые числа, то $\varphi(n) = (p-1)(q-1)$.

$n = 33$

$1 \quad 2 \quad \underline{3} \quad 4 \quad 5 \quad \underline{6} \quad 7 \quad 8 \_\_ u \_ m.д. \Rightarrow \varphi(33) = 20$

Если $n = k^r$, то $\varphi(n) = k^{r-1} \cdot (k-1)$.

$n = 8 = 2^3$

1 2 3 4 5 6 $7 \Rightarrow \varphi(8) = 4$

Тогда решение сравнения (1) через функцию Эйлера определяется по формуле

$x = a^{\varphi(n)-1} \bmod n$

Тогда и предыдущий пример этим способом решится

$x = a^{\varphi(n)-1} \bmod n \Rightarrow x = 4^{\varphi(13)-1} \bmod 13 = 4^{11} \bmod 13 = (4^2)^5 \cdot 4 \bmod 13 = (16 \bmod 13)^5 \cdot 4 \bmod 13 = (3^2)^2 \cdot 3 \cdot \cdot 4 \mathrm{r}$

$= (9 \bmod 13)^2 \cdot 12 \bmod 13 = 81 \cdot 12 \bmod 13 = 81 \bmod 13 \cdot 12 \bmod 13 = 3 \cdot 12 \bmod 13 = 36 \bmod 13 = 10$

т.е. получено также значение 10, что и методом прямого перебора

Расширенный алгоритм Евклида. Пусть дано сравнение вида (1). Расширенный алгоритм Евклида заключается в следующем:

1. Установить $(u_1, u_2, u_3) = (0,1,n); (v_1, v_2, v_3) = (1,0,a)$.
2. Если $u_3 = 1$, то алгоритм завершается и $x = u_1$. Иначе п.3.
3. $q = [u_3 / v_3]$

   $(t_1, t_2, t_3) = (u_1, u_2, u_3) - (v_1, v_2, v_3) \cdot q$

   $(u_1, u_2, u_3) = (v_1, v_2, v_3)$

   $(v_1, v_2, v_3) = (t_1, t_2, t_3)$

   Возвращаемся к п.2.

$4x \equiv 1 \bmod 13$

q	u_1	u_2	u_3	v_1	v_2	v_3
-	0	1	13	1	0	4
3	1	0	4	-3	1	1
4	**-3**	1	1			

Ответ: $x = -3 \bmod 13 \equiv 13 - 3 = 10$.

Задания для самостоятельного решения.

1.1 Решить сравнения

27x=1 mod 17 (ответ 12)
6x=1 mod 19 (ответ 16)
2x=1 mod 17 (ответ 9)
3x= 1 mod 7 (ответ 5)
3x=1mod 11 (ответ 4)
4x=1 mod 13 (ответ 10)
7x=1 mod 33 (ответ 19)
6x=1 mod 11 (ответ 2)
11x=1 mod 6 (ответ 5)
4x=1 mod 33 (ответ 25)

1.2 С помощью функции Эйлера вычислить

7^{-1} mod 13 (ответ 2)
4^{-1} mod 15 (ответ 4)
3^{-1} mod 16 (ответ 11)
7^{-1} mod 9 (ответ 4)
3^{-1} mod 25 (ответ 17)
2^{-1} mod 9 (ответ 5)
8^{-1} mod 13 (ответ 5)
5^{-1} mod 26 (ответ 21)

3^{-1} mod 8 (ответ 3)
4^{-1} mod 9 (ответ 7)
8^{-1} mod 9 (ответ 8)
5^{-1} mod 9 (ответ 2)

Практикалық тапсырма №5. RSA ашық кілтті криптожүйені қолдану арқылы құпия хабарлама алмасу

Выбираем большое натуральное число N=P*Q, где P,Q простые числа.

Рассмотрим генерацию ключей. В алгоритме RSA используются два ключа:

- e – открытый ключ;
- d – закрытый/секретный ключ.

Открытый ключ e выбирается из следующего условия:

$$НОД(e,\varphi(N)) \equiv 1$$

где $\varphi(N)$ - функция Эйлера.

Секретный ключ d вычисляется из сравнения по следующей формуле:

$$e \cdot d = 1 \bmod \varphi(N)$$

Криптографическую систему формирует получатель секретной информации, т.е. осуществляет генерацию ключей и публикует (e,N).

Таким образом, (e,N) – открытая информация, (d,P,Q) – секретная информация.

Шифрование и расшифрование реализуется по следующей схеме:

- Оцифровка исходного текста pt;
- Шифрование производится по следующей формуле:

$$pt^e \bmod N = ct$$

Действие производится отправителем.

- Расшифрование производится по следующей формуле:

$$ct^d \bmod N = (pt^e)^{d \bmod \varphi(N)} = pt$$

Действие производится получателем информации.

Пример 1: $pt = YES$

1. $p = 11, q = 3 \Rightarrow N = 33$
   $\varphi(33) = 20 \Rightarrow E = 7$
   $7 \cdot D = 1 \bmod 20 \Rightarrow D = 3$
2. $YES \leftrightarrow 24 \quad 4 \quad 18$

$$\left.\begin{array}{l} 24^7 \bmod 33 = 18 \rightarrow S \\ 4^7 \bmod 33 = 16 \rightarrow Q \\ 18^7 \bmod 33 = 6 \rightarrow G \end{array}\right\} \Rightarrow ct = SQG$$

3. $SQG \leftrightarrow 18 \quad 16 \quad 6$

$$\left.\begin{array}{l} 18^3 \bmod 33 = 24 \rightarrow Y \\ 16^3 \bmod 33 = 4 \rightarrow E \\ 6^3 \bmod 33 = 18 \rightarrow S \end{array}\right\} \Rightarrow pt = YES$$

Пример 2: $pt = NO$ ***Екінші мысалды өздерің шифрлеп, шифрден ашып көрсетіңіз***

Пример 3: Рассмотрим практически й пример обмена информацией между двумя абонентами. Пусть банкир и вкладчик решили установить между собой секретную передачу шифрованной информации с помощью алгоритма RSA. Независимо друг от друга они создают ключи:

Действия	Банкир	Вкладчик
1. Выбор двух простых чисел p и q.	$p_1 = 7; q_1 = 13$	$p_2 = 11; q_2 = 23$
2. Вычисление $N = p \cdot q$	$N_1 = 91$	$N_2 = 253$

3. Расчет функции Эйлера $\varphi(N)$	$\varphi(N_1) = 72$	$\varphi(N_2) = 220$
4. Выбор случайного числа e, взаимнопростого с $\varphi(N)$	$e_1 = 5$	$e_2 = 31$
5. Расчет секретного ключа d	$D_1 = 29$	$D_2 = 71$
6. Публикация открытого ключа	(5,91)	(31,253)

Пусть банкиру требуется переслать вкладчику сообщение, которое зашифровано методом замены числом 2 .

Шифровка банкира: $ct = 2^{31} \bmod 253 = 167$.

Далее число 167 передается вкладчику, который в свою очередь, получив шифрограмму используя свой секретный ключ, производит дешифрацию:

$$167^{71} \bmod 253 = 2$$

Практикалық тапсрыма №6. DH жүйесінде ортақ құпия жасау

Рассмотрим в качестве платформы (некоторое базовое множество, обладающее особыми свойствами, используемыми для построения шифра) мультипликативную группу конечного поля.

Дана Z_p- мультипликативная группа , пусть q-порождающий элемент => любой элемент

fϵZ_p* можно представить

$f=q^R, 1 \le R \le p-1$

Число R называют дискретным логарифмом элемента f по основанию q,и обозначить $R=\log_g f$

Задача нахождения R является трудной вычислительной проблемой, она не решается за реальное время.

В общем виде $q^x=f$ x-?

q-известное значение меняя f, получаем $f_1=q^{x1}$ $f_2=q^{x2}$

В криптографий p>>(очень большие числа) по этому поиск x_i- проходит долго (даже при организации на компьютере). Эта проблема используется в протоколах для секретной передачи ключей. Один из таких известных протоколов – протокол Д-Н(1976), где используется дискретный логарифм для формирования секретного ключа. Для рассмотрения примера этого алгоритма сначала продемонстрируем примеры выбора порождающего элемента.

Пример1

Z_5^* ={1,2,3,4}

$2^1=2$

$2^{2=}4$

$2^3=3$

$2^4=1$

Число 2 является порождающим

Пример2

Z_7^*={1,2,..,6}

$2^1=2$

$2^2=4$

$2^3=1$

$2^4=2$ этот элемент уже был, значит число 2 не может являться порождающим, элемент 3 может являться порождающим.

Пример 3
Z_{11}^*={0,1,2,3,4,5,6,7,8,9,10}, q – порождающий элемент группы

2^1 mod 11=**2**
2^2 mod 11=**4**
2^3 mod 11=**8**
2^4 mod 11=**5**
2^5 mod 11=**10**
2^6 mod 11=**9**
2^7 mod 11=**7**
2^8 mod 11=**3**
2^9 mod 11=**6**
2^{10} mod 11=**1**

т.к число 2 (возводимое в каждый элемент группы) содержит все элементы группы Z_{11}^*, то q=2

Далее излагается схема алгоритма формирования общего секретного ключа.

Имеются 2 корреспондента А↔В

1. 2 корреспондента открыто договариваются по сети о Z^*_P, q→порождающий элемент простого поля.
2. А загадывает секретное число a b Z^*_P и →B.q^a
3. В тоже загадывает секретное число в в Z^*_P→A $q^в$
4. B : q^{ab}-формирует
5. A : q^{ba}-формирует

Злоумышленник видит целиком q^a, q^b, но не видит q^{ab}, q^{ba}

Пример 1:

1. Z^*_7,q=3
2. A: a=4 →B $q^a=3^4 \bmod 7=4$
3. B: b=2→A $q^b=3^2 \bmod 7=2$
4. B : $q^{ab}=(3^4)^2 \bmod 7=4^2 \bmod 7=2$ общее секретное число =2
5. A: $q^{ba}=(3^2)^4 \bmod 7=(2)^4 \bmod 7=2$

Пример 2:

1) Z_{11}^*, q=2
2) A: a=3, $2^3 \bmod 11=8$ →B
3) B: b=7, $2^7 \bmod 11=7$ →A
4) A: $7^3 \bmod 11=$**2**
5) B: $8^7 \bmod 11=$**2**

Тапсырма: екі көрсетілген мысалдардың айырмашылығын тауып көрсетіңіз. Өз мысалыңызды құрастырыңыз

Практикалық жұмыс №7. Жоба әзірлеу

Жобалық жұмыс келесі кезеңдерді өтуге талап қойған:

1. Тақырып таңдау
2. Жобаның қысқаша сипаттамасын әзірлеу
3. Жобаның презентациясын жасау
4. Жобаны қорғау

Тақырыптар тізімі:

1) Блокчейн технологиялары мен криптография есептері
2) Кванттық криптография мүмкіндіктері

3) Эллипстік криптография болашағы
4) Электрондық сандық қолтаңба алу процедурасы және қазіргі мәселелері
5) Біржақты функциялар және NP-есептер
6) Хэш функциялары және криптография
7) Криптотұрақтылық түрлері және қолданбалы есептер
8) Криптовалюталарды өңдеу
9) Бұлттық қоймалады криптография арқылы қорғау
10) Аутентификация түрлері және қиындықтар
11) Деректерге қатынауды шектеу үлгілері
12) Идентификациялау хаттамалары
13) «Қытай қабырғасы» ақпаратқа қатынауды шектеу үлгісі
14) Рольдік басқару негізінде ақпаратқа қатынауды шектеу
15) Биба тұтастық шектеу үлгісі