Подготовка к XXXIII Межрегиональной олимпиаде школьников по математике и криптографии

Региональный школьный технопарк

Преподаватель Лим В.Г.

г. Астрахань 2023 г.

Элементарное введение в современную криптографию

Лим Владимир Григорьевич

Педагог дополнительного образования Регионального школьного технопарка

Доцент кафедры «Информационная безопасность» АГТУ

Элементарное введение в современную криптографию

Что такое криптография

Криптография - *наука о защите данных*

- *о способах передачи информации между двумя сторонами, чтобы она не стала известна третьей стороне*
- *о методам преобразрвания информации, обеспечивающих невозможность понять смысл сообщения в случае перехвата сообщения третьей стороной*

Что такое криптография - 2

Криптография («криптос» - тайна, «графэйн» - писать) - *наука о методах обеспечения*

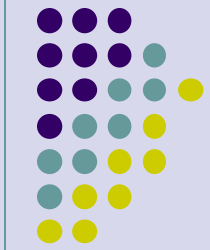
- *конфиденциальности (невозможности прочтения информации посторонним)*
- *аутентичности (целостности и подлинности авторства, а также невозможности отказа от авторства) информации.*

Для чего нужна криптография

Криптография позволяет:

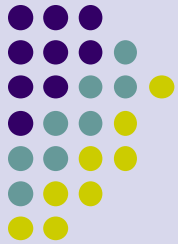
- *Предотвратить угрозы потери конфиденциальности информации, обеспечивая безопасность информации и связи с помощью правил, которые позволяют получать данные и обрабатывать их только тем, кто имеет соответствующий доступ.*
- *Обеспечить безопасную отправку паролей по сетям при совершении покупок в интернете.*

Криптографические алгоритмы и криптографические протоколы



- ***Криптографический алгоритм*** *- набор правил, который используется для шифрования информации, чтобы ее могли прочитать только авторизованные стороны. Алгоритм позволяет генерировать зашифрованный текст, который невозможно прочитать без расшифровки.*
- ***Криптографические протоколы*** *– это некие ритуалы, сценарии, правила, описывающие, как две стороны общаются между собой и могут обмениваться информацией с учетом обеспечения её конфиденциальности. Это сценарии действий двух сторон.*

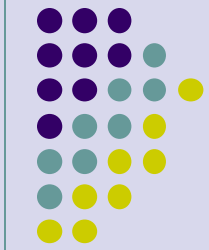
Понятие криптографического протокола



Криптографический протокол – это такой протокол, в котором используются криптографические алгоритмы и который служит для решения некоторой криптографической задачи, например, обеспечивает целостность, секретность, аутентичность информации.

Компонентами криптографического протокола являются **участники протокола**, **каналы связи** между участниками, а также либо **алгоритмы**, используемые участниками, либо **постановка той задачи**, которую протокол призван решать.

Основные разделы современной криптографии



Современная криптография включает в себя следующие основные разделы:

1. Симметричные криптосистемы
2. Криптосистемы с открытым ключом
3. Системы электронной подписи
4. Управление ключами
5. Протоколы установления подлинности (аутентификации).

Приведенный список неполон, так как на данный момент существуют десятки видов криптографических протоколов, не направленных непосредственно на шифрование данных или обмен ключами.

Схема тайной передачи информации

Как Алисе и Бобу общаться втайне от Евы?

Ева

Хочет знать все секреты. Подслушивает, но не влияет на сообщения.

Это Алиса

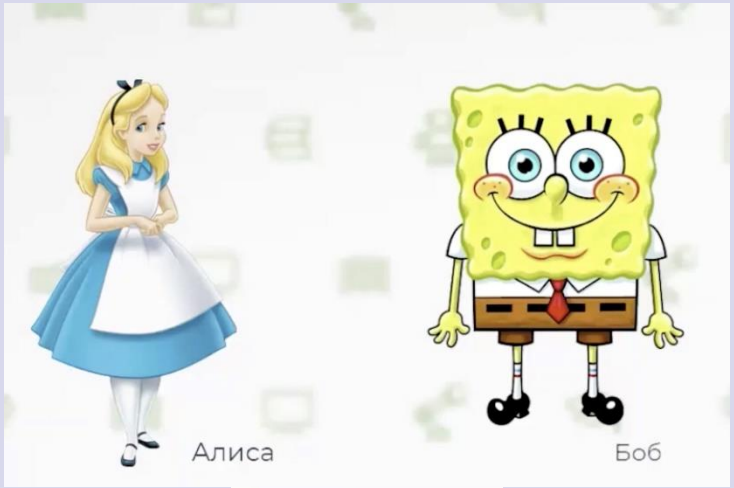
Она хочет отправить Бобу секретное сообщение.

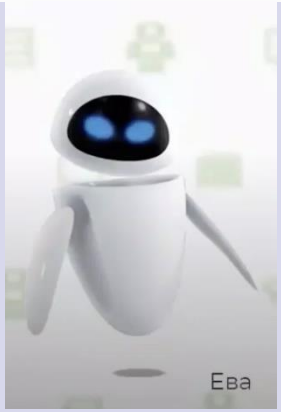
Это Боб

Боб хочет ответить Алисе.

Алиса, Боб и Ева

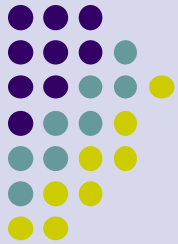
Как Алисе и Бобу общаться втайне от Евы?





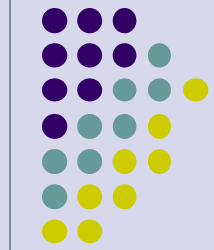
Ключи шифрования

Почему выбор ключей шифрования так важен



Очень **важно правильно выбирать ключи шифрования** – даже самые стойкие и продуманные шифры могут стать уязвимыми, если неправильно выбрать ключ шифрования или позволить украсть его злоумышленнику. Поэтому, чтобы шифрование действительно оправдало ожидания и обеспечило секретность сообщения, нужно правильно выбрать и заранее обговорить секретный ключ.

Основные типы ключей (глоссарий)

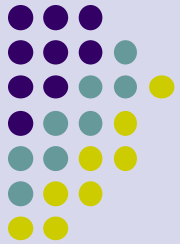


- Сессионный (сеансовый) ключ - применяется для одного сеанса связи. Уничтожается в короткий промежуток времени (от нескольких секунд до одного дня). Сеансовый ключ обеспечивает секретность одного диалога: если он попадет под угрозу, будет нарушена конфиденциальность одного сеанса, но не всей системы в целом.
- Долговременный ключ - используется в течение долгого периода времени (от нескольких часов до нескольких лет, в зависимости от назначения). Его компрометация ставит под угрозу всю систему и является большой проблемой.
- Открытый ключ - применяется в асимметричных криптосистемах шифрования, то есть системах, где для шифрования и расшифровки требуются разные ключи. Обычно исаользуется для проверки электронной подписи.
- Секретный ключ — используется криптографическим алгоритмом при шифровании/расшифровке сообщений и формировании электроной подписи.

Глоссарий (продолжение)

- Распределение ключей - последовательность действий по выработке участниками общих ключей для осуществления криптографических операций.
- Симметричное шифрование - это способ шифрования данных, при котором один и тот же ключ используется и для кодирования, и для восстановления информации. До 1970-х годов, когда появились первые асимметричные шифры, оно было единственным криптографическим методом.
- Асимметричное шифрование - это метод **шифрования** данных, предполагающий использование двух ключей - открытого и закрытого. Открытый (публичный) ключ применяется для **шифрования** информации и может передаваться по незащищенным каналам. Закрытый (приватный) ключ применяется для расшифровки данных, зашифрованных открытым ключом.

Неформальное сравнение симметричной и асимметричной систем шифрования



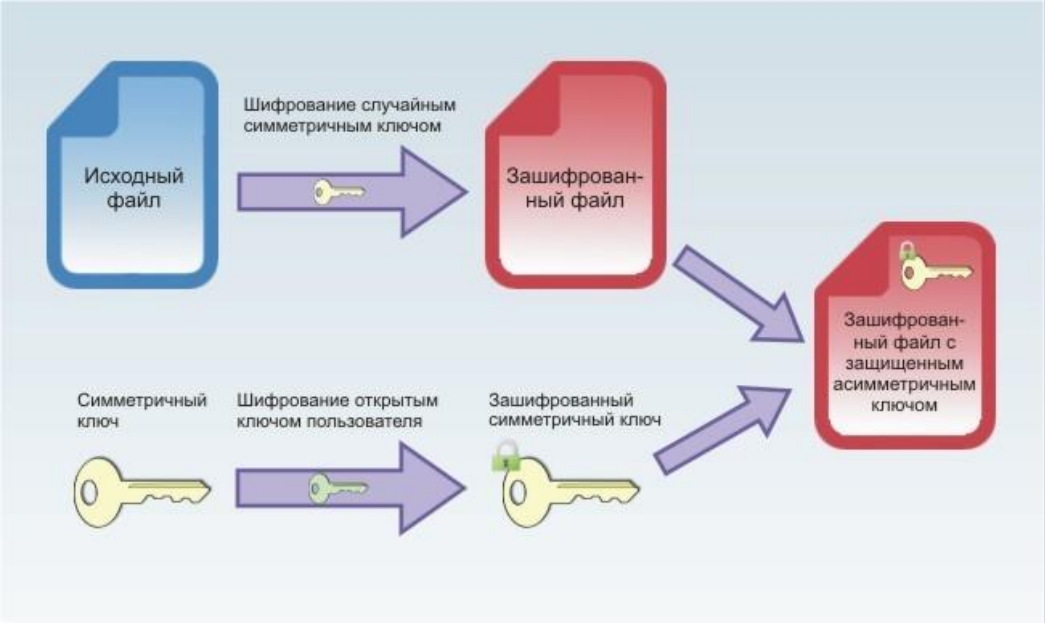
- Чтобы лучше понять симметричное и асимметричное шифрование, рассмотрим следующую ситуацию. Мы хотим отправить секретное сообщение с личными данными в банк. Для этого банк выдает нам коробку и ключ. Необходимо положить письмо в коробку и закрыть ее на ключ, банк при получении открывает эту коробку с помощью аналогичного (симметричного) ключа. Такой метод является симметричным, так как обе стороны используют один и тот же ключ для шифрования и расшифрования.
- Однако злоумышленник может перехватить ключ и открыть коробку. Чтобы это предотвратить, банк поступает следующим образом: он предоставляет нам коробку и навесной замок (который можно закрыть защёлкиванием), а единственный ключ банк хранит у себя. Таким образом, воспользоваться замком и закрыть замок может кто угодно, но открыть коробку может только обладатель ключа. Такой подход называется асимметричным: замок играет роль открытого (публичного) ключа, а ключ банка - секретного (приватного).

Технология «Цифрового конверта»

Технология «Цифрового конверта» - 2

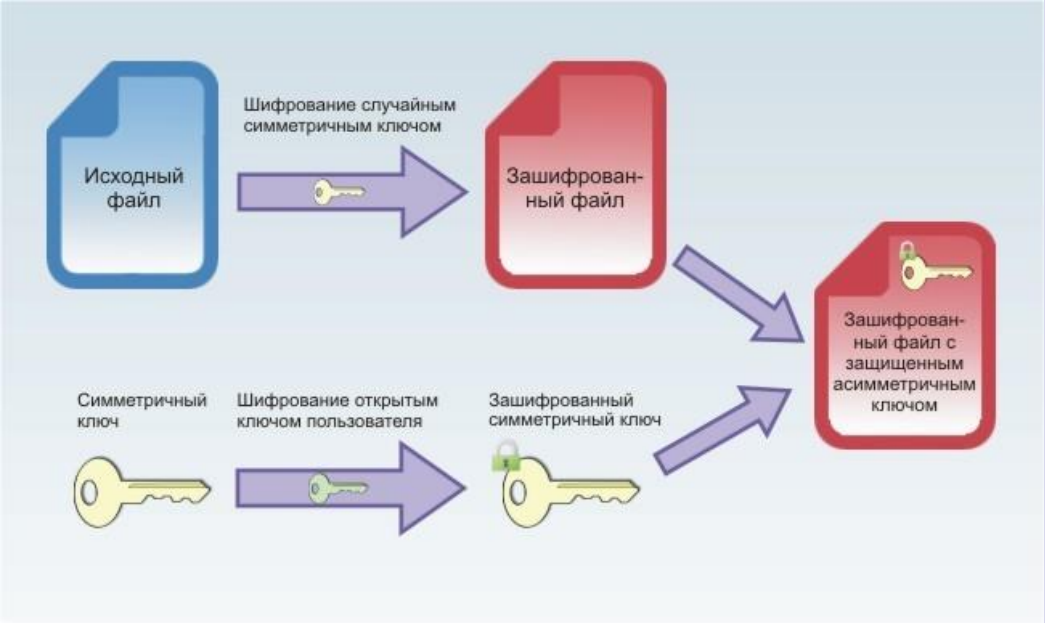
- Прозрачное шифрование работает следующим образом. Для шифрования файла используется случайно сгенерированный симметричный сеансовый ключ, который в свою очередь защищается при помощи открытого асимметричного ключа пользователя. Если пользователь обращается к файлу для того, чтобы внести в него какие-то изменения, драйвер прозрачного шифрования расшифровывает симметричный ключ при помощи закрытого (приватного) ключа пользователя и далее, при помощи симметричного ключа, расшифровывает сам файл.
- Как видно из рисунка, цифровой конверт содержит файл, зашифрованный при помощи случайно сгенерированного симметричного ключа, а также несколько копий этого симметричного ключа, защищенных при помощи открытых асимметричных ключей каждого из пользователей. Копий будет столько, скольким пользователям разрешен доступ к защищенной папке.

Технология «Прозрачного шифрования» файлов в Windows. Этап шифрования



- исходный файл шифруется с использованием алгоритма AES и случайно сгенерированного программой симметричного ключа длиной 256 бит;
- симметричный ключ защищается шифрованием по алгоритму RSA при помощи открытого ключа пользователя длиной до 8192 бит и сохраняется в альтернативном потоке данных NTFS.

Технология «Прозрачного шифрования» файлов в Windows. Автоматическое расшифрование



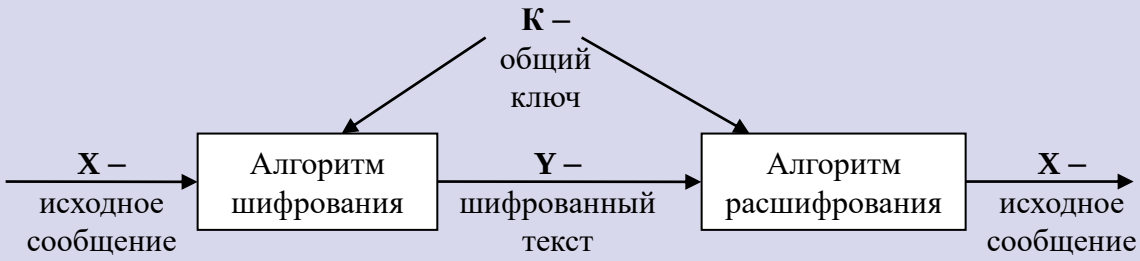
При работе пользователя с файлом во время обращения к нему соответствующего приложения файл автоматически расшифровывается по следующей схеме:

при помощи закрытого ключа пользователя, расшифровывается хранящийся в ADS симметричный ключ;

- при помощи симметричного ключа расшифровывается исходный файл.

Понятие симметричной криптосистемы

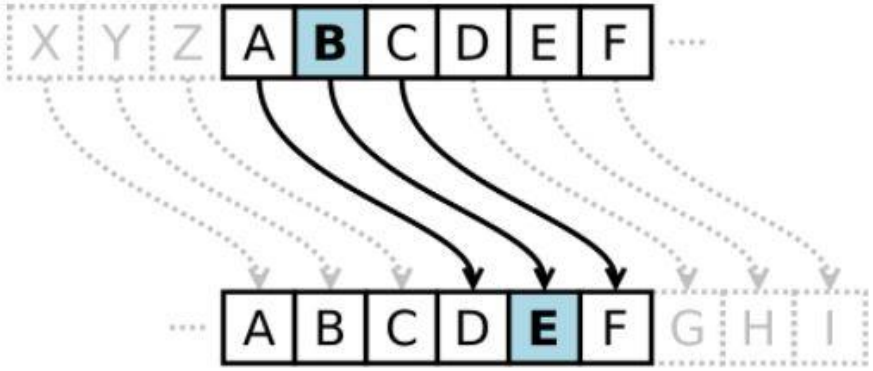
Симметричная криптосистема, или **криптосистема с секретным ключом**, или **двухключевая криптосистема** – система, при которой и шифрование, и расшифрование производятся с использованием одного и того же ключа. Ключ должен быть известен только отправителю и получателю. (необходима секретность ключа).



Шифр Цезаря

Шифр Цезаря — это вид шифра подстановки, в котором каждый символ в открытом тексте заменяется символом, находящимся на некотором постоянном числе позиций левее или правее него в алфавите.
Шифр назван в честь римского полководца Гая Юлия Цезаря, использовавшего его для секретной переписки со своими генералами.

Например, в шифре со сдвигом вправо на 3, A была бы заменена на D, B станет E, Z станет C, и так далее.



Алгоритм шифрования можно выразить следующими формулами:

$y = (x + k) \bmod n$

$x = (y - k) \bmod n$

где x — символ открытого текста, y — символ шифрованного текста, n — мощность алфавита, а k — ключ.

Шифр Цезаря

0.А	1.Б	2.В	3.Г	4.Д	5.Е	6.Ё	7.Ж	8.З	9.И	10.Й
11.К	12.Л	13.М	14.Н	15.О	16.П	17.Р	18.С	19.Т	20.У	21.Ф
22.Х	23.Ц	24.Ч	25.Ш	26.Щ	27.Ъ	28.Ы	29.Ь	30.Э	31.Ю	32.Я

Встретимся завтра утром

Ключ: 10

Лыьъоьтцыи сйльъй эьъшц

Щифр (криптосистема) –

Шифр Цезаря

0.А	1.Б	2.В	3.Г	4.Д	5.Е	6.Ё	7.Ж	8.З	9.И	10.Й
11.К	12.Л	13.М	14.Н	15.О	16.П	17.Р	18.С	19.Т	20.У	21.Ф
22.Х	23.Ц	24.Ч	25.Ш	26.Щ	27.Ъ	28.Ы	29.Ь	30.Э	31.Ю	32.Я

Встретимся завтра утром

Ключ: 10

Лыьъоьтцыи сйльъй эьъшц

Шифр (криптосистема) –

C(x)=(X+K)(MOD 32)

X – открытый текст

C(X) – шифртекст, K - ключ

Каждому символу открытого текста соответствует значение символа алфавита со смещением на величину K. Результат должен быть не больше 32, т.е. по модулю 32

Шифр Виженера

Шифр, задаваемый формулой

$$Y_i = X_i + k_i (\mathrm{mod}\ N),$$

где k_i – i-ая буква ключа, в качестве которого используются слово или фраза, называется *шифром Вижинера*.

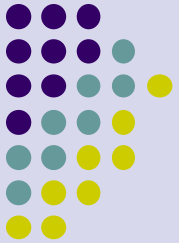
Пример. Открытый текст: «ЗАМЕНА». Ключ: «КЛЮЧ».

Таблица 5.3

Шифрование методом Вижинера [10]

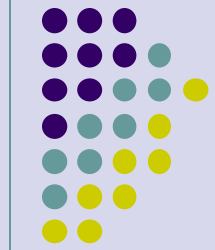
Открытый текст	Ключ	Преобразование	Шифр
З	К	y_1=8+11(mod 33)=19	Т
А	Л	y_2=1+12(mod 33)=13	М
М	Ю	y_3=13+31(mod 33)=11	К
Е	Ч	y_4=6+24(mod 33)=30	Э
Н	К	y_5=14+11(mod 33)=25	Ш
А	Л	y_6=1+12(mod 33)=13	М

Шифрованный текст: «ТМКЭШМ».



Модульная арифметика

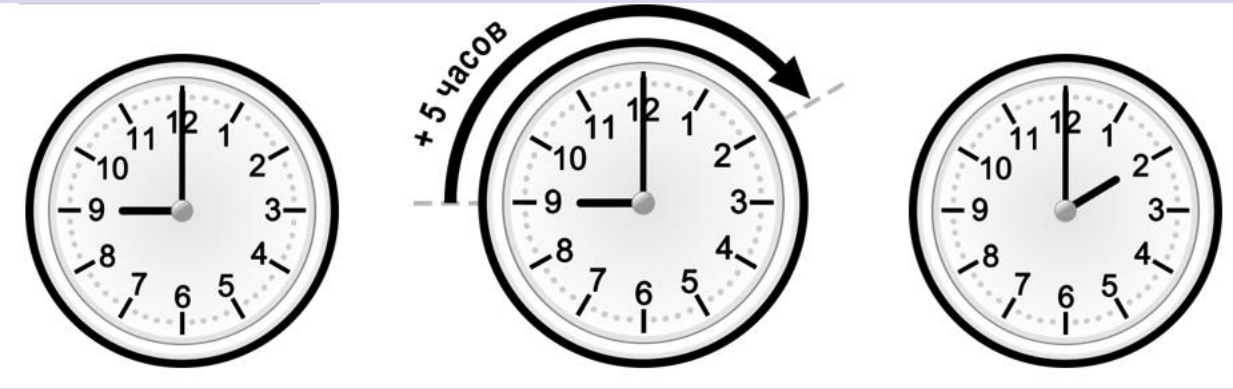
Арифметика часов - введение



- В школе вы научились использовать часы. Вас учили, что если в настоящее время стрелки часов показывают 9 утра, то через 12 часов они будут показывать то же самое время.
- На самом деле это разное время суток, но часы «не знают» этого. Таким образом, часы будут показывать одно и то же через 12 часов, 24 часа и любой кратный 12 часам отрезок времени в будущем или в прошлом, независимо от того, какое время на самом деле.

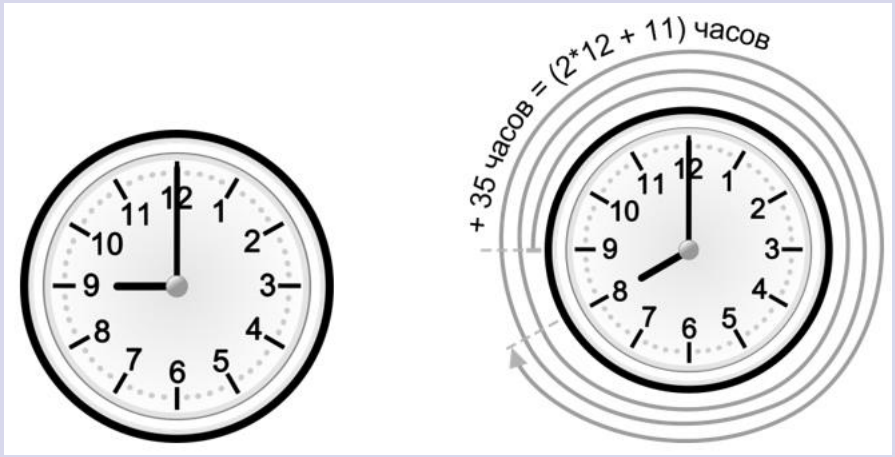
Арифметика часов - пример 1 Добавление 5 часов к 9 часам

- Вы освоили это как «арифметику часов». Если часы показывают 9 часов (не имеет значения, утра или вечера) и вы хотите узнать время через 5 часов, вы определите, что 9 + 5 = 14. Поскольку на циферблате нет 14 часов, вы должны вычесть 12 и получить 2 часа.

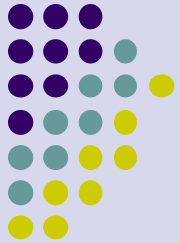


Арифметика часов - пример 2
Добавление 35 часов к 9 часам

- Если сейчас 9 часов, и вас интересует время через 35 часов, вы можете найти 9 + 35 = 44.
- Теперь последовательно вычитайте 12, пока не получите число в пределах от 1 до 12:
- 44 – 12 = 32; 32 – 12 = 20; 20 – 12 = 8.
- То есть через 35 часов ваши часы будут показывать 8 часов

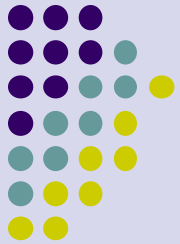


Арифметика часов - пример 3 Добавление 1000 часов к 9 часам



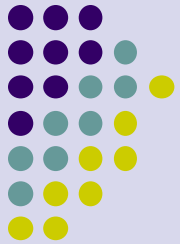
- Но предположим, что сейчас 9 часов, и вас интересует время через 1000 часов. Сложите 9 + 1000 и вы получаете 1009.
- Вы можете последовательно вычитать 12, но это довольно скучно и утомительно. Есть более простой способ. Подумайте, какой?

Арифметика часов - пример 3 Добавление 1000 часов к 9 часам



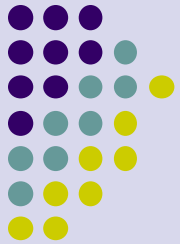
- Но предположим, что сейчас 9 часов, и вас интересует время через 1000 часов. Сложите 9 + 1000 и вы получаете 1009.
- Вы можете последовательно вычитать 12, но это довольно скучно и утомительно. Есть более простой способ. Подумайте, какой?
- Просто разделите 1009 на 12. Нас не интересует частное. Нас интересует остаток.
- 1009/12 = 84 и 1 в остатке.
- Так как остаток равен 1, то через 1000 часов наши часы будут показывать 1 час.
- Рассмотренная система называется модульной.

Модульные вычисления и конгруэнтность



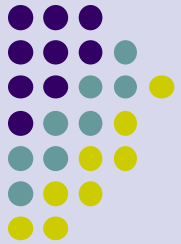
- Таким образом, при использовании часов мы можем добавить 12 или вычесть 12 из любого числа, не меняя его. Мы можем записать следующие утверждения:
- $13 \equiv 1 \bmod 12$, $25 \equiv 1 \bmod 12$, $37 \equiv 1 \bmod 12$, $-11 \equiv 1 \bmod 12$, $-23 \equiv 1 \bmod 12$ ...
- Первое утверждение читается как «13 является конгруэнтным (или эквивалентным) 1 в модульной системе 12» или «13 равно 1 по модулю 12». Что также означает, что 13 - 1 делится без остатка на 12.
- Второе утверждение $25 \equiv 1 \bmod 12$ говорит, что 25 - 1 делится без остатка на 12.
- Утверждение $-11 \equiv 1 \bmod 12$ говорит, что -11 - 1 делится на 12 без остатка. (mod читается как «по модулю»).

Использование модульной арифметики



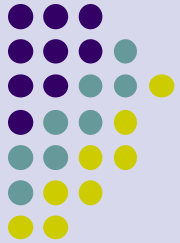
- Когда мы используем модульную систему с основанием 12, мы хотим выразить наши числа, используя наименьшие неотрицательные числа. Поэтому мы будем использовать числа от 0 до 11 (в отличие от часов, в которых числа от 1 до 12).
- Поэтому мы говорим, что 12 ≡ 0 mod 12 или 12 - 0 делится без остатка на 12.
- Если вы хотите изменить число так, чтобы оно было по модулю 12, вам надо разделить это число на 12 и посмотреть на остаток. Некоторые калькуляторы имеют клавишу «mod». Чтобы найти 77 mod 12, вы набираете mod (77, 12). Без такого калькулятора вычисление модуля становится проблемой, но вы можете упростить ситуацию.

Примеры применения модульной арифметики



- Например, если вы хотите найти 1234 mod 12, вместо деления вы можете рассуждать следующим образом: близкое к 1234 число, кратное 12, равно 1200. Так что, вы можете записать 1234 ≡ 34 mod 12. А поскольку 24 = 2*12, вы можете вычесть 24 из 34. В результате вы получаете 10. Итак можно заключить, что 1234 ≡ 10 mod 12.
- Если вы хотите найти 185 mod 12, вы можете вспомнить, что 122 = 144. Вычитайте 144 из 185 и вы получите 41. Поскольку 41 на 5 больше, чем 36 (=3*12), вы можете сделать вывод, что 185 ≡ 5 mod 12.

Работа в других модульных системах



- Вы можете работать и в других модульных системах. Если надо найти 79 mod 5, вы можете сообразить, что 75 = 15*5. Вычитайте 75 из 79 и вы поймете, что 79 ≡ 4 mod 5.
- Если вы хотите найти 8024 mod 8, вы можете сообразить, что 8024 кратно 8. Следовательно, 8024 ≡ 0 mod 8.

Задачи для самостоятельного решения

- Найдите:
- 321 mod 12 _____
- 321 mod 7 _____
- 576 mod 9 _____
- 885 mod 3 _____

357 mod 14 _____

87562 mod 21 _____

653 mod 4 _____

983 mod 5 _____

Задачи для самостоятельного решения

- Найдите:
- $321 \equiv 9 \bmod 12$
- $321 \equiv 6 \bmod 7$
- $576 \equiv 0 \bmod 9$
- $885 \equiv 0 \bmod 3$

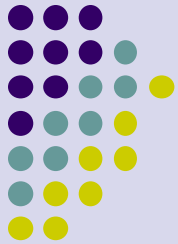
$357 \equiv 7 \bmod 14$

$87562 \equiv 13 \bmod 21$

$653 \equiv 1 \bmod 4$

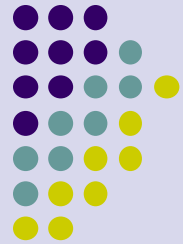
$983 \equiv 3 \bmod 5$

Использование модульной арифметики для системы шифрования русских текстов



- В системах шифрования, которые мы будем рассматривать, естественно использовать систему mod 33 для русских текстов и mod 26 для английских текстов. 0 будет соответствовать А (A), 1 – Б (B), 2 – В (C), ... Так как в системе mod 33 мы используем числа от 0 до 32, то числа 33 не будет. $33 \equiv 0 \bmod 33$.
- Таким образом, аддитивная система добавляет свой ключ к номеру буквы по модулю 33 (по модулю 26 для английских текстов). Если буквой в открытом тексте является «к», а ключ равен 18, то мы сначала определяем, что позиция буквы «к» равна 11 и затем добавляем к ней 18. Получаем 29, что соответствует букве «Ь».

Использование модульной арифметики для системы шифрования русских текстов - 2



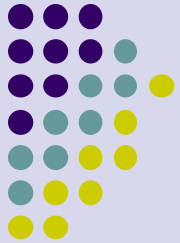
- Если буква открытого текста – «ф», а ключ – 19, мы добавляем 19 к позиции «ф», равной 21, и получаем 40. Далее находим 40 mod 33, равный 7, что соответствует букве «Ж».
- Если буква открытого текста – «у», а ключ – 13, мы добавляем 13 к позиции «у»", равной 20, и получаем 33. Далее находим 33 mod 33, который равен 0, что соответствует «А».

Использование модульной арифметики для расшифровки русских текстов

- Чтобы расшифровать мы должны выполнить обратный процесс. Если ключ был 7, то при шифровании мы добавили 7 к позиции каждой буквы открытого текста. Чтобы расшифровать, нам нужно вычесть 7. Но в модульных системах мы предпочитаем не использовать операцию вычитания. Так, учитывая, что -7 ≡ 26 mod 33, мы добавим 26 по модулю 33 к позиции каждой буквы шифротекста

15																
16	а	б	в	г	д	е	ё	ж	з	ы	ь	э	ю	я	Буквы алфавита	
17	0	1	2	3	4	5	6	7	8	28	29	30	31	32	Позиции букв	
18	7	8	9	10	11	12	13	14	15	35	36	37	38	39	Добавить	7
19	7	8	9	10	11	12	13	14	15	2	3	4	5	6	Позиции букв шифротекста	
20	Ж	З	И	Й	К	Л	М	Н	О	В	Г	Д	Е	Ё	Буквы шифротекста	
21																

Понятие аддитивного инверсного ключа



- Мы будем называть ключ расшифровки «аддитивным инверсным». Аддитивная инверсия 7 равна 26 mod 33.
- Если ключ был 24, то ключ расшифровки равен - 24. Но - 24 ≡ 9 mod 33. Итак, мы добавляем 9 по модулю 33 к каждой позиции букв в зашифрованном тексте. Таким образом, аддитивная инверсия 24 равна 9 mod 33.
- Найдите аддитивные инверсии для mod 33:

  23: _____ 40: _____ 1: _____

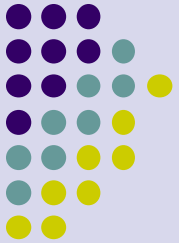
  548: _____ 300: _____

Нахождение аддитивного инверсного ключа - ответы

- Найдите аддитивные инверсии для mod 33:

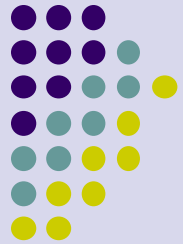
  23: 10 mod 33 40: 26 mod 33 1: 32 mod 33

  548: 13 mod 33 300: 30 mod 33



Мультипликативный шифр

Мультипликативная система шифрования



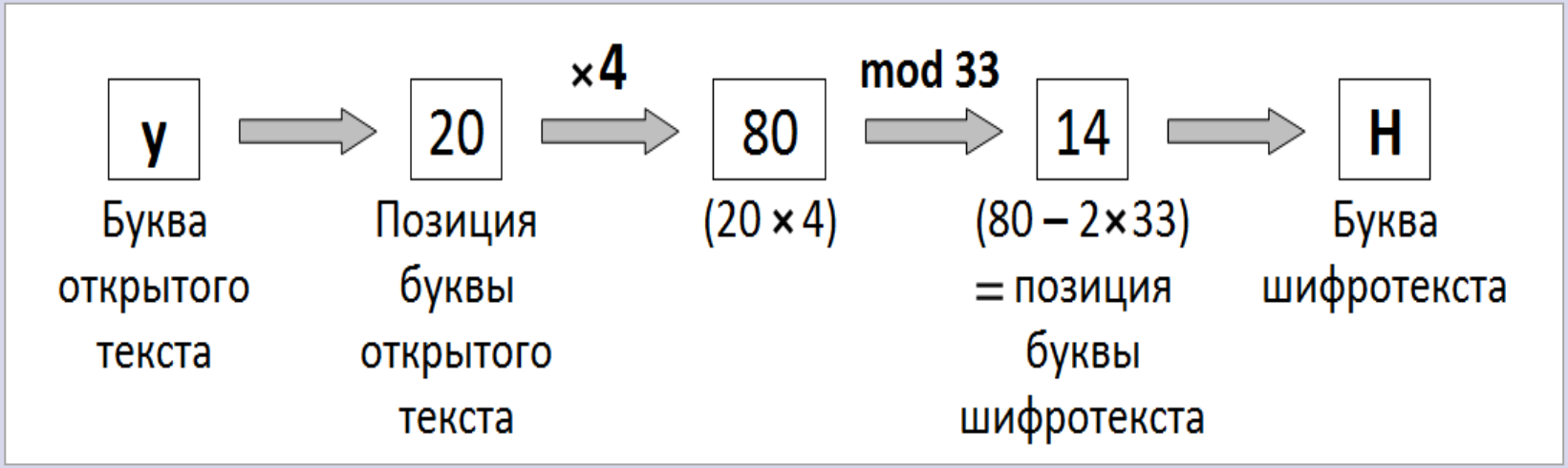
- Вместо добавления ключа к позициям букв открытого текста, мы просто умножаем его на номер позиции открытого текста.
- Формула для вычисления позиции C буквы зашифрованного текста на основе ключа k и буквы открытого русского текста в позиции P имеет следующий вид:

$$C = kP \bmod 33$$

- Для английских текстов формула имеет вид

$$C = kP \bmod 26.$$

Преобразование буквы «у» мультипликативным ключом, равным 4



Реализация мультипликативного шифра с ключом 4

Итак, если наш ключ равен 4, то для создания зашифрованного текста будет использоваться следующая таблица:

Буквы открытого текста	а	б	в	г	д	е	ё	ж	з	и	й
Позиции букв	0	1	2	3	4	5	6	7	8	9	10
Умножить на 4	0	4	8	12	16	20	24	28	32	36	40
mod 33	0	4	8	12	16	20	24	28	32	3	7
Буквы шифрованного текста	А	Д	З	Л	П	У	Ч	Ы	Я	Г	Ж

На слайде мы видим начало таблицы

Реализация мультипликативного шифра с ключом 4 - продолжение

На слайде мы видим продолжение таблицы.

Буквы открытого текста	к	л	м	н	о	п	р	с	т	у	ф
Позиции букв	11	12	13	14	15	16	17	18	19	20	21
Умножить на 4	44	48	52	56	60	64	68	72	76	80	84
mod 33	11	15	19	23	27	31	2	6	10	14	18
Буквы шифрованного текста	К	О	Т	Ц	Ъ	Ю	В	Ё	Й	Н	С

Буквы открытого текста	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я
Позиции букв	22	23	24	25	26	27	28	29	30	31	32
Умножить на 4	88	92	96	100	104	108	112	116	120	124	128
mod 33	22	26	30	1	5	9	13	17	21	25	29
Буквы шифрованного текста	Х	Щ	Э	Б	Е	И	М	Р	Ф	Ш	Ь

Таким образом, мультипликативный шифр с ключом, равным 4, сообщение «**Электронная цифровая подпись**» преобразует к виду: **ФОУКЙВЪЦЦАЬЩГСВЪЗАЬЮЪПЮГЁР**

Реализация мультипликативного шифра с ключом 3

Итак, если наш ключ равен 3, то для создания зашифрованного текста будет использоваться следующая таблица:

Буквы открытого текста	а	б	в	г	д	е	ё	ж	з	и	й
Позиции букв	0	1	2	3	4	5	6	7	8	9	10
Умножить на 3	0	3	6	9	12	15	18	21	24	27	30
mod 32	0	3	6	9	12	15	18	21	24	27	30
Буквы шифрованного текста	А	Г	Ё	И	Л	О	С	Ф	Ч	Ъ	Э

На слайде мы видим начало таблицы

Реализация мультипликативного шифра с ключом 3 - продолжение

На слайде мы видим продолжение таблицы.

Буквы открытого текста	к	л	м	н	о	п	р	с	т	у	ф
Позиции букв	11	12	13	14	15	16	17	18	19	20	21
Умножить на 3	33	36	39	42	45	48	51	54	57	60	63
mod 32	0	3	6	9	12	15	18	21	24	27	30
Буквы шифрованного текста	А	Г	Ё	И	Л	О	С	Ф	Ч	Ъ	Э

Буквы открытого текста	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я
Позиции букв	22	23	24	25	26	27	28	29	30	31	32
Умножить на 3	66	69	72	75	78	81	84	87	90	93	96
mod 32	0	3	6	9	12	15	18	21	24	27	30
Буквы шифрованного текста	А	Г	Ё	И	Л	О	С	Ф	Ч	Ъ	Э

Опишите возникшую проблему:
Слово «**где**» зашифровано как «**ИЛО».** Как бы Вы его расшифровали?

Проблема обратимости ключей

- Ключ, равный **3**, непригоден, потому что он не является обратимым для модуля **33**. Можно заметить, что ключи, равные **6** и **9** также непригодны. Какие же ключи все-таки пригодны?
- Обратным ключу **k** будем называть число k^{-1} такое, что $k * k^{-1} = 1 \bmod 33$. В общем случае для модульной системы R обратный ключ должен удовлетворять уравнению

$$k * k^{-1} = 1 \bmod R \qquad (1)$$

Проблема обратимости ключей-2

- Обозначим $m = k * k^{-1}$. Тогда выражение (1) можно записать в виде

$$m = R * n + 1 \qquad (2)$$

где n – некоторое целое число. Рассмотрим число **q = m – 1**. Тогда равенство **(2)** можно записать в виде

$$q + 1 = R * n + 1 \qquad (3)$$

$$q = R * n \qquad (4)$$

- Из **(4)** следует, что **q** имеет те же делители, что и **R**, а число **m = q + 1** не может иметь те же делители, что и **R**. Поскольку ключи **k** и k^{-1} в выражении **(1)** можно поменять местами, то из утверждения, что их произведение **m** не может быть кратно делителям **R**, следует, что и каждый из ключей **k** и k^{-1} не может быть кратным делителям **R**

Проблема обратимости ключей-3

- Таким образом, для модульной системы **33**, соответствующей русским текстам, непригодными являются ключи, кратные **3** и **11**. Это ключи, равные **3, 6, 9, 11, 12, 15, 18, 21, 22, 24, 27, 30**.
- Ниже приведем таблицу со значениями пригодных ключей и соответствующих им обратных ключей для модульной системы **33**

k	1	2	4	5	7	8	10	13	14	16
$\mathbf{k^{-1}}$	1	17	25	20	19	29	10	28	26	31

k	17	19	20	23	25	26	28	29	31	32
$\mathbf{k^{-1}}$	2	7	5	23	4	14	13	8	16	32

Таблица ключей для модульной системы 26

- Для модульной системы **26**, используемой в криптографических преобразованиях английских текстов, непригодными являются ключи, кратные **2** и **13** (так как эти числа являются делителями **26**). Заполните таблицу, приведенную ниже. Для каждого ключа **k** модульной системы **26** найдите обратный ключ **k-1**.

K	1	3	5	7	9	11	15	17	19	21	23	25
K^{-1}												

Независимо от того, насколько велик мультипликативный ключ этой модульной системы, его обратный, если он есть, будет в пределах от **1** до **25** (для модульной системы **33** – от **1** до **32**).

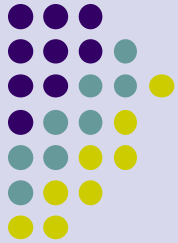
Таблица ключей для модульной системы 26

- В таблице приведены значения прямых и соответствующих им обратных ключей.

K	1	3	5	7	9	11	15	17	19	21	23	25
K^{-1}	1	9	21	15	3	19	7	23	11	5	17	25

Заметим, что ключу 1 соответствует обратный ключ -1, но использовать такую пару ключей не имеет смысла, так как шифрование в этом случае приводит к получению шифртекста, идентичного открытому тексту, например:
шифруя текст **you will excuse me for not waiting for you**
при помощи ключа 1, получим:
youwillexcusemefornotwaitingforyou

Вскрытие мультипликативного шифра



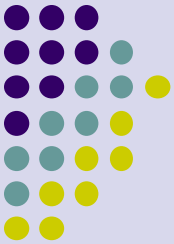
- Предположим, вам передали следующее сообщение:

ЮАЦЛЩ ДЖДНЖ АВЙЫФ ДХГЕЁ Ъ

и сказали, что оно создано с использованием мультипликативного шифра.

- Возникает вопрос, как дешифровать полученное сообщение?
- Полезным будет знание о том, что оно создано с использованием мультипликативного шифра. При аддитивном шифровании с **mod 33** было бы **32** числа, которые могли быть вашим аддитивным ключом (довольно бессмысленно рассматривать ключ, равный нулю). В случае мультипликативных ключей имеется всего **19** возможностей (опять же, бессмысленно рассматривать ключ, равный единице).

Вскрытие мультипликативного шифра - 2



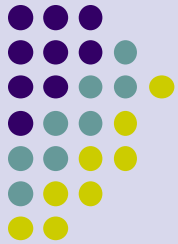
ЮАЦЛЩ

1 - юацлщ	29 - зажсы	2 - ьамчт	14 - еашгб
17 - яаыём	10 - маяфь	7 - таьср	13 - жавчз
25 - пангц	28 - йарёв	5 - цапъю	8 - ратэй
20 - щаюиш	26 - надоп	23 - уаблд	16 - баеъу
19 - ыазэя	31 - дауин	4 - шащое	32 - вайфж

Из таблицы мы видим, что осмысленный текст может быть получен на ключе 26. Таким образом, при дешифровании шифртекста
ЮАЦЛЩ ДЖДНЖ АВЙЫФ ДХГЕЁ Ъ
при помощи перебора ключей мы получаем единственный вариант открытого текста
Надоперебратьвсеключи или
НАДО ПЕРЕБРАТЬ ВСЕ КЛЮЧИ

Аффинный шифр

Предпосылки появления аффинного шифра



- Взлом зашифрованного текста при отсутствии информации о методах шифрования является достаточно сложной задачей.
- Информация о том, что что для шифрования использовался аддитивный шифр, намного упрощает задачу, поскольку известно, что, например, для русских текстов количество всех возможных сдвигов равно 32.
- Если известно, что это мультипликативный шифр, вариантов перебора становится еще меньше – только 19.
- Если известно, что шифр был создан либо аддитивным, либо мультипликативным шифром, необходимо выполнить 46 проверок различных вариантов ключей. При этом общее количество вариантов ключей для модульной системы 33 равно 32, а не 46, поскольку мультипликативные ключи являются подмножеством аддитивных.

Аффинный метод шифрования

- Информация о том, какой метод шифрования был использован, может сделать бессмысленным само шифрование.
- Однако данный вопрос не так прост, как кажется. Позже мы дадим обоснование тому, что все же следует сообщать об использованном методе шифрования.
- Совершенно очевидно, что аддитивные и мультипликативные методы являются довольно простыми для расшифровки. Теперь мы рассмотрим метод аффинного шифрования. Аффинный – это понятие, которое означает «линейное преобразование». Аффинный метод – это не что иное, как комбинация мультипликативного и аддитивного методов.

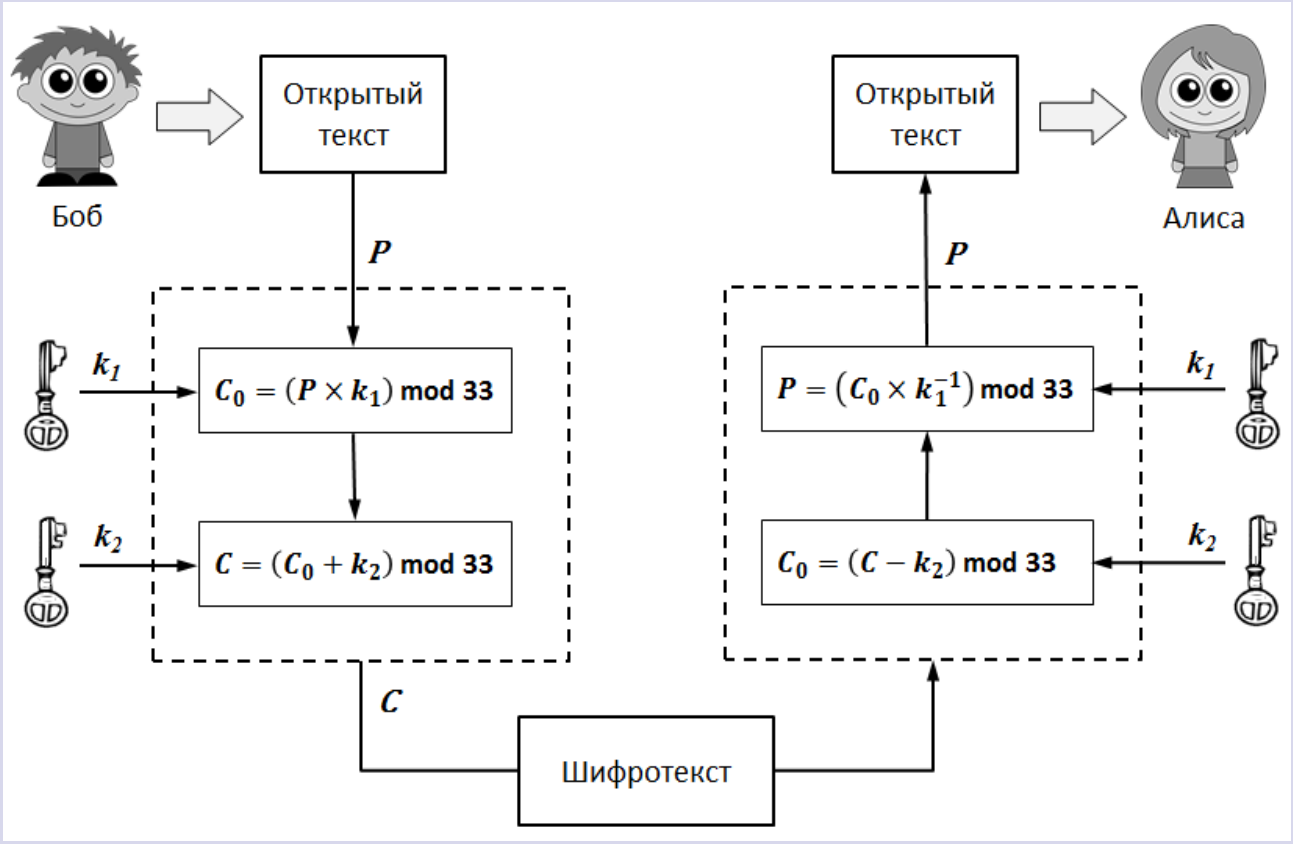
Аффинный метод шифрования - 2

- В аффинной системе шифрования мы выбираем мультипликативное число **a** и аддитивное число **b**. Если **p** является номером позиции символа открытого текста на русском языке, то мы определяем номер позиции зашифрованного символа по формуле

$$C = (ap + b) \bmod 33$$

Схема аффинного шифрования

На рисунке представлена схема аффинного ширования



Пример аффинного шифрования - 1

- Например, предположим, что мы хотим зашифровать текстовое сообщение «**ель**» с использованием аффинной системы шифрования при **a=5** и **b = 20**. Ниже в таблице приведены этапы шифрования:

Символы открытого текста	е	л	ь
Позиция p	5	12	29
5p + 20	45	80	165
(5p + 20) mod 33	12	14	0
Символы зашифрованного текста	Л	Н	А

Пример аффинного шифрования - 2

- Ниже приведены этапы шифрования открытого текста «план омега», с использованием аффинной системы при **a=239** и **b=152**:

Символы открытого текста	п	л	а	н	о	м	е	г	а
Позиция p	16	12	0	14	15	13	5	3	0
239p + 152	3976	3020	152	3498	3737	3259	1347	869	152
(239p + 152) mod 33	16	17	20	0	8	25	27	11	20
Символы зашифрованного текста	П	Р	У	А	З	Ш	Ъ	К	У

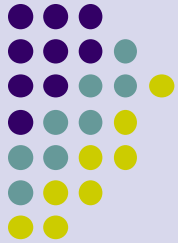
Пример аффинного шифрования - 3

- Однако, если бы мы хотели зашифровать открытый текст «**балка**» аффинной системой шифрования при **a = 3** и **b = 8**, то получили бы следующее:

Символы открытого текста	б	а	л	к	а
Позиция p	1	0	12	11	0
3p + 8	11	8	44	41	8
(3p + 8) mod 33	11	8	11	8	8
Символы зашифрованного текста	К	З	К	З	З

Результат декодирования будет неоднозначным

Ограничения на ключи при аффинном шифровании



- Очевидно, у нас появилась проблема. Процесс декодирования невозможен, поскольку в процессе кодирования разные символы «**б**» и «**л**» преобразовались в один и тот же символ «**К**», а символы «**а**» и «**к**» – в символ «**З**». Результат декодирования будет неоднозначным. Следовательно, некоторые пары **a** и **b** не позволяют выполнить обратное преобразование. Что это за пары?
- Так как **a** – мультипликативное число, то оно должно удовлетворять правилам мультипликативной системы шифрования. Это означает, что допустимые значения a не могут быть кратными **3** и **11** (делителям модуля **33**). На **b** нет ограничений.

Вскрытие аффинного шифра

- Очевидно, что число вариантов в аффинной системе резко возрастает. Имеем **19** вариантов для мультипликативной части ключа **a** и **32** варианта для аддитивной части ключа **b**. Итого **19 • 32 = 608** вариантов. Отсюда мы должны убрать вариант {**a=1; b=32**}.
- Следовательно, если хотим декодировать сообщение на русском языке, нам придется перебрать **607** вариантов. Для английских текстов это число меньше: **12 • 25 = 300** вариантов.

Вскрытие аффинного шифра - 2

- Итак, теперь мы переходим к процессу декодирования. Для этого нам нужно сгенерировать числа, обратные **a** и **b**, которые будем обозначать **c** и **d**. Это не так просто. Рассмотрим пример..
- Предположим, что **p** – это позиция буквы, которую мы хотим зашифровать. Пусть **a = 25** и **b = 8**. Тогда позиция зашифрованного символа будет определяться из выражения

$$C = (25p + 8) \bmod 33$$

- Для нахождения **c** и **d** мы должны преобразовать это выражение к виду

$$p = (cC + d) \bmod 33$$

- (Далее будем использовать знак равенства вместо ≡). Примечание: не путайте **C** и **c**.
- .

Вскрытие аффинного шифра - 3

• Чтобы обратить процедуру, мы должны решить уравнение (уравнение шифрования):	$C = (25p + 8) \bmod 33$
• Переносим 8 на другую сторону:	$C - 8 = 25p \bmod 33$
• Исключаем -8 (добавляем 33):	$C + 25 = 25p \bmod 33$
• Нам нужно найти p. Поэтому умножаем обе стороны на число, обратное 25, то есть умножаем на 4. (В процессе преобразований не используется действие деления):	$4\,(C + 25) = 1p \bmod 33$
• Открываем скобки:	$4C + 100 = p \bmod 33$
• Заменяем 100 mod 33 на 1 mod 33:	$p = (4C + 1) \bmod 33$
• Выделяем в уравнении **c** и **d**:	$c = 4,\ d = 1$

Вскрытие аффинного шифра - 4

- Рассмотрим еще один пример. Теперь для **mod 26**. Пусть **a = 5** и **b = 20**. Если **p** – позиция буквы, которую мы хотим зашифровать, то позиция зашифрованной буквы определяется из выражения **C = (5p + 20) mod 26**.

• Чтобы обратить процедуру, мы должны решить уравнение:	$C = (5p + 20) \bmod 26$
• Переносим 20 на другую сторону:	$C - 20 = 5p \bmod 26$
• Исключаем -20 (добавлением 26):	$C + 6 = 5p \bmod 26$
• Нам нужно найти p. Поэтому умножаем обе стороны на число, обратное 5, то есть умножаем на 21. (В процессе преобразований не используется действие деления):	$21\ (C + 6) = p \bmod 26$
• Открываем скобки:	$21C + 126 = p \bmod 26$
• Заменяем 126 mod 26 на 22 mod 26:	$p = (21C + 22) \bmod 26$
• Выделяем в уравнении **c** и **d**:	$c = 21, d = 22$

Пример вскрытия аффинного шифра

Применение метода грубой силы

- Предположим, что перехвачено зашифрованое сообщение:

ЕСШКЩ ЪЧЩПС РЕДЭИ ТЩЦЬЯ МФЖФЦ ХНЧЛЭ КЭТЭП

Единственное, что нам известно, это то, что для шифрования использовался аффинный шифр

$$C = (ap + b) \bmod 33$$

- Можно начать с того, что для различных сочетаний **a** и b существует 607 вариантов (сообщение составлено из букв русского алфавита). Можно проверить все. В среднем, получим решение на полпути или примерно после 303 испытаний. Предполагая что требуется 5 секунд на то, чтобы ввести значения каждой пары a и b и проверить, является ли это правильным решением, получим общее время 1515 секунд. То есть можно ожидать, что путем проб и ошибок мы сможем получить наше решение в среднем за 25 минут. В лучшем случае это будет 5 секунд, а в худшем – 50 минут.

Применение метода частотного анализа

- Существует способ, который иногда позволяет получить ответ гораздо быстрее, чем метод полного перебора вариантов
- В текстах на любом языке некоторые буквы появляются гораздо чаще, чем другие. Следующая таблица показывает относительную частоту букв для русского языка:

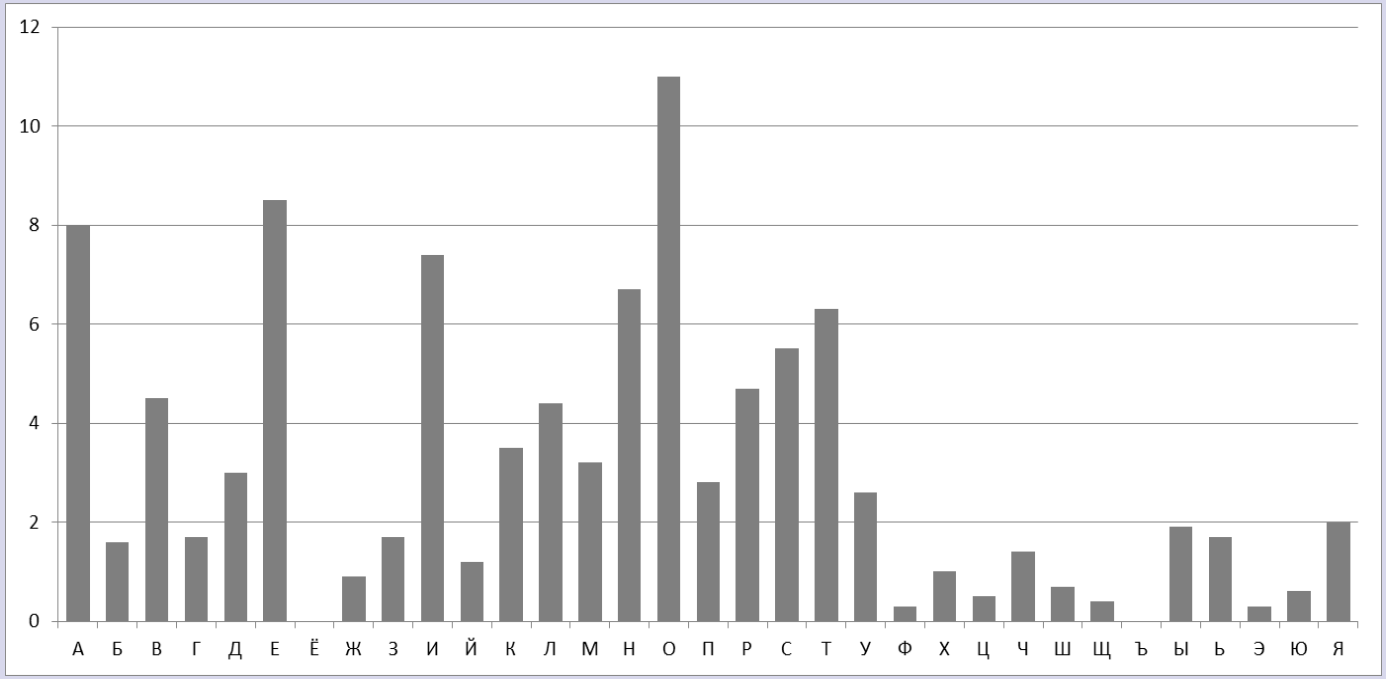
Буквы открытого текста	а	б	в	г	д	е	ё	ж	з	и	й
Относительная частота (%)	8,0	1,6	4,5	1,7	3,0	8,5	0,0	0,9	1,7	7,4	1,2

Буквы открытого текста	к	л	м	н	о	п	р	с	т	у	ф
Относительная частота (%)	3,5	4,4	3,2	6,7	11,0	2,8	4,7	5,5	6,3	2,6	0,3

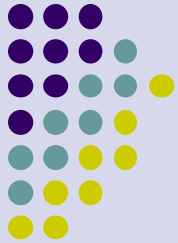
Буквы открытого текста	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я
Относительная частота (%)	1,0	0,5	1,4	0,7	0,4	0,0	1,9	1,7	0,3	0,6	2,0

Частота букв русского языка

- Из таблицы видно, что буква «о» и буква «е» наиболее часто(соответственно с частотой 11% и 8,5 %) встречаются в обычных (нормальных) текстах на русском языке.
- На рисунке ниже табличные данные представлены в виде гистограммы



Вскрытие аффинного шифра с помощью частотного анализа - 1



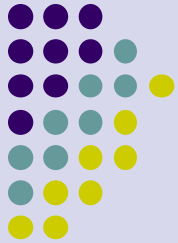
- Внимательно посмотрим на зашифрованое сообщение:

ЕСШКЩ ЪЧЩПС РЕДЭИ ТЩЦЬЯ МФЖФЦ ХНЧЛЭ КЭТЭП

Определим, какие буквы встречаются чаще других.

- Наиболее часто встречается буква «**Э**» – **4** раза. Затем идет буква «**Щ**» – **3** раза. Остальные буквы встречаются примерно одинаково. Если открытый текст был «нормальным», можно ожидать, что одна из букв «**Э**» и «**Щ**» является буквой «**о**». Итак, начнем с предположения, что буква «**о**» зашифрована буквой «**Э**». Затем будем поочередно рассматривать варианты «**Щ**» → «**о**», «**Э**» → «**е**», и «**Щ**» → «**е**».

Вскрытие аффинного шифра с помощью частотного анализа - 2



- Вспомним формулу шифрования **C = (ap + b) mod 33**. Найдем номера позиций букв "**о**" и "**Э**" открытого текста в алфавите. Это **15** и **30**, соответственно. Подставим эти значения в уравнение:

  C = (ap + b) mod 33 или **30 = (15a + b) mod 33**.

- Как решить это уравнение? Мы знаем, что **a** может принять одно из следующих значений:

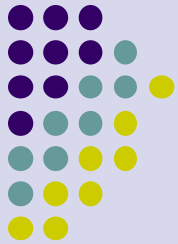
  1, 2, 4, 5, 7, 8, 10, 13, 14, 16, 17, 19, 20, 23, 25, 26, 28, 29, 31, 32.

- Это множество целых чисел от **1** до **32** за исключением кратных **3** и **11**. Поочередно проверим эти варианты, подставляя различные значения **a** в уравнение

  30 = (15a + b) mod 33.

- Пусть **a = 1:** имеем: **30 = (15 + b) mod 33**. Это дает нам **b = 15**.

Вскрытие аффинного шифра с помощью частотного анализа - 3



- Пусть **a = 2:** имеем: **30 = (30 + b) mod 33**. Это дает нам **b = 0**.

Необходимо проверить **{a = 2, b = 0}.**

- Пусть **a = 4:** имеем: **30 = (60 + b) mod 33**. Это дает нам

b = -30 mod 33 или **3.**

Необходимо проверить **{a = 4, b = 3}.**

- Пусть **a = 5:** имеем: **30 = (75 + b) mod 33**. Это дает нам

b = -45 mod 33 или **21.**

Необходимо проверить **{a = 5, b = 21}.**

- Пусть **a = 7:** имеем: **30 = (105 + b) mod 33**. Это дает нам

b = -75 mod 33 или **24.**

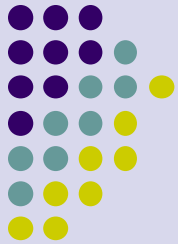
Необходимо проверить **{a = 7, b = 24}.**

Получили **{c = 19, d = 6}.** Открытый текст для данного шифртекста:

"Встречаемся в полдень у хижины за городом"

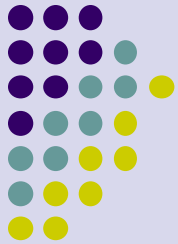
Таким образом, удалось дешифровать сообщение.

Вскрытие аффинного шифра с помощью частотного анализа - 4



- А что бы было, если бы мы не выполняли проверку на каждом шаге? Нам бы пришлось выполнить огромное количество вычислений, причем не только для буквы «**о**», но и для букв «**е**», «**а**», «**и**».
- При этом необходимо помнить, что такой метод основан на предпосылке, что буквы «**о**» и «**е**» являются наиболее распространенными буквами в открытом русском тексте. Если сообщение длинное, то это, вероятно, хорошее предположение. Но если оно короткое, то использование метода, основанного на частоте встречаемости букв, не является обоснованным. Итак, хоть и трудно в это поверить, но длинное сообщение проще расшифровать, чем короткое.
- Также отметим, что много сообщений легче расшифровать, чем одно сообщение (имеется в виду, что они зашифрованы одним и тем же отправителем).

Применение метода частотного анализа для английского языка

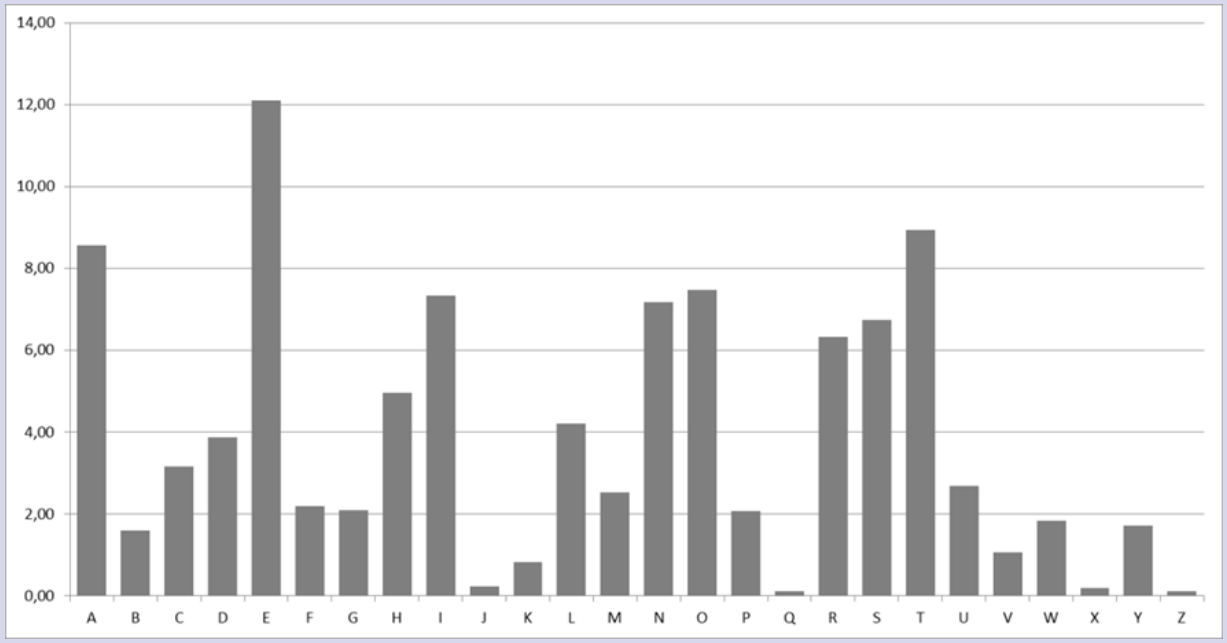


- приведем статистические данные о частоте букв английского языка.
- В таблице приведена частота встречаемости одиночных букв (монограмм) в английском языке

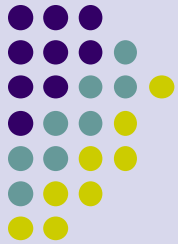
Буква	%	Буква	%	Буква	%
A	8,55	K	0,81	U	2,68
B	1,6	L	4,21	V	1,06
C	3,16	M	2,53	W	1,83
D	3,87	N	7,17	X	0,19
E	12,1	O	7,47	Y	1,72
F	2,18	P	2,07	Z	0,11
G	2,09	Q	0,1		
H	4,96	R	6,33		
I	7,33	S	6,73		
J	0,22	T	8,94		

Частота букв английского языка

- Из таблицы видно, что буква «E» и буква «T» наиболее часто(соответственно с частотой 12,1% и 8,94 %) встречаются в обычных (нормальных) текстах на русском языке.
- На рисунке ниже табличные данные о частоте букв английского языка представлены в виде гистограммы



Инверсные аффинные преобразования – алгоритм



Автоматическое вычисление параметров c и d, инверсных параметрам a и b, выполняется следующим образом.

- В цикле перебираются все возможные значения c от 1 до 32 (для английских текстов – от 1 до 25).
- Среди них выбирается то значение, для которого выполняется условие

  $(a \cdot c) \bmod M = 1$,

  где M = 33 для русских текстов и M = 26 для английских текстов.
- Для вычисления аддитивного параметра d, обратного параметру b, сначала надо найти

  $b2 = (-b) \bmod M$.
- Если $b2 < 0$, то добавляем к нему M:

  $b2 = b2 + M$.

  Далее находим

  $d = (c \cdot b2) \bmod M$.

Пример задачи – аффинный шифр

Условие: Зашифровать и расшифровать слово **АЛГЕБРА**, используя приведенную в Таблице нумерацию букв русского алфавита, функцию шифрования $f(x) = 2x + 3$ и соответствующий аффинный шифр.

А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П
00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16
Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	
17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	

Решение: Чтобы использовать описанные выше алгоритмы шифрования и расшифрования аффинного шифра, заметим, что числа 2 и 33 взаимно просты, и поэтому ключ k = (2, 3) определяет аффинный шифр в Z_{33}
Для зашифрования слова **АЛГЕБРА** его надо вначале оцифровать. Получим следующий открытый текст в алфавите Z_{33}:
m = 00 12 03 05 01 17 00. Далее вычисляем значения функции $E_k(x) = f(x) = 2x + 3$ при x = 0, 12, 3, 5 , 1 , 17, 0 и п олучаем шифртекст с = 03 27 09 13 05 04 03, а затем, переходя к буквам, – криптограмму **ГЪИМЕДГ**.

Пример задачи – аффинный шифр-2

Продолжение решения - расшифрование: Для расшифрования криптограммы **ГЪИМЕДГ** надо её вначале оцифровать и получить шифртекст c = 03 27 09 13 05 04 03. Затем воспользоваться функцией расшифрования $D_k(y)$ = = $f^{-1}(y) = (y - 3)2^{-1} \bmod 33$ и тем, что обратным к числу 2 в кольце Z_{33} будет число 17, вычислить ее значения при y = = 3, 27, 9, 13, 7, 4, 3 и получить оцифрованный открытый текст m. Имеем:

А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П
00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16
Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	
17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	

$\dot{D}_k(3) = (3 - 3)\cdot 17 \bmod 33 = 0$; $D_k(27) = (27 - 3)\cdot 17 \bmod 33 = 408 \bmod 33 = 12$,
$D_k(9) = (9 - 3)\cdot 17 \bmod 33 = 102 \bmod 33 = 3$,
$D_k k13) = (13 - 3)\cdot 17 \bmod 33 = 170 \bmod 33 = 5$, $D_k(7) = (5 - 3)\cdot 17 \bmod 33 = 1$,
$D_k(4) = (4 - 3)\cdot 17 \bmod 33 = 17$, $D_k(3) = (3 - 3)\cdot 17 \bmod 33 = 0$.
Таким образом, mm = 00 12 03 05 01 17 00. Переходя к буквам, получим исходный текст **АЛГЕБРА**.

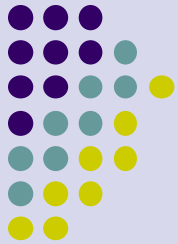
Пример задачи – аффинный шифр-2

Продолжение решения - расшифрование: Для расшифрования криптограммы **ГЪИМЕДГ** надо её вначале оцифровать и получить шифртекст c = 03 27 09 13 05 04 03. Затем воспользоваться функцией расшифрования $D_k(y)$ = = $f^{-1}(y) = (y - 3)2^{-1} \bmod 33$ и тем, что обратным к числу 2 в кольце Z_{33} будет число 17, вычислить ее значения при y = = 3, 27, 9, 13, 7, 4, 3 и получить оцифрованный открытый текст m. Имеем:

А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П
00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16
Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	
17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	

$\dot{D}_k(3) = (3 - 3)\cdot 17 \bmod 33 = 0$; $D_k(27) = (27 - 3)\cdot 17 \bmod 33 = 408 \bmod 33 = 12$,
$D_k(9) = (9 - 3)\cdot 17 \bmod 33 = 102 \bmod 33 = 3$,
$D_k k13) = (13 - 3)\cdot 17 \bmod 33 = 170 \bmod 33 = 5$, $D_k(7) = (5 - 3)\cdot 17 \bmod 33 = 1$,
$D_k(4) = (4 - 3)\cdot 17 \bmod 33 = 17$, $D_k(3) = (3 - 3)\cdot 17 \bmod 33 = 0$.
Таким образом, mm = 00 12 03 05 01 17 00. Переходя к буквам, получим исходный текст **АЛГЕБРА**.

Шифр Цезаря – частный случай аффинного шифра



Частным случаем аффинного шифра, когда a = 1, т. е. ключ k = (a, b) шифрования имеет вид k= (1, b), является так называемый сдвиговый шифр. В этом случае можно считать, что множество ключей K совпадает с множеством Z_n.

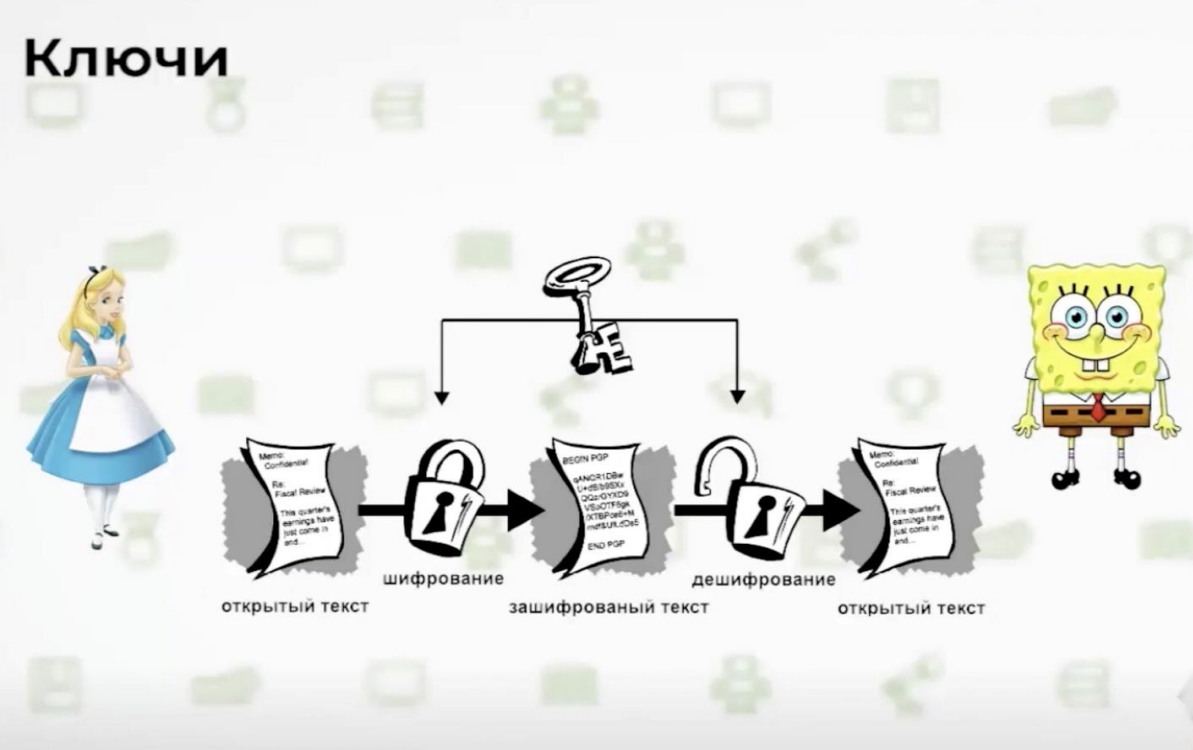
Алгоритмы шифрования и расшифрования в этом случае значительно упрощаются:

$c = E_k(m) = E_k(x_1x_2 \ldots x_l) = (x_1 + b)(x_2 + b)\ldots(x_l + b) = y_1y_2 \ldots y_l$;

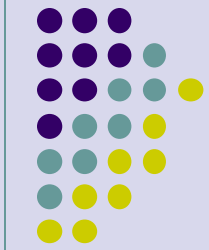
При k =3 получим шифр Цезаря

Симметричное шифрование и ключи шифрования - 1

Основная проблема заключается в распределении ключей



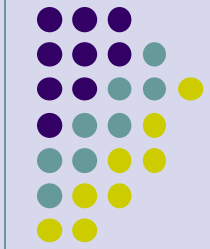
Симметричное шифрование и ключи шифрования - 2



- Симметричное шифрование предусматривает шифрование и расшифрование с помощью одного и того же секретного ключа, поэтому пользователям важно правильно выработать совместный ключ, а также безопасно его передать.
- В условиях незащищенного канала это сделать очень сложно.
- Необходимо сначала передать отправителю и получателю сообщения секретный ключ, только после передачи ключей можно будет начать обмен зашифрованными сообщениями.

Шифрование с закрытым ключом

Пример: использование различных ключей для передачи секрета



- Вы хотите послать другу документ, содержание которого должно остаться в тайне. У Вас есть коробочка с двумя парами ушек для навесных замков, которую Вы можете посылать своему другу, а он - вам. Подходящий замок имеется как у Вас, так и у Вашего друга. Но это различные замки, и ключи от одного не подходят к другому. Посылать ключ в незапертой коробочке вы не хотите, опасаясь, что он может быть скопирован. Как вы должны поступить?
- РЕШЕНИЕ: вы кладете документ в коробочку и запираете ее на свой замочек. Получив коробочку, ваш друг запирает ее на свой замочек и посылает вам. Получив коробочку, вы снимаете свой замочек, и посылаете её другу.

Количество ключей. Кодовый замок

Количество ключей. Количество цифровых и символьных комбинаций

Количество ключей. Символы алфавита

- a..z - 26
- A..Z - 26
- 0..9 - 10
- !@#$%^&*() - 10
- Итого - 72

Количество комбинаций в зависимости от длины кода и числа используемых символов

		длина кода							
		3	4	5	6	7	8	9	10
кол-во используемых символов	26	17576	456976	11881376	308915776	8031810176	208827064576	5429503678976	141167095653376
	52	140608	7311616	380204032	19770609664	1028071702528	53459728531456	2779905883635710	144555105949057000
	72	373248	26873856	1934917632	139314069504	10030613004288	722204136308736	51998697814229000	3743906242624490000

Перехват хеша пароля

*Ева - потенциальный злоумышленник (условное обозначение в криптографии)

*Хэш пароля - уникальный набор символов, связанный с конкретным паролем, но не раскрывающий сам пароль.

*Алиса - отправитель сообщения (условное обозначение в криптографии)

Пароль длиной 7 символов. Перебор миллиона паролей в секунду

Время подбора пароля в зависимости от длины кода и числа используемых символов

		длина кода			
		7	8	9	10
кол-во используемых символов	26	2 часа	2,5 дня	63 дня	4,5 года
	52	12 дней	1,7 лет	88 лет	4584 года
	72	116 дней	22,9 лет	1649 лет	118718 лет

Спасибо за внимание