Министерство образования и науки Российской Федерации

ФИЛИАЛ ГОСУДАРСТВЕННОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ
ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«БАЙКАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ЭКОНОМИКИ И ПРАВА» В Г. УСТЬ-ИЛИМСКЕ

(Филиал ГОУ ВПО в г. Усть-Илимске)

Кафедра Экономики

УТВЕРЖДАЮ
Заместитель директора
по учебно-методической работе
_____Н.Н.Шелепетко
_____

# «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

## МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ВЫПОЛНЕНИЮ КОНТРОЛЬНОЙ РАБОТЫ ВОПРОСЫ К ЭКЗАМЕНУ

Составитель:
Преподаватель Д.В. Пиминов

Усть-Илимск, 2010

СОДЕРЖАНИЕ

# ВВЕДЕНИЕ

Современное общество не мыслимо без интенсивного обмена информацией, поэтому именно в последние десятилетия вопрос её защиты касается не только специалистов соответствующей квалификации, но и обычных людей.

Современный человек доверяющий важную информацию вычислительным устройствам,  и вообще владеющий подобной информацией, обязан знать о возможных угрозах её целостности, конфиденциальности и надёжности. Для этого необходимо ознакомиться с возможными информационными рисками, способами их прогнозирования, предотвращения и ликвидации последствий в случае их реализации. Важно знать принципы защиты информации и особенности работы и использования применяющихся для этого технологий.

Данная контрольная работа состоит из двух частей: теоретической и практической. В первой необходимо написать реферат по одному из наиболее актуальных вопросов информационной безопасности, во второй — решить три задачи, показывающих суть некоторых методов криптографии.

## ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

1. Информационная безопасность и государство.
2. Технология электронной цифровой подписи.
3. Методы криптографии (виды, особенности, способы применения).
4. Технология хеширования (виды, особенности, способы применения в том числе и с точки зрения информационной безопасности).
5. Методика создания политики безопасности.
6. Требования по работе с конфиденциальной информацией. Рассмотреть различные виды тайн (коммерческая тайна, государственная тайна, и несколько профессиональных тайн).
7. Особенности работы с персональными данными в цифровую эпоху (проблема, взгляд законодательства, способы решения).
8. Особенности использования технических средств защиты авторских прав (ТСЗАП или DRM) их виды, принципы работы, согласованность с законодательством и правами потребителей.
9. Социальная инженерия, как метод получения несанкционированного доступа к информации (особенности, способы, виды).
10. Побочное электромагнитное излучение и наводки (ПЭМИН), как угроза информационной безопасности.
11. Методы обеспечения безопасности при передаче информации по каналам связи.
12. Принципы работы систем электронного документооборота.
13. Вредоносные программы — виды, принципы работы, распространенность, угрозы и способы защиты.
14. Типичные угрозы в среде Интернет.
15. Использование средств безопасности для защиты Интернет-сервисов (удаленный доступ, электронная почта, электронная коммерция).
16. Авторизация и аутентификация. Способы аутентификации, принципы работы, достоинства и недостатки.

17. Проблема защиты авторских прав в информационную эпоху и способы их решения.

18. Проблемы обеспечения подлинности электронных цифровых подписей.

Номер варианта выбирается по сумме последних двух цифр зачетки. В случае, если итоговое число равно нулю, то следует выбрать первый вариант.

## ПРАКТИЧЕСКАЯ ЧАСТЬ

### Симметричное зашифровывание — расшифровывание

Предлагается зашифровать заданный текст с помощью шифра «Виженера».

Блез Виженер

Этот метод является простой формой многоалфавитной замены. Шифр Виженера изобретался многократно. Впервые этот метод описал Джован Баттиста Беллазо (итал. *Giovan Battista Bellaso*) в книге La cifra del. Sig. Giovan Battista Bellaso в 1553 году, однако в XIX веке получил имя Блеза Виженера, швейцарского дипломата. Метод прост для понимания и реализации, он является недоступным для простых методов криптоанализа.

Первое точное документированное описание многоалфавитного шифра было сформулированно Леоном Баттиста Альберти в 1467 году, для переключения между алфавитами использовался металлический шифровальный диск. Система Альберти переключает алфавиты после нескольких зашифрованных слов. Позднее, в 1518 году, Иоганн Трисемус в своей работе «Полиграфия» изобрел tabula recta — центральный компонент шифра Виженера.


Репродукция шифровального диска Конфедерации

То, что сейчас известно под шифром Виженера, впервые описал Джованни Батиста Беллазо в своей книге La cifra del. Sig. Giovan Battista Bellaso. Он использовал идею tabula recta Трисемуса, но добавил ключ для переключения алфавитов шифра через каждую букву.

Блез Виженер представил своё описание простого, но стойкого шифра перед комиссией Генриха III во Франции в 1586 году, и позднее изобретение

шифра было присвоено именно ему. Давид Кан в своей книге «Взломщики кодов» отозвался об этом осуждающе, написав, что история «проигнорировала важный факт и назвала шифр именем Виженера, несмотря на то, что он ничего не сделал для его создания».

Шифр Виженера имел репутацию исключительно стойкого к «ручному» взлому. Известный писатель и математик Чарльз Лютвидж Доджсон (Льюис Кэрролл) назвал шифр Виженера невзламываемым в своей статье «Алфавитный шифр» англ. *The Alphabet Cipher*, опубликованной в детском журнале в 1868 году. В 1917 году Scientific American также отозвался о шифре Виженера, как о неподдающемся взлому. Это представление было опровергнуто после того, как Казиски полностью взломал шифр в XIX веке, хотя известны случаи взлома этого шифра некоторыми опытными криптоаналитиками ещё в XVI веке.

Шифр Виженера достаточно прост для использования в полевых условиях, особенно если применяются шифровальные диски. Например, «конфедераты» использовали медный шифровальный диск для шифра Виженера в ходе Гражданской войны. Послания Конфедерации были далеки от секретных, и их противники регулярно взламывали сообщения. Во время войны командование Конфедерации полагалось на три ключевых словосочетания: «Manchester Bluff», «Complete Victory» и — так как война подходила к концу — «Come Retribution».

Гилберт Вернам попытался улучшить взломанный шифр (он получил название шифр Вернама-Виженера в 1918 году), но, несмотря на его усовершенствования, шифр так и остался уязвимым к криптоанализу. Однако работа Вернама в конечном итоге всё же привела к получению шифра, который по-настоящему трудно взломать.

Шифр Виженера достаточно прост для использования в «полевых условиях», особенно если применяются шифровальные диски.

Задача 1

Зашифруйте текст: «Защита информации». Ключ выбирается в соответствии с табл.1, где *i* — предпоследняя цифра зачетной книжки, *j* — последняя.

Таблица 1

| i, j | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|---|---|
| Элемент ключа | А | Г | Ж | К | Н | Р | У | Ц | Щ | Э |
| | Б | Д | З | Л | О | С | Ф | Ч | Ъ | Ю |
| | В | Е | И | М | П | Т | Х | Ш | Ы | Я |

В том случае, если *i*=*j*, то взять *j*=*i*+1. Например, если последние цифры зачетной книжки 21, то в качестве ключа выбирается следующий набор букв: ЖЗИГДЕ. Если последние цифры совпадают, например 33 (*i*=3, *j*=3); то *j* изменяют: *j*=*i* +1, т.е. *j*=3+1 = 4. Следовательно ключ — КЛМНОП.

Методические указания по решению задачи

Для решения задачи составляется таблица, которая представляет собой квадратную матрицу с числом элементов *k*, где *k* — число символов в алфавите. В первой строке матрицы записываются буквы в порядке очередности их в алфавите, во второй — та же последовательность, но со сдвигом влево на одну позицию, в третьей — со сдвигом на две позиции и т.д. освободившиеся места справа заполняются вытесненными влево буквами, записываемыми в естественной последовательности табл. 2.

Таблица 2

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| А | Б | В | Г | Д | Е | … | Э | Ю | Я |
| Б | В | Г | Д | Е | Ж | … | Ю | Я | А |
| В | Г | Д | Е | Ж | З | … | Я | А | Б |
| Г | Д | Е | Ж | З | И | … | А | Б | В |
| Д | Е | Ж | З | И | К | … | Б | В | Г |
| Е | Ж | З | И | К | Л | … | В | Г | Д |
| … | … | … | … | … | … | … | … | … | … |
| Я | А | Б | В | Г | Д | … | Ь | Э | Ю |

Для шифрования текста устанавливается ключ, представляющий собой некоторое слово или набор букв. Далее из полной матрицы выбирается подматрица шифрования, включающая, например, первую строку и строки матрицы,

начальными буквами которых являются последовательно буквы ключа, например в варианте, указанном выше, строки, начинающиеся с букв Ж, З, И, Г, Д, Е (табл. 3).

Таблица 3

Таблица шифрования

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

Процесс шифрования включает следующую последовательность действий (табл. 4):

– под каждой буквой шифруемого текста записываются буквы ключа, причем ключ повторяется требуемое число раз;

– каждая буква шифруемого текста заменяется на букву, расположенную на пересечении столбца, начинающегося с буквы текста, и строки, начинающиеся с буквы ключа, находящейся под буквой текста.

Так, под первой буквой «З» шифруемого текста оказалась буква «Ж» ключа. На пересечении столбца, начинающегося с «З», и строки, начинающейся с «Ж», находится буква «О» (см табл. 4). Буква «О» будет первой буквой шифрованного текста.

Таблица 4

Механизм шифрования заменой

| Шифруемый текст | З | А | Щ | И | Т | А | | И | Н | Ф | О | Р | М | А | Ц | И | И |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Текст после замены | О | З | Б | М | Ц | Е | | П | Ф | Ь | С | Ф | С | Ж | Э | С | М |

Для расшифровывания необходимо знать ключ. Расшифровка текста выполняется в следующей последовательности (табл. 5.):

– над буквами шифрованного текста сверху последовательно записываются буквы ключа;

– в строке подматрицы таблицы Виженера, начинающейся с буквы ключа, отыскивается буква шифрованного текста; буква первой строки находящаяся в соответствующем столбце, будет буквой расшифрованного текста;

– полученный текст группируется в слова по смыслу.

Таблица 5

Механизм расшифровывания

| Ключ | Ж | З | И | Г | Д | Е | Ж | З | И | Г | Д | Е | Ж | З | И | Г |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Зашифрованный текст | О | З | Б | М | Ц | Е | П | Ф | Ь | С | Ф | С | Ж | Э | С | М |
| Расшифрованный текст | З | А | Щ | И | Т | А | И | Н | Ф | О | Р | М | А | Ц | И | И |

Естественно, что компьютер работает с информацией представленной в битах и на сегодня существуют более совершенные и устойчивые к криптоанализу шифры, которые используют аналогичные принципы замены и перестановки.

Асимметричное шифрование — расшифровывание

RSA (буквенная аббревиатура от фамилий Rivest, Shamir и Adleman) — криптографический алгоритм с открытым ключом. Он стал первым алгоритмом такого типа, пригодным и для шифрования, и для цифровой подписи. Алгоритм используется в большом числе криптографических приложений.

Опубликованная в ноябре 1976 года статья Уитфилда Диффи и Мартина Хеллмана «Новые направления в криптографии» перевернула представление о криптографических системах, заложив основы криптографии с открытым ключом. Разработанный впоследствии алгоритм Диффи-Хеллмана-Меркля позволял двум сторонам получить общий секретный ключ, используя незащищенный канал связи. Однако этот алгоритм не решал проблему аутентификации. Без дополнительных средств, один из пользователей не мог быть уверен, что он обменялся ключами именно с тем пользователем, который ему был нужен.

Изучив эту статью, трое ученых Рональд Райвест (Ronald Linn Rivest), Ади Шамир (Adi Shamir) и Леонард Адлеман (Leonard Adleman) из Массачусетского Технологического Института (MIT) приступили к поискам математической функции, которая бы позволяла реализовать сформулированную Уитфилдом Диффи и Мартином Хеллманом модель криптографической системы с открытым ключом. После работы над более чем 40 возможными вариантами, им удалось найти алгоритм, основанный на различии в том, насколько легко на-

ходить большие простые числа и насколько сложно раскладывать на множители произведение двух больших простых чисел, получивший впоследствии название RSA. Система была названа по первым буквам фамилий её создателей.

Описание RSA было опубликовано в августе 1977 года в журнале Scientific American. Авторы RSA поддерживали идею её активного распространения. В свою очередь, Агентство национальной безопасности (США), опасаясь использования этого алгоритма в негосударственных структурах, на протяжении нескольких лет безуспешно требовало прекращения распространения системы. Ситуация порой доходила до абсурда — например, когда программист Адам Бек (Adam Back) описал алгоритм RSA на языке Perl, состоящий из пяти строк, правительство США запретило распространение этой программы за пределами страны. Люди, недовольные подобным ограничением, в знак протеста напечатали текст этой программы на своих футболках.

Криптографические системы с открытым ключом используют так называемые необратимые функции, которые обладают следующим свойством:

- если известно $x$, то $f(x)$ вычислить относительно просто;
- если известно $y=f(x)$, то для вычисления у нет простого (эффективного) пути.

Под однонаправленностью понимается не теоретическая однонаправленность, а практическая невозможность вычислить обратное значение, используя современные вычислительные средства, за обозримый интервал времени.

В основу криптографической системы с открытым ключом RSA положена задача умножения и разложения составных чисел на простые сомножители, которая является вычислительно однонаправленной задачей.

В криптографической системе с открытым ключом каждый участник располагает как открытым ключом (англ. public key), так и закрытым ключом (англ. private key). Каждый ключ — это часть информации. В криптографической системе RSA каждый ключ состоит из пары целых чисел. Каждый участник создаёт свой открытый и закрытый ключ самостоятельно. Закрытый ключ каждый из них держит в секрете, а открытые ключи можно сообщать кому

угодно или даже публиковать их. Открытый и закрытый ключи каждого участника обмена сообщениями образуют «согласованную пару» в том смысле, что они являются взаимно обратными.

### Алгоритм создания открытого и секретного ключей

RSA-ключи генерируются следующим образом:

1. Выбираются два случайных простых числа $p$ и $q$ заданного размера (например, 1024 бита каждое).
2. Вычисляется их произведение $n = pq$, которое называется модулем.
3. Вычисляется значение функции Эйлера от числа $n$: $f(n)=(p-1)(q-1)$.
4. Выбирается целое число $e$ ($1<e<f(n)$), взаимно простое (целые числа называются взаимно простыми, если они не имеют никаких общих делителей, кроме ±1. Например 14 и 25 взаимно просты, а 15 и 25 не взаимно просты) со значением функции $f(n)$ (обычно в качестве $e$ берут простые числа, содержащие небольшое количество единичных битов в двоичной записи, например, простые числа Ферма 17, 257 или 65537).
5. Вычисляется число $d$, мультипликативно обратное к числу $e$ по модулю $f(n)$, то есть число, удовлетворяющее условию: $de = 1+ k\,f(n)$, где $k$ — некоторое целое число. Можно вычислять и так: $(e*d) \bmod ((p-1)*(q-1))=1$. Результат операции $i \bmod j$ — остаток от целочисленного деления $i$ на $j$, то есть если имеем $(e*3) \bmod 20=1$. Значит $e$ будет, например 7. (Может быть и другим, например 21).
6. Число $e$ называется открытой экспонентой (англ. *public exponent*), а число $d$ называется секретной экспонентой ($d$ и $e$ должны быть различны).
7. Пара $P = (e,n)$ публикуется в качестве открытого ключа RSA (англ. *RSA public key*). Зашифровываем сообщение в соответствии с формулой $C=M'^{e} \bmod n$, где $C$ — зашифрованное сообщение, $M'$ — исходное сообщение, mod — функция вычисляющая остаток от деления.

8. Пара $S=(d,n)$ играет роль секретного ключа RSA (англ. *RSA private key*) и держится в секрете. Расшифровываем сообщение в соответствии с формулой $M'=C^d \bmod n$.

Задача 2

Требуется зашифровать информацию по методу RSA для последующей передачи. Вариант задания определяется последними цифрами номера зачетной книжки (i — предпоследняя; j — последняя) (см. табл. 6). По номеру i студент выбирает слово для зашифровывания, j — требуемые для реализации этого алгоритма числа ($p$, $q$) (на практике эти числа очень большие).

Таблица 6.

| i: | 0. | Беда | 3. | Кабак | 6. | Багдад | j: | 0. | (2,5) | 3. | (2, 17) | 6. | (3,11) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 1. | Дева | 4. | Багаж | 7. | База | | 1. | (2, 7) | 4. | (2,23) | 7. | (2,5) |
| | 2. | Забава | 5. | Бивак | 8. | Диван | | 2. | (2,11) | 5. | (3,5) | 8. | (2,7) |
| | | | | | 9. | Диво | | | | | | 9. | (2,11) |

Дальнейшие действия выполняются в соответствии с алгоритмом шифрования описанным выше.

Методические указания по решению задачи

Шифруемое слово Бег . коэффициенты $p$=3, $q$=11.

Определим $n=pq$=3*11=33. Найдем ($p$-1)(q-1)=20. Выберем e=7 — взаимно простое число, такое, что ($1<e<f(n)$). Найдем число $d$, для которого справедливо ed mod [(p-1)(q-1)]=1 или e$d$=1+$k(p-1)(q-1)$. $d$=3. Функция mod — остаток от деления, в MS «Excel» она называется «ОСТАТ». Представим шифруемое слово в виде последовательности чисел 2 6 4 (см. табл. 7.).

Таблица 7.

Соответствие букв их номеру в алфавите

| Буквы алфавита | А | Б | В | Г | Д | Е | Ж | З | И | К |
|---|---|---|---|---|---|---|---|---|---|---|
| Номер буквы | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |

Шифрование по открытому ключу {e,n} {7, 33}:

$C_1 = 2^7 \bmod (33) = 128 \bmod (33) = 29;$

$C_2 = 6^7 \bmod (33) = 279936 \bmod (33) = 30;$

$C_3 = 4^7 \ mod \ (33) = 16384 \ mod \ (33) = 16.$

Полученное зашифрованное сообщение: 29 30 16

Расшифруем зашифрованное сообщение по секретному ключу {d,n} {3;33}:

$M_1 = 29^3 \ \text{mod} \ (33) = 24389 \ \text{mod} \ (33) = 2;$

$M_2 = 30^3 \ \text{mod} \ (33) = 27000 \ \text{mod} \ (33) = 30;$

$M_3 = 16^3 \ \text{mod} \ (33) = 4096 \ \text{mod} \ (33) = 4.$

В итоге получаем исходное сообщение Бег.

Разница между этим учебным примером и реальной задачей для ЭВМ заключается в том, что для простоты счета информация здесь преобразована не в битовое ее представление (010110), а в числовое в соответствии с номером буквы в алфавите, а значения *p* и *q* взяты гораздо более меньшими, чем обычно.

Система RSA может использоваться не только для шифрования, но и для цифровой подписи. Поскольку цифровая подпись обеспечивает как аутентификацию автора сообщения, так и подтверждение целостности содержимого подписанного сообщения, она служит аналогом подписи, сделанной от руки в конце рукописного документа.

Важное свойство цифровой подписи заключается в том, что её может проверить каждый, кто имеет доступ к открытому ключу ее автора. Один из участников обмена сообщениями после проверки подлинности цифровой подписи может передать подписанное сообщение ещё кому-то, кто тоже в состоянии проверить эту подпись. Например, сторона А может переслать стороне В электронный чек. После того как сторона В проверит подпись стороны А на чеке, она может передать его в свой банк, служащие которого также имеют возможность проверить подпись и осуществить соответствующую денежную операцию.

Заметим, что подписанное сообщение M' не зашифровано. Оно пересылается в исходном виде и его содержимое не защищено. Путём совместного применения представленной выше схемы шифрования и схемы цифровой подписи в системе RSA можно создавать сообщения, которые будут и зашифрованы, и

содержать цифровую подпись. Для этого автор сначала должен добавить к сообщению свою цифровую подпись, а затем — зашифровать получившуюся в результате пару (состоящую из самого сообщения и подписи к нему) с помощью открытого ключа принадлежащего получателю. Получатель расшифровывает полученное сообщение с помощью своего секретного ключа. Если проводить аналогию с пересылкой обычных бумажных документов, то этот процесс похож на то, как если бы автор документа поставил под ним свою печать, а затем положил его в бумажный конверт и запечатал, с тем чтобы конверт был распечатан только тем человеком, кому адресовано сообщение.

### Хеширование сообщений

Хеширование (иногда хэширование, англ. hashing) — преобразование входного массива данных произвольной длины в выходную битовую строку фиксированной длины. Такие преобразования также называются хеш-функциями или функциями свёртки, а их результаты называют хешем, хеш-кодом или дайджестом сообщения (англ. message digest).

Хеширование применяется для сравнения данных: если у двух массивов хеш-коды разные, массивы гарантированно различаются; если одинаковые — массивы, скорее всего, одинаковы. В общем случае однозначного соответствия между исходными данными и хеш-кодом нет в силу того, что количество значений хеш-функций меньше, чем вариантов входного массива; существует множество массивов, дающих одинаковые хеш-коды — так называемые коллизии. Вероятность возникновения коллизий играет немаловажную роль в оценке качества хеш-функций.

Существует множество алгоритмов хеширования с различными характеристиками (разрядность, вычислительная сложность, криптостойкость и т. п.). Выбор той или иной хеш-функции определяется спецификой решаемой задачи. Простейшим примером хеш-функции может служить контрольная сумма.

Хеш-функции применяются:

- сверка данных;

– проверка на наличие ошибок;

– ускорение поиска данных;

– для хранения и передачи пароля (например, когда пароль хешируется с каким-либо переменным параметром и в таком виде передаётся системе аутентификации);

– в алгоритмах ЭЦП для ускорения процесса подписи (подписывается не само сообщение, а его хеш-код).

Задача 3

Получить хеш-код для сообщения по номеру *i*, используя упрощенный вариант хеш-функции X.509 с параметрами по номеру *j*. Вариант задания определяется последними цифрами номера зачетной книжки (*i* — предпоследняя; *j* — последняя, табл. 8). Вектор инициализации $H_0$ следует выбирать самостоятельно.

Таблица 8.

| i: | 0. | Предел | 3. | Модуль | 6. | Ампер-сант | J: | 0. | (3,7) | 3. | (5, 7) | 6. | (11, 5) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 1. | Интеграл | 4. | Плюс | 7. | Корень | | 1. | (13,7) | 4. | (13,5) | 7. | (5,17) |
| | 2. | Минус | 5. | Числитель | 8. | Остаток | | 2. | (3,13) | 5. | (3,17) | 8. | (7,11) |
| | | | | | 9. | Степень | | | | | | 9. | (11,3) |

Хеш-функция на основе рекомендаций МККТТ X.509

Криптостойкость данной функции основана на сложности решения задачи факторизации (разложения на простые множители) известного произведения двух простых чисел *p* и *q* (*p***q*).

Задача разложения числа на простые множители эквивалентна следующей трудно решаемой задаче. Пусть *n*=*p***q*. В этом случае легко вычислить квадрат числа по модулю n $\{X^2(\mathrm{mod}\ n)\}$. Однако вычислительно трудно извлечь корень по этому модулю. На этом основании хеш-функция X.509 записывается следующим образом:

$H_i=[(H_i\text{-}1+M_i)^2]\ (\mathrm{mod}\ n)$,

где $i=1,n$, $H_0=i=0$, $M= M_1, M_2, M_3 \ldots M_n$

$H_0$ — вектор инициализации выбирается случайным образом.

Порядок вычисления хеш-функции следующий:

1. Выбираются два простых числа $p$, $q$ и вычисляется их произведение.

2. Каждая буква хешируемого слова представляется в виде цифр соответствующих положению буквы в алфавите ($M_1$, $M_2$, $M_3$ …$M_n$).

3. В каждой последующей итерации $H_i$ используется значение предыдущего вычисления $H_{i-1}$ и следующая буква слова $M_i$ в цифровом эквиваленте.

Методические указания по решению задачи 3

Хешируемое слово ДВА. Коэффициент $p$=7, $q$=3. Вектор инициализации $H_o$ выберем равным 9 (выбираем случайным образом). Слово «ДВА» в числовом эквиваленте можно представить как 531 (по номерам букв в алфавите). Тогда хеш-код сообщения 531 получается следующим образом:

1-ая итерация:

$M_1 + H_o = 5 + 9 = 14$; $[M_1 + H_o]^2 \bmod (21) = 14^2 \bmod (21) = 7 = H_1$;

2-ая итерация:

$M_2 + H_1 = 3 + 7 = 10$; $[M_2 + H_1]^2 \bmod (21) = 10^2 \bmod (21) = 16 = H_2$;

3-ая итерация:

$M_3 + H_2 = 1 + 16 = 17$; $[M_3 + H_2]^2 \bmod (21) = 17^2 \bmod (21) = 16 = H_3$;

В итоге получаем хеш-код сообщения «ДВА», равный 16.

В оригинальном алгоритме компьютерная программа работает с массивом битов, а полученное хеш-значение обычно несколько длинней полученного в учебном примере и выглядит например так:
92C2517532C627BCE1413ED464BE160B09894E4F.

## СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

1. Становление и развитие информационного общества.

История развития информационного общества. Понятие и основные черты информационного общества. Влияние информатизации на жизнь.

2. Понятие информации и её свойства.

Подходы к пониманию информации с точки зрения теории информации, кибернетики, законодательства. Особенности и виды информации. Свойства информации.

3. Информационная система.

Определение и состав информационной системы. Параметры информационной системы.

4. Информационная безопасность и безопасность информации.

Определение безопасности информации и информационной безопасности их типичные задачи и направления защиты. Доктрина информационной безопасности РФ. Типичные угрозы информационной безопасности и безопасности информации.

5. Виды информации по условиям защиты (конфиденциальная информация).

Сведения конфиденциального характера: коммерческая, налоговая, банковская, государственная тайны, персональные данные, служебные тайны и т. д. Законодательное обеспечение защиты.

6. Источники конфиденциальной информации (люди, публикации, документы, продукция, технические средства обработки информации, отходы), действия приводящие к незаконному овладению информацией (разглашение, утечка, несанкционированный доступ) и способы защиты.

7. Управление рисками. Виды рисков и классификация. Управление рисками.

Статические и динамические, страхуемые и не страхуемые риски. Процесс управления рисками.

8. Виды угроз и концепция защиты.

Принципы построения системы защиты. Оценка чистых рисков. Экспертный и статистический методы оценки.

9. Виды противников и нарушителей. Социальная инженерия, определение, виды, способы защиты: антропогенный и технический.

10. Вредоносные программы. Способы защиты.

Определение вредоносной программы. Виды: компьютерные вирусы и их типы и принципы действия. Способы защиты. Принципы работы антивирусов.

11. Понятие и виды аутентификации.

Определение аутентификации. Виды: пароль, одноразовый пароль, карты памяти, смарт-карты, биометрические технологии (принципы работы, надежность, возможные виды атак).

12. Криптография. Симметричные криптосистемы.

История криптографии, определение, основные термины. Определение симметричной криптосистемы, общие принципы работы, основные характеристики, достоинства и недостатки, возможные атаки. Правовой статус криптографии.

13. Асимметричные криптосистемы, электронная-цифровая подпись.

Определение асимметричной криптосистемы, общие принципы работы, основные характеристики, достоинства и недостатки. Определение ЭЦП, принцип работы, характеристики, возможные атаки. Применение. Правовой статус. Инфраструктура обеспечения достоверности. Сертификаты и удостоверяющие центры.

14. Хеширование. Стеганография.

Определение, принцип работы, применение.

15. Правовые аспекты защиты информации. Авторское право. Технические средства защиты авторских прав.

Нормы определяющие порядок документирования информации. Нормы, регулирующие право собственности на информацию и информационные ресурсы. Нормы определяющие порядок доступа к информации. Нормы определяющие порядок защиты информации. Правовая охрана программ и баз данных.

## ВОПРОСЫ К ЭКЗАМЕНУ

1. Становление информационного общества (история, последствия).
2. Подходы к определению информации и её свойства.
3. Определение и состав информационной системы. Параметры обеспечиваемые информационной системой.
4. Понятия информационной безопасности и безопасности информации. Различие и типичные угрозы.
5. Виды информации по условиям ее защиты. Конфиденциальная информация, виды тайн. Требования к обеспечению безопасности конфиденциальной информации.
6. Источники информации и способы несанкционированного доступа.
7. Управление рисками. Виды рисков и их классификация.
8. Виды угроз и принципы построения системы защиты.
9. Виды противников и нарушителей. Социальная инженерия.
10. Вредоносные программы. Способы защиты.
11. Понятие и виды аутентификации (пароль, одноразовый пароль, карты памяти, смарт-карты, биометрические технологии).
12. Криптография. Симметричные криптосистемы.
13. Асимметричные криптосистемы, электронная-цифровая подпись.
14. Хеширование. Стеганография.
15. Авторское право.
16. Технические средства защиты авторских прав.

МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ

1. Галатенко В. А. Основы информационной безопасности: курс лекций: учебное пособие / Издание третье / Под редакцией академика РАН В. Б. Бетелина / — М.: ИНТУИТ.РУ «Интернет университет информационных технологий», 2006. — 208 с.

2. Корнеев И. К., Степанов Е. А. Защита информации в офисе: учеб. — М.: ТК Велби, Изд. Проспект, 2008. — 336 с.

3. Куприянов А. И. Сахаров А. В., Швецов В. А. Основы защиты информации: учеб. пособие для студ. высш. учеб. заведений. — М.: Издательский центр «Академия», 2006. — 256 с.

4. Курило А. П., Зефиров С. Л., Голованов В. Б. и др. Аудит информационной безопасности — М.: Издательская группа «БДЦ-пресс», 2006. —304 с.

5. Мельников В. П., Клейменов С. А., Петраков А. М. Информационная безопасность и защита информации: учеб. пособие для студ. высш. учеб. заведений — 3-е изд., стер. — М.: Издательский центр «Академия», 2008. — 336 с.

6. Панасенко С. П., Батура В. П. Основы криптографии для экономистов: Учеб. пособие. — М.:Финансы и статистика, 2005. — 176 с.: ил.

7. Партыка Т. Л., Попов И. И. Информационная безопасность: учебное пособие для студентов учреждений среднего профессионального образования. — 3-е изд., перераб. и доп. — М.: ФОРУМ, 2008 — 432 с. : ил. (Профессиональное образование).

8. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие. — М.: ИД «Форум» : ИНФРА-М, 2008. — 416 с.: ил. — (Профессиональное образование).

9. Щербаков А. Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты.: учебное пособие. — М.: Книжный мир, 2009. — 352 с.

10. Ярочкин В. И. Информационная безопасность: учеб. — 3-е изд. — М.: Академический Проект: Трикста. — 2005. — 544 с. — («Gaudeamus»).