Содержание

1

ИНСТРУМЕНТЫ “БУМАЖНОЙ” КРИПТОГРАФИИ

“Джин шифрования выпущен из бутылки”.
Ян Кум, основатель WhatsApp

Прежде чем приступать к написанию шифровальных программ, давайте рассмотрим, как реализуется процесс шифрования и дешифрования с помощью карандаша и бумаги. Это позволит вам лучше понять природу шифров и тех математических инструментов, которые применяются для создания секретных сообщений. В данной главе вы узнаете о том, что такое криптография и чем коды отличаются от шифров. Затем мы воспользуемся простым шифром, известным как *шифр Цезаря*, для шифрования и расшифровки бумажных сообщений.

В этой главе...

- Что такое криптография
- Коды и шифры
- Шифр Цезаря
- Шифровальные диски
- Криптография и арифметика
- Двойное шифрование

Что такое криптография

С незапамятных времен все, кому требовалось обмениваться тайными сведениями, например шпионы, военные, пираты, торговцы и дипломаты, прибегали к засекречиванию своих сообщений, чтобы тайны оставались надежно скрыты от посторонних глаз. *Криптография* — это наука, которая изучает способы создания и применения секретных кодов. Чтобы понять, как работают криптографические методы, рассмотрим следующие два фрагмента текста.

```
nyr N.vNwz5uNz5Ns6620Nz0N3z2v
N yvNwz9vNz5N6!9Nyvr9
y0QNnvNwv tyNz
Nw964N6!9N5vzxys690,N.vN2z5u-
3vNz Nr Ny64v,N.vNt644!5ztr vNz
N 6N6 yv90,Nr5uNz Nsvt64v0N
yvN7967v9 BN6wNr33Q N-m63 rz9v
```

```
!NN2 Nuwv,N9,vNN!vNrBN3zyN4vN
N6 Qvv0z6nvN.7N0yv4N 4 zzvNN
vyN,NN99z0zz6wz0y3vv26 9
w296vyNNrrNyQst.560N94Nu5y
rN5nz5vv5t6v63zNr5.
N75sz6966NNvw6 zu0 wtNxs6t
49NrN3Ny9Nvzy!
```

Текст слева — секретное сообщение, которое было *зашифровано*, т.е. преобразовано в секретный код. Любому человеку, не знающему способа его *дешифрования*, или *расшифровки*, оно кажется полной абракадаброй. Сообщение справа — случайный набор символов, не имеющий никакого скрытого смысла. Шифрование позволяет сохранить смысл сообщения в тайне от тех, кому не известен способ его расшифровки, даже если сообщение попадет им в руки. *Шифрованное сообщение воспринимается посторонними как случайный набор букв, не несущий в себе никакого смысла.*

Криптограф, или *шифровальщик*, использует и изучает секретные коды. Разумеется, секретные сообщения не всегда остаются секретными. *Криптоаналитик*, т.е. *взломщик кодов*, или *хакер*, способен взламывать и читать сообщения, зашифрованные другими людьми. Цель книги — научить вас зашифровывать и расшифровывать сообщения с помощью различных методов. К счастью, все те методы взлома, которые вы изучите, не настолько опасны, чтобы у вас из-за них могли возникнуть проблемы с законом.

Коды и шифры

В отличие от шифров *коды* изначально создаются такими, чтобы они были понятны и общедоступны. Коды заменяют буквы символами, которые любой человек может использовать для перевода в форму сообщения.

В начале XIX века развитие электрического телеграфа привело к созданию известного кода, обеспечивавшего почти мгновенный обмен сообщениями между континентами по проводам. Сообщения, отправляемые по телеграфу, достигали своих адресатов гораздо быстрее, чем прежняя лошадиная почта, перевозившая мешки с письмами. Однако телеграф не позволял отправлять сообщения в том же виде, в каком они были написаны на бумаге, т.е. в виде последовательностей букв. По нему могли пересылаться только два типа электрических импульсов: короткий, который назвали “точка”, и длинный, который назвали “тире”.

Для преобразования букв алфавита в электрические импульсы необходимо располагать системой кодов, с помощью которой можно было бы переводить привычные для нас буквы на язык точек и тире. Процесс преобразования букв алфавита в последовательности точек и тире для отправки по телеграфу называется *кодированием*, а обратный процесс преобразования электрических импульсов в буквы при получении сообщения — *декодированием*. Способ, применяемый для кодирования и декодирования телеграфных сообщений (а впоследствии и сообщений, передаваемых по радио), был изобретен Сэмюэлем Морзе и Альфредом Вейлем и получил название *код Морзе*, или *азбука Морзе* (табл. 1.1).

Таблица 1.1. Международная азбука Морзе

Латинский символ	Код	Латинский символ	Код	Цифра	Код
A	•−	N	−•	1	•−−−−
B	−•••	O	−−−	2	••−−−
C	−•−•	O	•−−•	3	•••−−
D	−••	Q	−−•−	4	••••−
E	•	R	•−•	5	•••••
F	••−•	S	•••	6	−••••
G	−−•	T	−	7	−−•••
H	••••	U	••−	8	−−−••
I	••	V	•••−	9	−−−−•
J	•−−−	W	•−−	0	−−−−−
K	−•−	X	−••−		
L	•−••	Y	−•−−		
M	−−	Z	−−••		

Используя телеграфный ключ для передачи точек и тире, телеграфист отправлял текстовые сообщения, способные почти мгновенно достигать адресата, находящегося на другом конце земного шара[1]!

В отличие от знакового кодирования *шифр* — специфический тип кодов, обеспечивающих сохранение содержания сообщения в тайне. Шифр можно использовать для того, чтобы преобразовать исходный текст, написанный на понятном языке (так называемый *простой текст*), в бессвязный набор символов, называемый *шифротекстом*, который скрывает смысл секретного сообщения. Шифр — это набор правил преобразования между простым и зашифрованным текстом. В правилах для шифрования и дешифрования часто используется один и тот же ключ, который называется *секретным* и известен только отправителю и получателю сообщения. В книге вы изучите несколько видов шифров и напишете программы для шифрования и дешифрования текста с их помощью. Но сначала следует научиться шифровать сообщения вручную, используя простые средства "бумажной" криптографии.

Шифр Цезаря

Первый из шифров, который мы изучим, — шифр Цезаря, названный так в честь Юлия Цезаря, который пользовался им 2000 лет тому назад. Хорошая новость состоит в том, что он прост и несложен для изучения. Но есть и плохая новость: в силу простоты этого шифра криптоаналитику не составит большого труда взломать его. Тем не менее ознакомление с ним даст вам полезный опыт.

Шифр Цезаря основан на замене одной буквы другой после предварительного смещения всего алфавита на определенное число позиций. Юлий Цезарь заменял буквы в своих сообщениях путем смещения алфавита на три позиции и последующей замены каждой буквы соответствующей буквой из смещенного алфавита.

Например, вместо каждой буквы 'A' он подставлял букву 'D', вместо каждой буквы 'B' — букву 'E' и т.д. Если Цезарю нужно было сдвинуть букву, находящуюся в конце алфавита, скажем, 'Y', то он возвращался в начало алфавита, смещаясь в целом на три позиции и подставляя букву 'B'. В этом разделе мы будем шифровать сообщения вручную, применяя шифр Цезаря.

[1] Более подробную информацию об азбуке Морзе можно найти в Википедии: `https://ru.wikipedia.org/wiki/Азбука_Морзе`.

Шифровальный диск

Чтобы упростить преобразование простого текста в зашифрованный с помощью шифра Цезаря, мы будем использовать *шифровальный диск*. Он состоит из двух колец, каждое из которых разбито на 26 ячеек (по числу букв английского алфавита). Внешнее кольцо представляет алфавит исходного текста, а внутреннее — соответствующие буквы зашифрованного текста. Буквы на внутреннем кольце пронумерованы числами от 0 до 25. Эти числа определяют ключ шифрования, в данном случае — количество позиций, на которое нужно перейти от буквы 'A' к соответствующей букве на внутреннем кольце. Поскольку сдвиг выполняется по кругу, смещение с ключом, значение которого превышает 25, продолжается с начала алфавита, соответственно, смещение на 26 позиций равносильно отсутствию сдвига, смещение на 27 позиций — сдвигу на 1 позицию и т.д.

Виртуальный шифровальный диск доступен по адресу `https://inventwithpython.com/cipherwheel/` (рис. 1.1). Чтобы провернуть диск, щелкните на нем один раз и перемещайте указатель мыши по кругу, пока не будет достигнута нужная конфигурация. Повторный щелчок останавливает дальнейшее вращение диска.

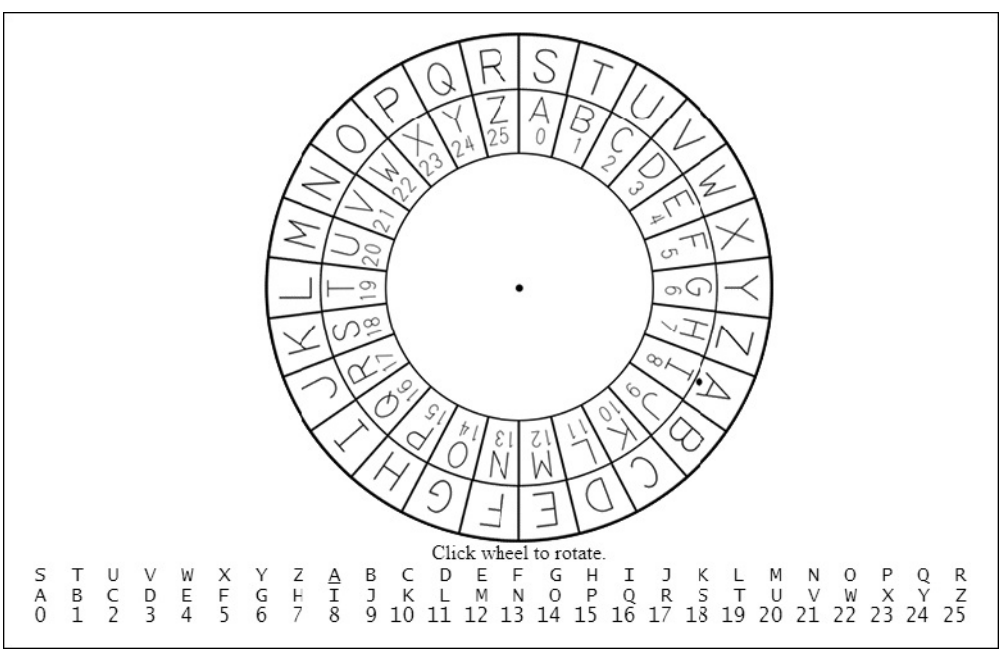

Рис. 1.1. *Онлайновый шифровальный диск*

Вы сможете получить бумажную версию шифровального диска, распечатав изображение, доступное по указанному адресу. Вырежьте два круга,

вложите меньший из них в больший и закрепите по центру булавкой, чтобы их можно было вращать.

Используя либо бумажную, либо виртуальную модель, вы сможете вручную зашифровать секретное сообщение.

Шифрование сообщения с помощью шифровального диска

В качестве примера зашифруем сообщение “THE SECRET PASSWORD IS ROSEBUD” с помощью онлайнового шифровального диска. Проверните диск так, чтобы деления внутреннего и внешнего кругов совпадали. Обратите внимание на изображение точки под буквой ‘A’. Число на внутреннем круге под этой точкой и есть ключ шифрования, который будет применяться при данной конфигурации диска.

На рис. 1.1 таким числом является 8. Мы используем его в качестве ключа для того, чтобы зашифровать сообщение (рис. 1.2).

T	H	E		S	E	C	R	E	T		P	A	S	S	W	O	R	D		I	S		R	O	S	E	B	U	D
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
B	P	M		A	M	K	Z	M	B		X	I	A	A	E	W	Z	L		Q	A		Z	W	A	M	J	C	L

Рис. 1.2. *Шифрование сообщения с помощью шифра Цезаря по ключу 8*

Найдите каждую букву сообщения на внешнем круге и замените ее соответствующей буквой из внутреннего круга. В данном примере сообщение начинается с буквы ‘T’ (первая буква ‘T’ во фразе “THE SECRET...”), поэтому находим букву ‘T’ на внешнем круге, а затем соответствующую ей букву на внутреннем круге, которой является буква ‘B’. Таким образом, в исходном сообщении буква ‘T’ всегда будет заменяться буквой ‘B’. (Если бы вы использовали другой ключ шифрования, то каждая буква ‘T’ заменялась бы другой буквой.) Следующая буква сообщения — ‘H’, которая превращается в букву ‘P’. Далее буква ‘E’ превращается в букву ‘M’. Каждая буква внешнего круга всегда шифруется одной и той же буквой внутреннего круга. Как только вы найдете первую букву ‘T’ в сообщении “THE SECRET...” и увидите, что она шифруется буквой ‘B’, можете заменить буквой ‘B’ все буквы ‘T’ в сообщении с целью экономии времени, чтобы каждую букву приходилось искать на шифровальном диске всего лишь раз.

Завершив процесс шифрования всего исходного сообщения “THE SECRET PASSWORD IS ROSEBUD”, вы получите результирующее зашифрованное сообщение “BPM AMKZMB XIAAEWZL QA ZWAMJCL”. Обратите внимание на то, что небуквенные символы, в данном случае пробелы, остаются неизменными.

Теперь вы сможете спокойно отправить зашифрованное сообщение нужному получателю (или оставить его при себе), и никто не сможет прочитать его, если вы не сообщите ему ключ шифрования. Убедитесь, что ключ хранится в надежном месте, поскольку любой человек, которому станет известно, что вы использовали ключ шифрования 8, сможет прочитать зашифрованное сообщение.

Дешифрование сообщения с помощью шифровального диска

Чтобы дешифровать зашифрованный текст, начните с внутреннего круга шифровального диска. Предположим, вы получили зашифрованный текст "IWT CTL EPHHLDGS XH HLDGSUXHW". Вы не сможете расшифровать его, пока не узнаете ключ (если только вы не криптоаналитик). К счастью, отправитель уже сообщил вам, что в своих сообщениях он использует ключ 15. Конфигурация шифровального диска для этого ключа приведена на рис. 1.3.

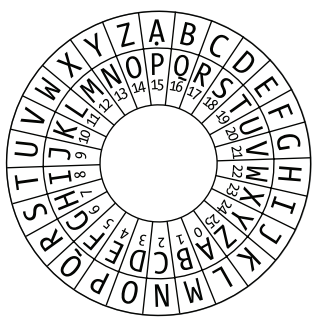

Рис. 1.3. *Конфигурация шифровального диска для ключа 15*

Установите букву 'A' на внешнем круге (помечена точкой) напротив буквы на внутреннем круге с номером 15 (буква 'P'). Затем найдите первую букву секретного сообщения на внутреннем круге (буква 'I') и запишите букву, которая соответствует ей на внешнем круге (буква 'T'). Вторая буква секретного сообщения, 'W', дешифруется в букву 'H'. Расшифровав все буквы зашифрованного текста, вы получите сообщение в виде простого текста: "THE NEW PASSWORD IS SWORDFISH" (рис. 1.4).

I	W	T		C	T	L		E	P	H	H	L	D	G	S		X	H		H	L	D	G	S	U	X	H	W
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
T	H	E		N	E	W		P	A	S	S	W	O	R	D		I	S		S	W	O	R	D	F	I	S	H

Рис. 1.4. *Дешифрование сообщения с помощью шифра Цезаря по ключу 15*

Если использовать некорректный ключ, например 16, то расшифрованное сообщение превратится в бессмысленный набор символов "SGD MDV OZRRVNQC HR".

Шифрование и дешифрование средствами арифметики

Шифровальный диск — удобный инструмент для применения шифра Цезаря, но аналогичные операции можно выполнять и в арифметическом

виде. Запишите буквы алфавита от ‘A’ до ‘Z’ и пронумеруйте их числами от 0 до 25. Начните с нуля под ‘A’, единицей под ‘B’ и т.д., пока не поставите номер 25 под ‘Z’ (рис. 1.5).

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Рис. 1.5. *Нумерация алфавита числами от 0 до 25*

Полученную таблицу перекодировки букв в цифры можно использовать для представления букв, что позволяет выполнять над буквами арифметические операции. Например, если вы запишете слово “CAT” цифрами 2, 0 и 19, то сможете прибавить к каждой из них 3, получив в результате последовательность 5, 3 и 22. Эти новые числа представляют буквы “FDW”. Позже мы сможем написать компьютерную программу, которая все сделает за нас.

Чтобы использовать арифметику для шифрования с помощью шифра Цезаря, найдите число под буквой, которую хотите зашифровать, и прибавьте к ней номер ключа. Результирующая сумма и есть число, находящееся под зашифрованной буквой. Зашифруем, например, текст “HELLO. HOW ARE YOU?” с помощью ключа 13. (В качестве ключа можно использовать любое другое число от 1 до 25.) Прежде всего найдите число под буквой ‘H’, т.е. 7. Затем прибавьте 13 к этому числу: 7 + 13 = 20. Поскольку число 20 находится под буквой ‘U’, то буква ‘H’ превращается в букву ‘U’.

Точно так же, чтобы зашифровать букву ‘E’ (4), выполните сложение 4 + 13 = 17. Буква над 17 — ‘R’, поэтому ‘E’ преобразуется в ‘R’ и т.д.

Этот процесс отлично работает до тех пор, пока мы не достигнем буквы ‘O’. Число под ‘O’ — 14. Но 14 + 13 = 27, а список чисел доходит лишь до значения 25. Если сумма чисел буквы и ключа равна или превышает 26, придется вычесть из нее 26. В данном случае 27 – 26 = 1. Буква над цифрой 1 — ‘B’, поэтому, если используется ключ 13, буква ‘O’ превращается в ‘B’. Зашифровав подобным образом каждую букву сообщения, получим зашифрованный текст “URYYB. UBJ NER LBH?”.

Чтобы расшифровать зашифрованный текст, следует вместо прибавления ключа к каждой букве использовать вычитание. Букве ‘B’ в зашифрованном тексте соответствует число 1. Результатом вычитания 13 из 1 будет отрицательное число –12. Аналогично нашему правилу “вычитания 26”, если результат меньше нуля при дешифровании, то к нему нужно прибавить 26. Поскольку –12 + 26 = 14, буква ‘B’ в зашифрованном тексте дешифруется в букву ‘O’.

Как видите, чтобы воспользоваться шифром Цезаря, вовсе не обязательно иметь шифровальный диск. Все, что нам для этого нужно, — карандаш, бумага и минимальные знания арифметики!

Почему не работает двойное шифрование

У кого-то из читателей может возникнуть мысль, что использование двух разных ключей шифрования подряд позволит вдвое увеличить стойкость шифра. Однако в случае шифра Цезаря (и большинства других шифров) это не так. В действительности результат двойного шифрования будет эквивалентен тому, который вы могли бы получить обычным способом с помощью единственного ключа. Попробуем применить двойное шифрование, чтобы понять, почему так происходит.

Если вы зашифруете слово "KITTEN" с помощью ключа 3, то будете прибавлять 3 к кодам букв простого текста, и результирующим текстом будет "NLWWHQ". Если после этого зашифровать слово "NLWWHQ", только теперь с ключом 4, то получим слово "RPAALU". Но аналогичного результата можно достичь, если сразу зашифровать слово "KITTEN", используя ключ 7.

Для большинства шифров многократное повторное шифрование не приводит к повышению стойкости шифра. Более того, если зашифровать простой текст с использованием двух ключей, сумма которых равна 26, то получим зашифрованный текст, полностью совпадающий с исходным!

Резюме

Шифр Цезаря и другие подобные ему шифры не одно столетие применялись для шифрования секретной информации. Но если вы захотите вручную зашифровать длинное сообщение, например целую книгу, то на это у вас может уйти несколько дней или недель. Тут нам на помощь и приходит программирование. С шифрованием и дешифрованием больших объемов текста компьютер способен справиться менее чем за секунду!

Чтобы использовать компьютер для шифрования информации, следует освоить понятный ему язык и научиться писать программы, т.е. наборы инструкций, следуя которым компьютер будет делать то же самое, что сделали бы мы. К счастью, изучить язык программирования наподобие Python гораздо легче, чем, скажем, японский или испанский. Что касается знания математики, то от вас потребуется лишь умение выполнять операции сложения, вычитания и умножения.

В следующей главе вы узнаете о том, как применять интерактивную оболочку Python для построчного изучения программного кода.

Контрольные вопросы

Ответы на контрольные вопросы приведены в приложении Б.

1. Зашифруйте следующие фразы из книги Амброза Бирса "Словарь Сатаны" ("The Devil's Dictionary"), используя указанные ключи.
   А. "AMBIDEXTROUS: ABLE TO PICK WITH EQUAL SKILL A RIGHT-HAND POCKET OR A LEFT." (ключ 4).
   Б. "GUILLOTINE: A MACHINE WHICH MAKES A FRENCHMAN SHRUG HIS SHOULDERS WITH GOOD REASON." (ключ 17).
   В. "IMPIETY: YOUR IRREVERENCE TOWARD MY DEITY." (ключ 21).
2. Дешифруйте следующие зашифрованные фрагменты текста, используя указанные ключи.
   А. "ZXAI: P RDHIJBT HDBTIXBTH LDGCQN HRDIRWBTC XC PBTGXRP PCS PBTGXRPCHXC HRDIAPCS." (ключ 15).
   Б. "MQTSWXSV: E VMZEP EWTMVERX XSTYFPMG LSRSVW." (ключ 4).
3. Зашифруйте следующее предложение, используя ключ 0:
   "THIS IS A SILLY EXAMPLE."
4. Ниже приведены пары исходных слов и их зашифрованных версий. Какие ключи использовались в каждом случае?
   А. ROSEBUD — LIMYVOX
   Б. YAMAMOTO — PRDRDFKF
   В. ASTRONOMY — HZAYVUVTF
5. Как будет выглядеть приведенное ниже предложение, зашифрованное с помощью ключа 8, если дешифровать его с помощью ключа 9?
   "UMMSVMAA: CVKWUUWV XIBQMVKM QV XTIVVQVO I ZMDMVOMBPIB QA EWZBP EPQTM."