ПРЕДИСЛОВИЕ

Развитие информационного общества, ядром которого является сеть интернет, сделало нашу жизнь очень удобной, позволив свободно получать информацию, публикуемую на веб-сайтах, общаться по электронной почте, пользоваться услугами интернет-магазинов и интернет-банкинга.

Но, наслаждаясь этими удобствами, нам всем почему-то часто приходится слышать вызывающие некоторое беспокойство слова: «информационная безопасность», «защита личной информации» и, наконец, «шифрование». В чём же заключается проблема?

Дело в том, что пользоваться сетью – значит обмениваться по ней разнообразной информацией, в том числе и конфиденциальной, то есть такой, которую требуется держать в секрете. К ней относятся, например, номера кредитной карты и банковского счета, история болезни и кредитная история, адрес электронной почты и т. п. Попав в руки злоумышленников, такие сведения могут быть использованы для совершения различных преступлений, поэтому защита информации, несомненно, является главной задачей в области сетевых технологий. Основой для построения безопасных систем, предоставляющих разнообразные сетевые услуги с надёжной аутентификацией (установлением подлинности) данных, защитой от спуфинга (злонамеренных действий под видом законных пользователей), перехвата информации и фальсификации данных является шифрование.

За последние годы в развитии криптографии※ произошёл огромный скачок: она перестала быть уделом только специалистов по информационной безопасности и прочно вошла в жизнь обычных людей, пользующихся услугами информационных сетей.

Каким же образом шифрование обеспечивает информационную безопасность и защиту личной информации?

В этой книге на основе манги описываются механизмы шифрования и его роль в нашей жизни. Объяснения сложных математических понятий, без которых понимание криптологии невозможно, даются в легком для понимания виде, поэтому вы сможете освоить их без особого напряжения, просто следя за развитием сюжета. В самом повествовании, конечно же, тоже заложен шифр, разгадав который, читатель получит дополнительное удовольствие. Надеюсь, что эта книга поможет вам овладеть базовыми знаниями в области криптологии※ и информационной безопасности.

В завершение хотим поблагодарить коллектив Отдела разработок издательства Ohmsha и художника Хиноки Идэро, рисовавшего мангу.

Апрель 2007 *Авторы*

※ Криптография – раздел криптологии, в котором изучают собственно методы шифрования. В другом разделе криптологии – криптоанализе, – занимаются поиском уязвимости шифров.

СОДЕРЖАНИЕ

ПРОЛОГ **1**

Глава 1
ОСНОВЫ КРИПТОГРАФИИ **15**

1-1 Основные понятия криптографии **16**
- Термины криптографии 20
- Связь между ключами Ek и Dk 21

1-2 Классические шифры **24**
- Шифр Цезаря 24
- Шифр одноалфавитной замены 25
- Шифр многоалфавитной замены (шифр Виженера) 26
- Шифр перестановки 27

1-3 Стойкость шифра **28**
- Число ключей шифра многоалфавитной замены 32
- Число ключей шифра перестановки 32
- Возможность криптоанализа 35
- Совершенно стойкий шифр 35
- Типы криптостойкости 37

Глава 2
ОДНОКЛЮЧЕВОЙ ШИФР **45**

2-1 Двоичные числа и сложение по модулю 2 ..... **46**
2-2 Что такое одноключевой шифр? **57**
- Особенности одноключевого шифра 62

2-3 Устройство потокового шифра **63**
2-4 Устройство блочного шифра **66**
- Режим сцепления блоков шифртекста (CBC) 69

2-5 Устройство шифра DES **70**
- Основы строения сети Фейстеля 71
- Инволюция 72

• Генерирование ключей шифрования DES 75
• Устройство нелинейной функции f шифра DES 76
• Обобщённая модель шифрования и расшифрования DES 77
2-6 Шифры 3-DES и AES 78
• Общие сведения о шифре AES 83
Пример использования упрощённого DES 87
• Преобразование в двоичные данные 87
• Генерирование шифртекста DES 87
• Расшифрование шифртекста DES 95
• Генерирование ключей шифрования DES 100
• Генерирование ключей расшифрования DES 104

Глава 3
ШИФР С ОТКРЫТЫМ КЛЮЧОМ 107

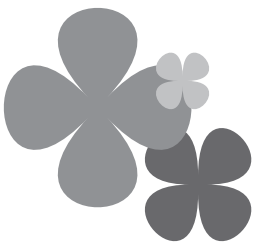
3-1 Основы шифра с открытым ключом 108
• Основные разновидности шифра с открытым ключом 117
• Односторонние функции 118
• Рождение шифра RSA 121
3-2 Простые числа и факторизация 122
• Тест на простоту 131
3-3 Модульная арифметика 136
• Сложение по модулю и вычитание по модулю 139
• Умножение по модулю и деление по модулю 148
3-4 Малая теорема Ферма и теорема Эйлера 154
• Ферма – отец теории чисел 155
• Тест Ферма и псевдопростые числа 157
• Теорема Эйлера 158
• Математик Эйлер 159
• Функция Эйлера от произведения двух простых чисел 160
3-5 Устройство шифра RSA 163
• Шифрование и расшифрование RSA 165
• Метод генерирования ключей RSA 167

• Генерирование открытого и секретного ключей 169
• Генерирование шифртекста RSA 171
• Расшифрование RSA 173
3-6 Шифр с открытым ключом и задача дискретного логарифмирования 175
• Задача дискретного логарифмирования 176
• Шифрование и расшифрование Эль-Гамаля 178
Расширенный алгоритм Евклида 183

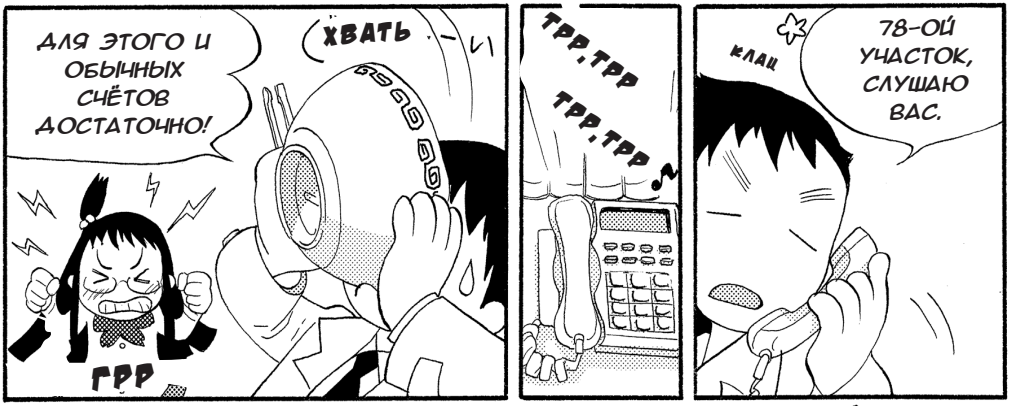
Глава 4
КАК ИСПОЛЬЗУЮТ ШИФР НА ПРАКТИКЕ? 187

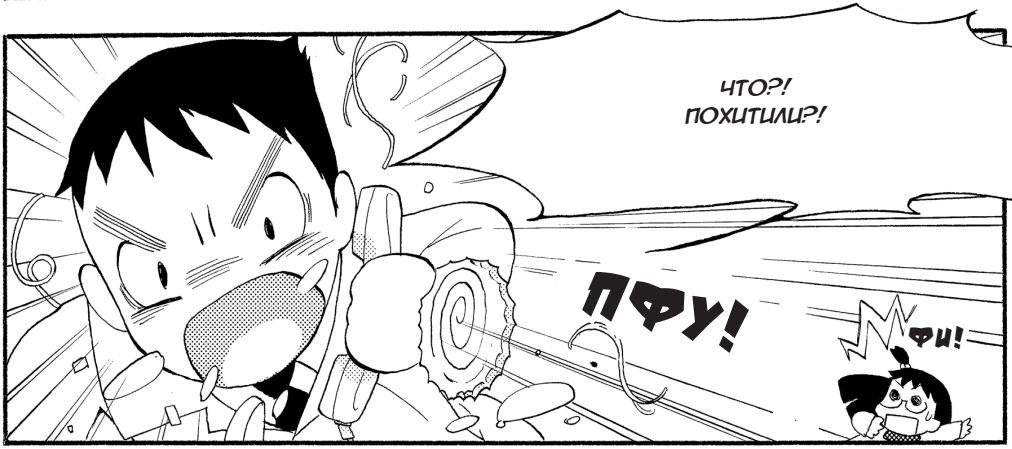
4-1 Гибридные криптосистемы 188
4-2 Хеш-функция и код аутентификации сообщения 192
• Подмена данных 192
• Защита от подмены 194
• Хеш-функция 195
• Спуфинг 196
• Защита от спуфинга 197
• Устройство имитовставки 198
• Отказ 199
• Два недостатка имитовставки 201
4-3 Цифровая подпись 202
• Защита от отказа 202
• Устройство цифровой подписи 203
• Атака посредника 205
• Защита от атаки посредника 206
• Сертификат и удостоверяющий центр 206
4-4 Инфраструктура открытых ключей (ИОК) 208
Доказательство с нулевым разглашением 219
Разъяснение некоторых терминов 225
Список использованной литературы 227
Предметный указатель 228

ПРОЛОГ

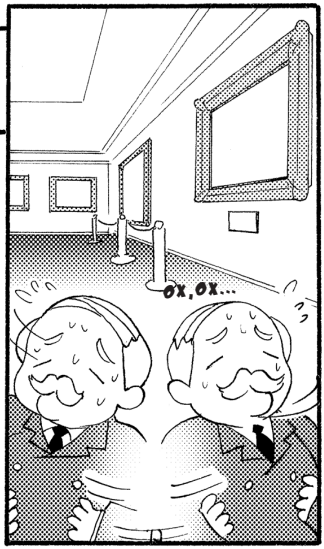



Полицейский участок № 78
в каком-то городе
Безопасность дорожного движения
отдел
.....
Приёмная
Мегуро Рика
БРАТЕЦ, НУ КУПИ!
Мегуро
помощник инспектора
НЕТ! КОМПЬЮТЕР ДЛЯ ШКОЛЬНИЦЫ - СЛИШКОМ БОЛЬШАЯ РОСКОШЬ!
ФШШ
ОН НУЖЕН МНЕ ДЛЯ ИЗУЧЕНИЯ МАТЕМАТИКИ!
$ax + by = gcd(a,b)$
$a^{p-1} \equiv 1 \pmod{p}$
$\varphi(p) = p - 1$
x
y^2
.....
ХОЧУ!


ДЛЯ ЭТОГО И ОБЫЧНЫХ СЧЁТОВ ДОСТАТОЧНО!
ХВАТЬ
ГРР
ТРР,ТРР
ТРР,ТРР
КЛАЦ
78-ОЙ УЧАСТОК, СЛУШАЮ ВАС.


ЧТО?! ПОХИТИЛИ?!
ПФУ!
ФИ!

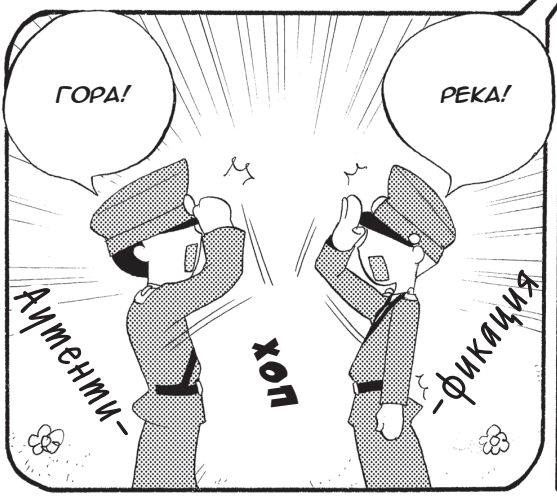

Музей исскуств «Мраморный»
ВИУ
ВИУ
ПРОВЕРЬТЕ ЗАПАДНОЕ КРЫЛО!
ПЕРЕКРОЙТЕ ВОН ТОТ ВЫХОД!
ВОСТОЧНОЕ КРЫЛО!


ОХ,ОХ...


ТАК... ЗНАЧИТ, ПОХИЩЕНА ЗНАМЕНИТАЯ КАРТИНА, КОТОРУЮ ТЩАТЕЛЬНО ОХРАНЯЛИ?

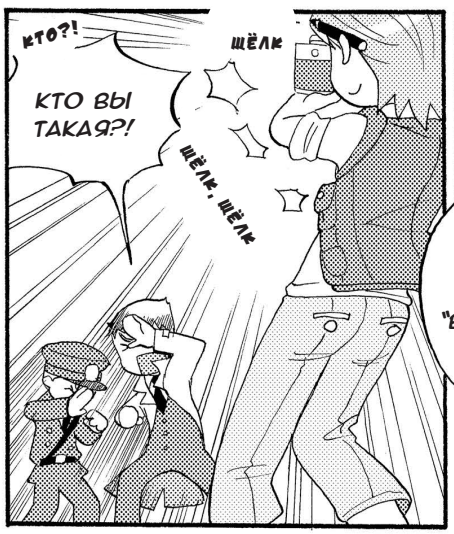

ОХ! НЕ МОГУ ПОВЕРИТЬ!
ЭТО БЫЛА "УЛЫБКА МАДОННЫ" СТОИМОСТЬЮ 300 МЛН ЕН!
ПОЛИЦИЯ ДЕЙСТВИТЕЛЬНО ХОРОШО ОХРАНЯЛА?
...


ЗА БЕЗОПАСНОСТЬЮ СЛЕДИЛИ ХОРОШО?
ТАК ТОЧНО!
ВСЕХ ДЕЖУРНЫХ ПРОВЕРЯЛИ
ПО СИСТЕМЕ "ПАРОЛЬ-ОТЗЫВ"!

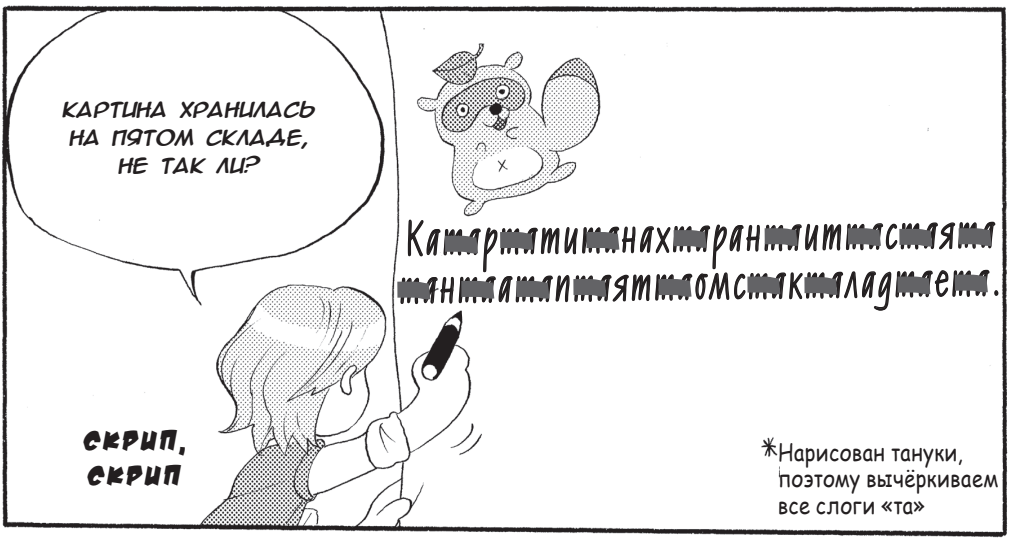

ГОРА!
РЕКА!
Аутентификация
ХОП

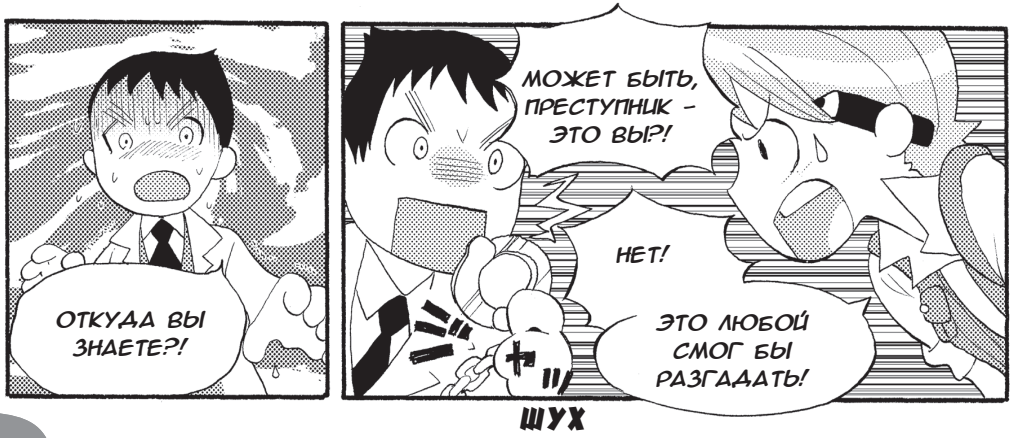

ЯСНО! ВСЁ ПРАВИЛЬНО!
АХ...
УРОВЕНЬ МЛАДШЕЙ ШКОЛЫ...
УЙ

※ Изображена енотовидная собака тануки.

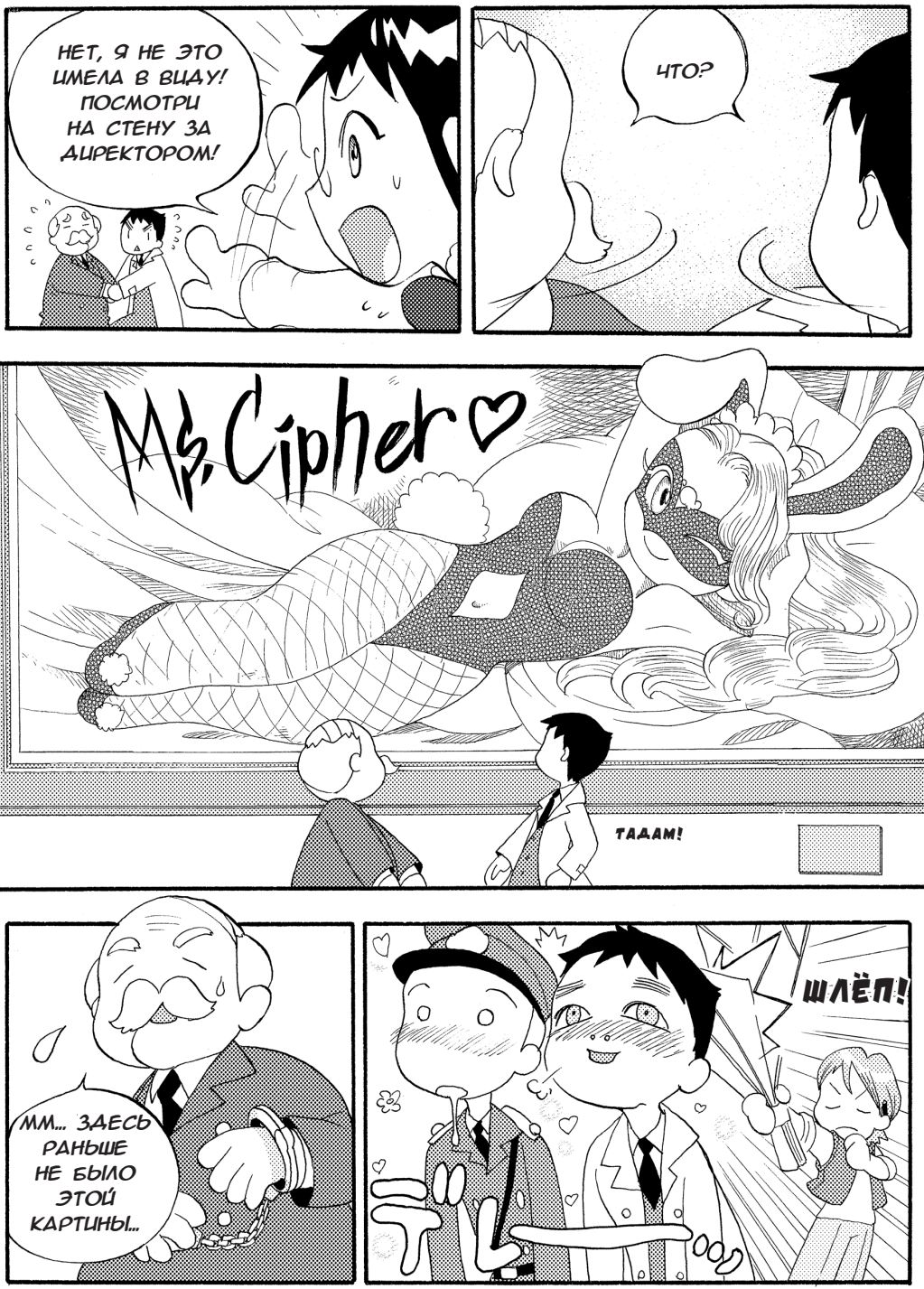



КАК?! ГАЗЕТЧИКИ УЖЕ ВСЁ ПРОНЮХАЛИ?
ЧТО БЫЛО НЕ ТАК С БЕЗОПАСНОСТЬЮ?!
ПАРОЛЬ И ШИФР НИКУДА НЕ ГОДЯТСЯ!
ЧТО?! ПОЧЕМУ?!


КАРТИНА ХРАНИЛАСЬ НА ПЯТОМ СКЛАДЕ, НЕ ТАК ЛИ?
Катартинанахранитастаятанатапятомскладтета.
СКРИП, СКРИП
*Нарисован тануки, поэтому вычёркиваем все слоги «та»

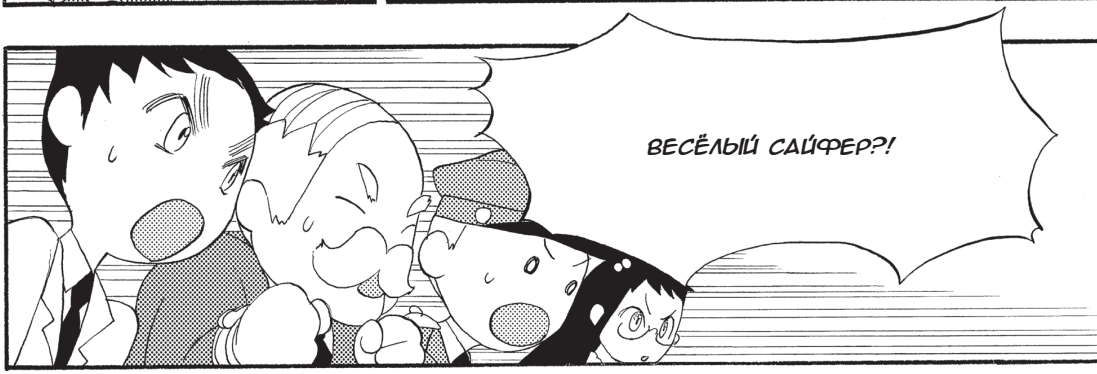

ОТКУДА ВЫ ЗНАЕТЕ?!
МОЖЕТ БЫТЬ, ПРЕСТУПНИК – ЭТО ВЫ?!
НЕТ!
ЭТО ЛЮБОЙ СМОГ БЫ РАЗГАДАТЬ!
ШУХ

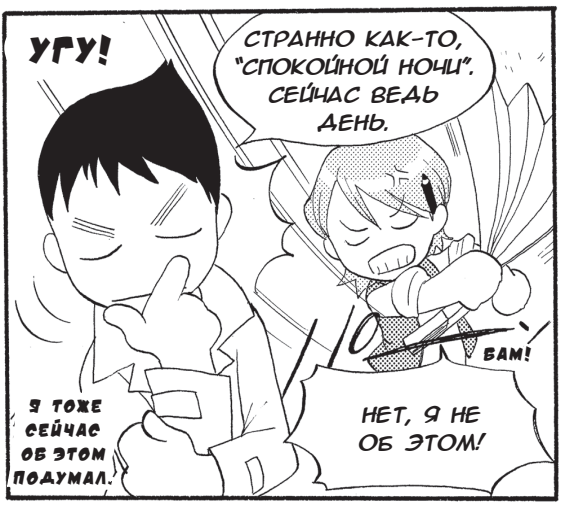

КАК? НЕУЖЕЛИ?
ИНСПЕКТОР МЭГУРО, НЕ ТРАТЬТЕ ВРЕМЯ! ПОСКОРЕЕ НАЙДИТЕ ПРЕСТУПНИКА!
ГРР...
ДА... ПРЕСТУПНИКА..
ВОТ ОН, ПРЕСТУПНИК!
ЧТО?!
ДИРЕКТОР, ВЫ АРЕСТОВАНЫ!
ЩЁЛК!
ОЙ!


НЕТ, Я НЕ ЭТО ИМЕЛА В ВИДУ! ПОСМОТРИ НА СТЕНУ ЗА ДИРЕКТОРОМ!
ЧТО?
Ms. Cipher♡
ТАДАМ!
ММ... ЗДЕСЬ РАНЬШЕ НЕ БЫЛО ЭТОЙ КАРТИНЫ...
ШЛЁП!
ГЛЫГ

Я – Весёлый сайфер.
Это я украла картину.
В следующий раз
украду VDVIRCU.

Спокойной ночи ♥






Это я украла картину.
В следующий раз украду VDVIRCU.
ЭТО ЖЕ ШИФР! УКАЗАНА ВЕЩЬ, КОТОРАЯ БУДЕТ УКРАДЕНА СЛЕДУЮЩЕЙ.
ЧТО ОЗНАЧАЕТ ЭТО VDVIRCU?
У МЕНЯ С АНГЛИЙСКИМ НЕ ОЧЕНЬ...
ЭХ...
НО ЭТО ЯВНО НЕ ШИФР "ТАНУКИ": ВЫЧЁРКИВАНИЕ БУКВ НЕ ДАЁТ НИЧЕГО ОСМЫСЛЕННОГО.
ДАВАЙТЕ ТОГДА ИЗУЧИМ КРИПТОЛОГИЮ И ПОКАЖЕМ ЭТОМУ ВЕСЁЛОМУ САЙФЕРУ!
(ГОРЯЧО)
ЭТО ЖЕ НЕ ШПИОНСКИЙ РОМАН.... КАКОЙ НАМ ПРОК ОТ ЭТИХ ШИФРОВ?

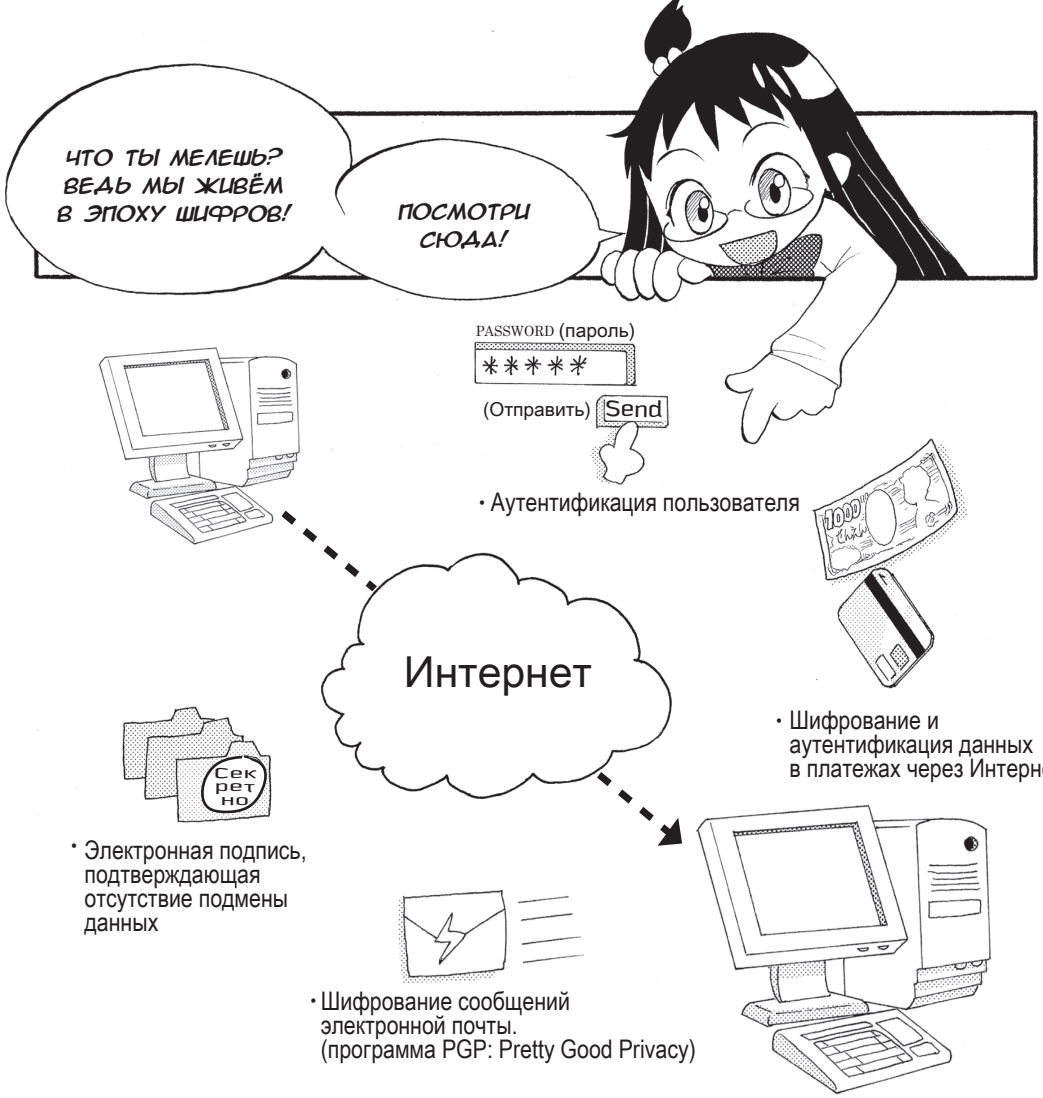
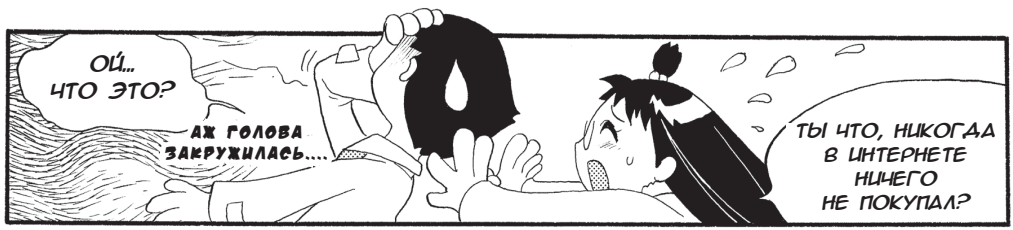


Рис. 0.1. Роль криптографии в современном обществе

Как показано на рис. 0.1, в нашу эпоху компьютеров и связи шифрование незаменимо для борьбы с подменой данных, перехвата информации и т. п.



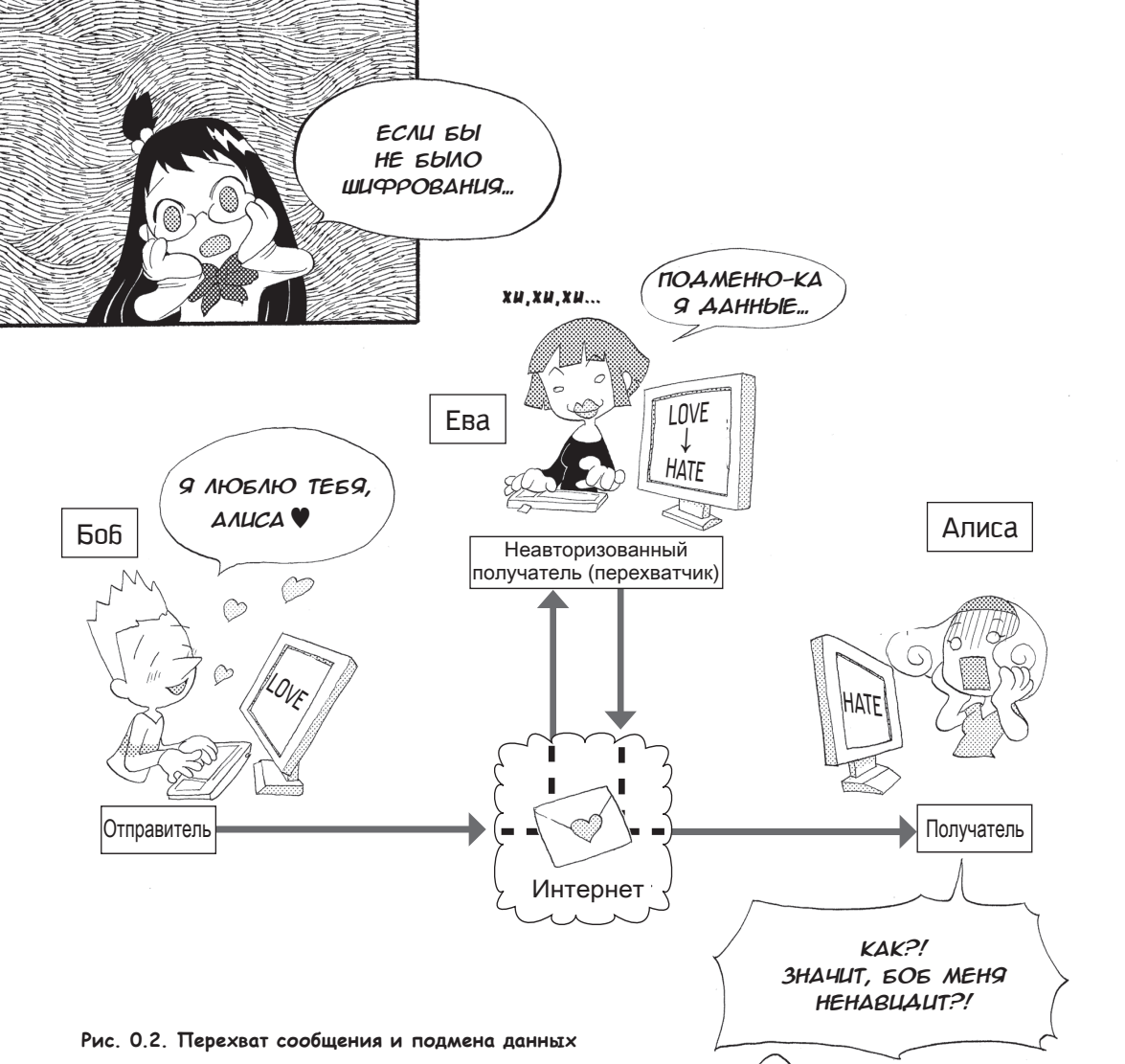
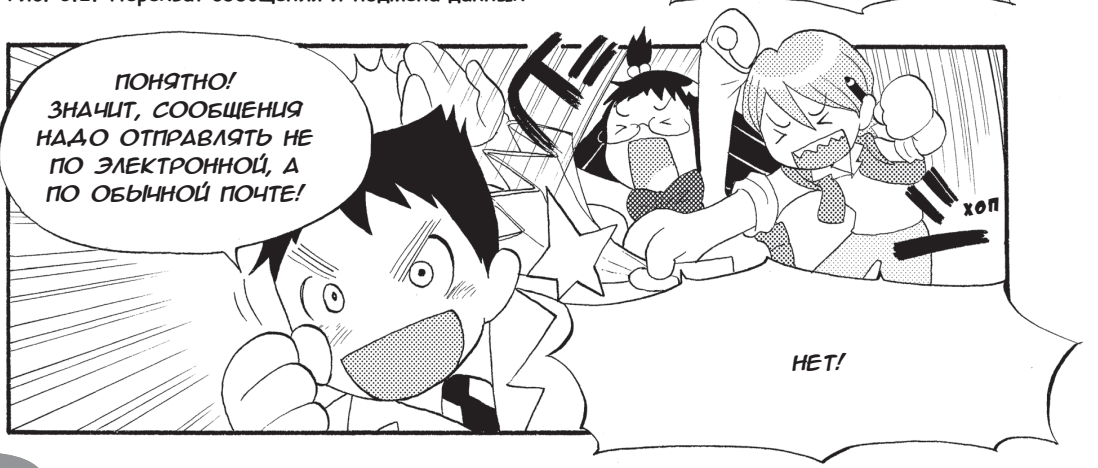


Рис. 0.2. Перехват сообщения и подмена данных



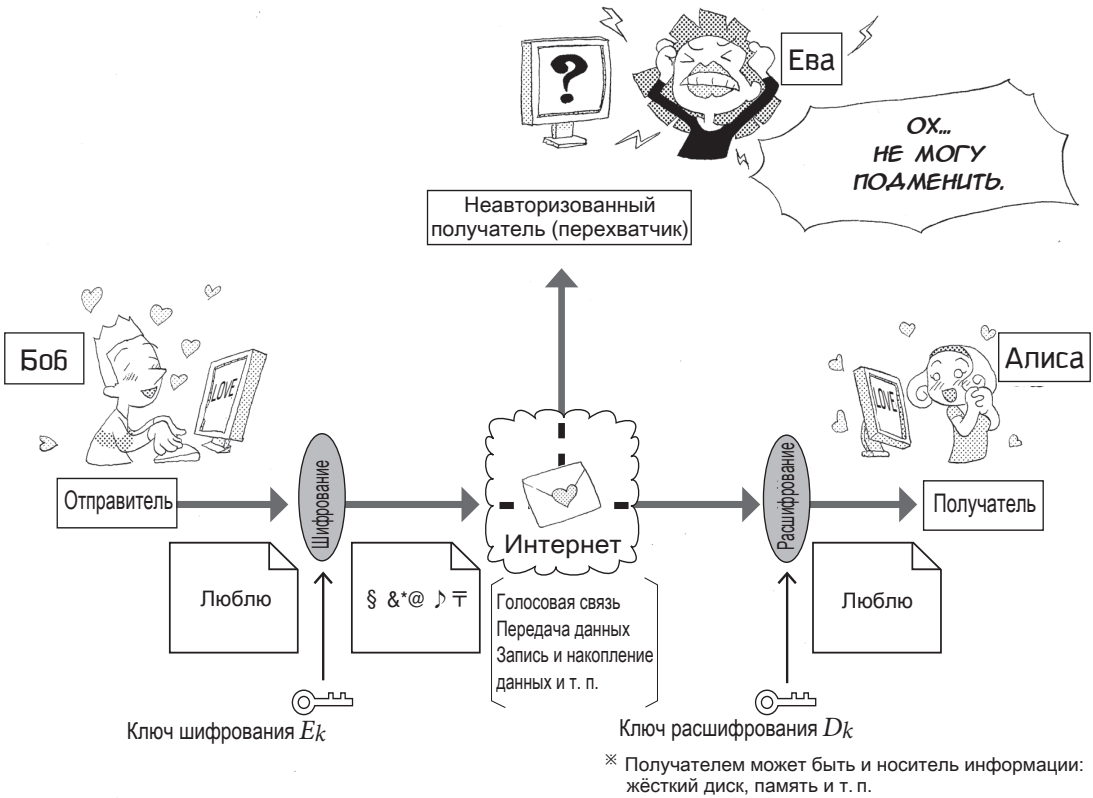
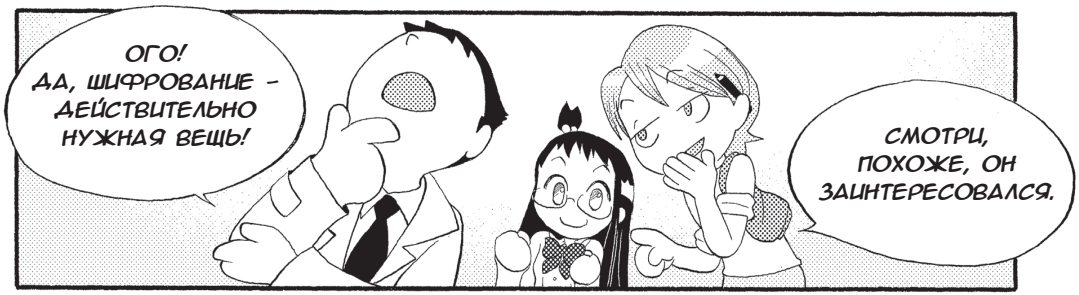


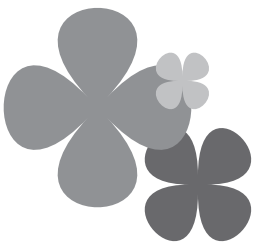
Рис. 0.3. Модель шифрования (криптосистема)



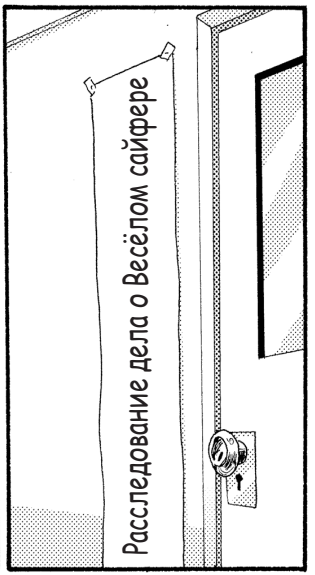

ЕСЛИ ХОЧЕШЬ,
Я МОГУ ПРЕПОДАВАТЬ
ТЕБЕ ШИФРОВАНИЕ!
ДА, ХОЧУ!
Я ИЗУЧУ ШИФРОВАНИЕ
И ПОЙМАЮ САЙФЕРА!
ИНСПЕКТОР...
УВАЖАЕМЫЙ ДИРЕКТОР,
НЕ БЕСПОКОЙТЕСЬ!
ПРЕСТУПЛЕНИЕ СКОРО
БУДЕТ РАСКРЫТО!
ОХ...
СНИМИТЕ
С МЕНЯ
НАРУЧНИКИ!

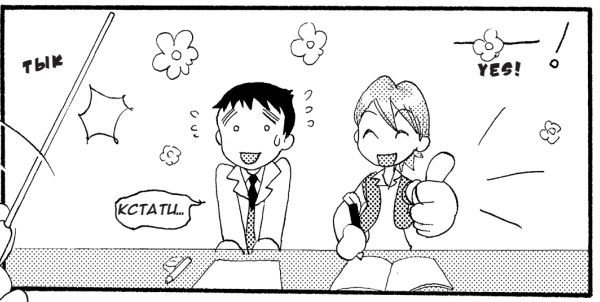
ГЛАВА 1

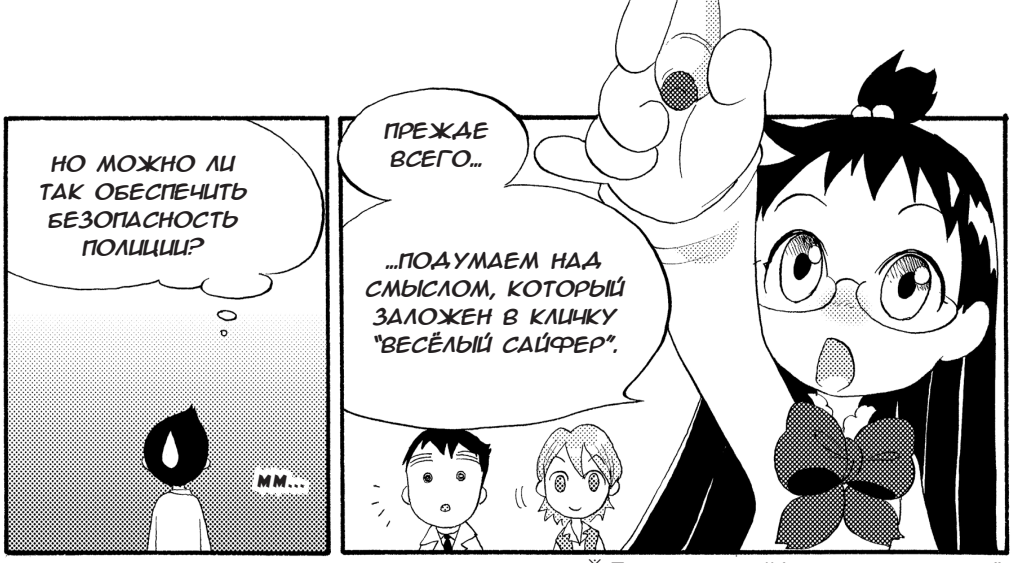
ОСНОВЫ КРИПТОГРАФИИ



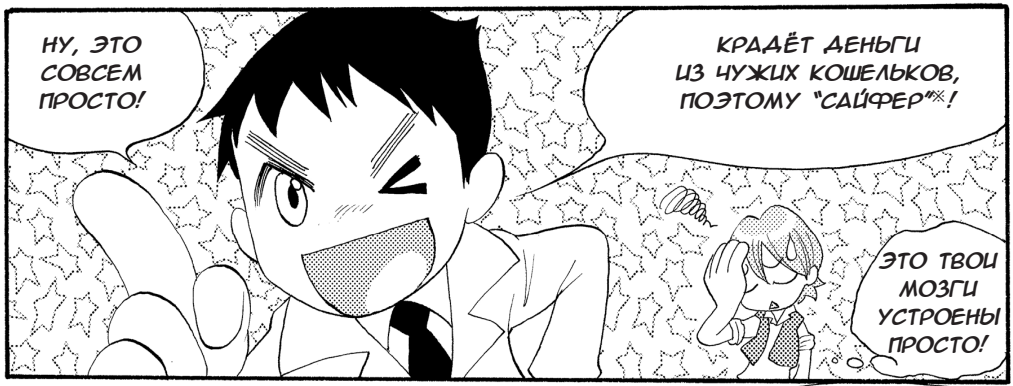
1-1 Основные понятия криптографии

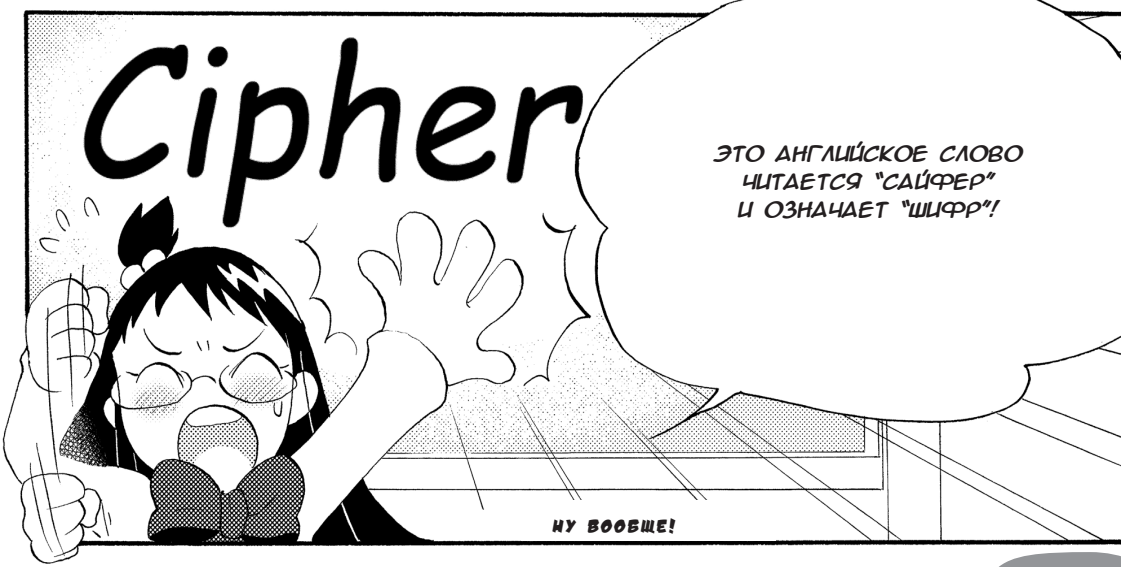






※ По-японски «сайфу» означает «кошелёк».



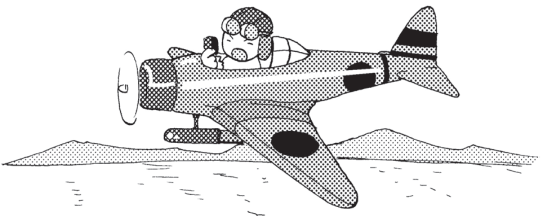


«Ниитака-яма ноборэ» ※1 = «Начать атаку»

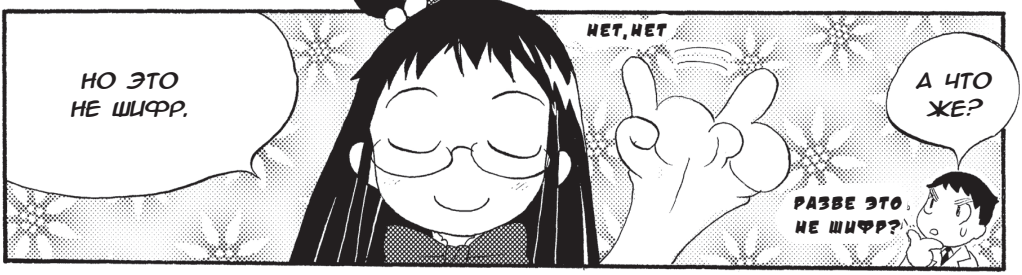
«Тора тора тора» ※2 = «Атака была успешной»

※1 Дословно: «Поднимайтесь на гору Ниитака».

※2 Дословно: «Тигр, тигр, тигр».



※ Обе кодовые фразы использовались Императорским флотом Японии при нападении на Пёрл-Харбор во время Второй мировой войны.



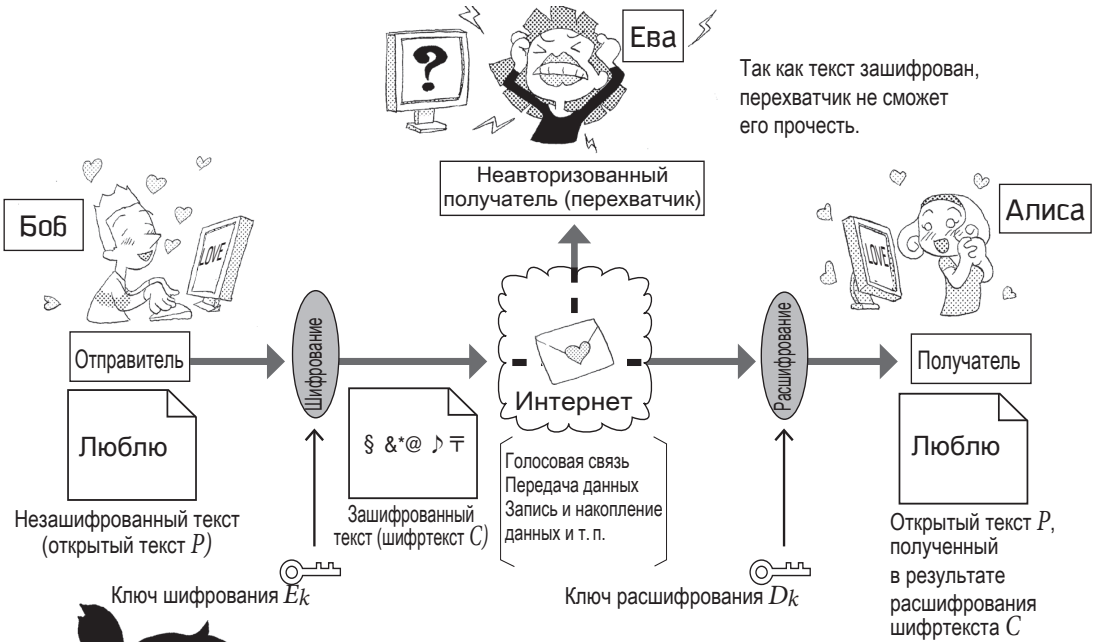
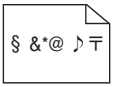


Рис. 1.1. Модель шифрования (криптосистема, шифр)

✤ Термины криптографии

Открытый текст *P* (Plain text): обычный незашифрованный текст.

Шифртекст *C* (Cipher text): зашифрованный текст. Другое название – криптограмма.



Шифрование (Encryption/Encipherment): преобразование открытого текста в шифртекст.

Расшифрование (Decryption/Decipherment): преобразование шифртекста в открытый текст.

Ключ шифрования E_k (Encryption Key): ключ, используемый для шифрования.

Ключ расшифрования D_k (Decryption Key): ключ, используемый для расшифрования.

✽ Связь между ключами E_k и D_k

Отправитель зашифровывает открытый текст: используя открытый текст P и ключ шифрования E_k (функцию шифрования), он генерирует шифртекст C.

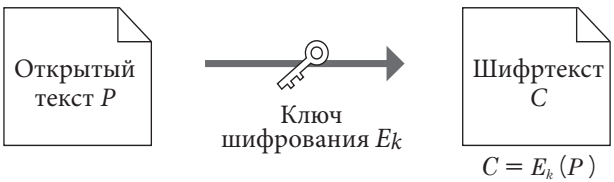
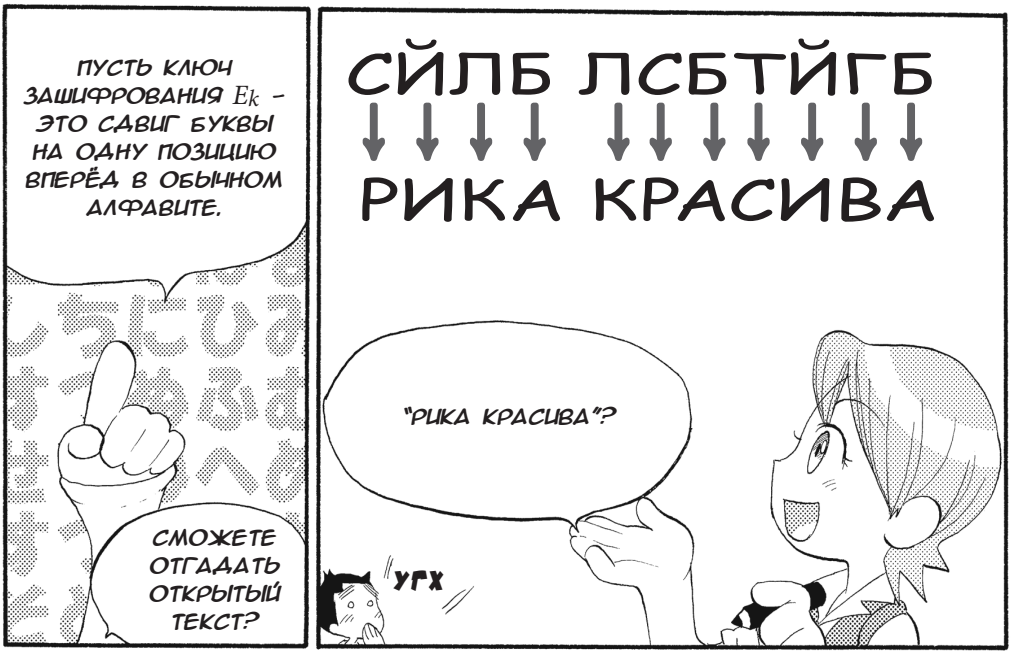


Рис. 1.2. Шифрование с использованием ключа E_k

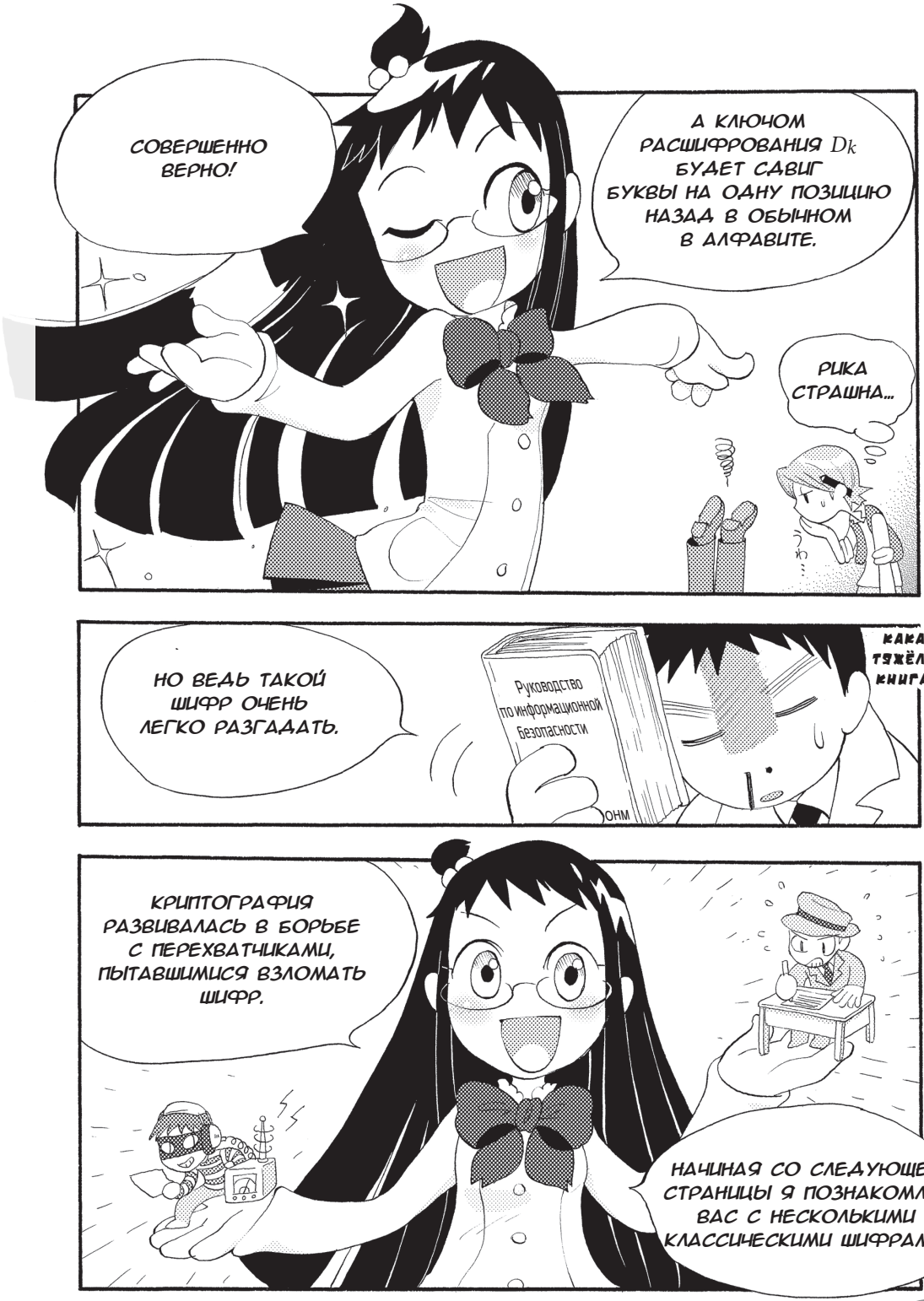
Получатель расшифровывает шифртекст: используя шифртекст C и ключ расшифрования D_k (функцию расшифрования), он генерирует открытый текст P.

Рис. 1.3. Расшифрование с использованием ключа D_k


А ТЕПЕРЬ – ЗАДАЧКА!
СЙЛБ ЛСБТЙГБ
СКРИП, СКРИП


ПУСТЬ КЛЮЧ ЗАШИФРОВАНИЯ Ek – ЭТО СДВИГ БУКВЫ НА ОДНУ ПОЗИЦИЮ ВПЕРЁД В ОБЫЧНОМ АЛФАВИТЕ.
СМОЖЕТЕ ОТГАДАТЬ ОТКРЫТЫЙ ТЕКСТ?
СЙЛБ ЛСБТЙГБ
РИКА КРАСИВА
"РИКА КРАСИВА"?
УГХ


ТУДУХ
ХА,ХА,ХА! "РИКА КРАСИВА" – ЭТО ОЧЕВИДНАЯ ВСЕМ ОШИБ...
БАХ
РИ!

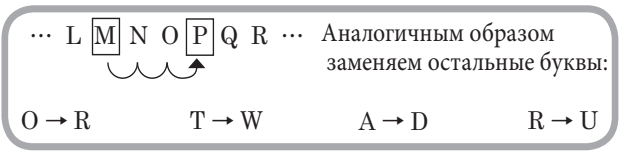

СОВЕРШЕННО ВЕРНО!
А КЛЮЧОМ РАСШИФРОВАНИЯ D_k БУДЕТ СДВИГ БУКВЫ НА ОДНУ ПОЗИЦИЮ НАЗАД В ОБЫЧНОМ В АЛФАВИТЕ.
РИКА СТРАШНА...
НО ВЕДЬ ТАКОЙ ШИФР ОЧЕНЬ ЛЕГКО РАЗГАДАТЬ.
Руководство по информационной безопасности
ОНМ
КАКАЯ ТЯЖЁЛАЯ КНИГА...
КРИПТОГРАФИЯ РАЗВИВАЛАСЬ В БОРЬБЕ С ПЕРЕХВАТЧИКАМИ, ПЫТАВШИМИСЯ ВЗЛОМАТЬ ШИФР.
НАЧИНАЯ СО СЛЕДУЮЩЕЙ СТРАНИЦЫ Я ПОЗНАКОМЛЮ ВАС С НЕСКОЛЬКИМИ КЛАССИЧЕСКИМИ ШИФРАМИ.

1-2 Классические шифры

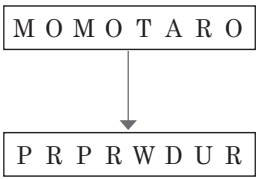
❀ Шифр Цезаря

Каждая буква открытого текста заменяется на букву, сдвинутую относительно неё на *n* позиций в алфавите. В качестве примера попробуем зашифровать слово MOMOTARO.

Примем $n = 3$.

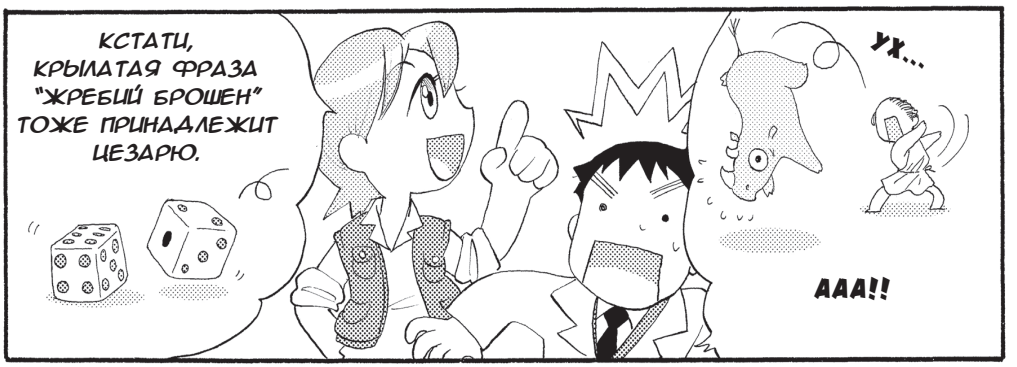


Таким образом, у нас получится шифртекст.

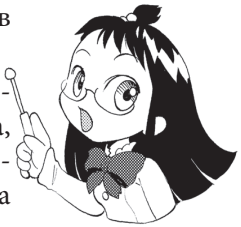


Последним трём буквам алфавита соответствуют первые.

Цезарь – это древнеримский полководец и политик Гай Юлий Цезарь (100 г. до н. э. – 44 г. до н. э.), придумавший этот шифр во время Галльской войны для обмена с союзниками сообщениями, которые не мог прочесть неприятель.



✤ Шифр одноалфавитной замены



Если немного усложнить шифр Цезаря, изменяя сдвиг в зависимости от буквы, то мы получим шифр замены.

Шифр замены, в котором есть взаимно-однозначное соответствие между буквами открытого текста и шифртекста, называется шифром одноалфавитной (или простой) замены. Шифр Цезаря тоже является разновидностью шифра одноалфавитной замены.

Положим, что 26 букв английского алфавита заменяются так, как показано ниже.

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

Правило замены σ («сигма»)

Тогда шифрование будет осуществляться следующим образом.

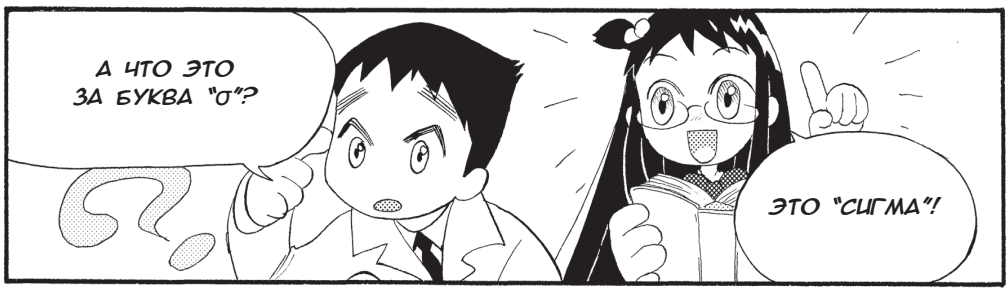
M	O	M	O	T	A	R	O
↓							
D	G	D	G	Z	Q	K	G

(Открытый текст *P)*

Заменяем буквы по правилу замены σ

(Шифртекст *C)*

В этом шифре алгоритмом является замена букв, а ключом шифрования E_k – правило замены σ.



❖ Шифр многоалфавитной замены (шифр Виженера)

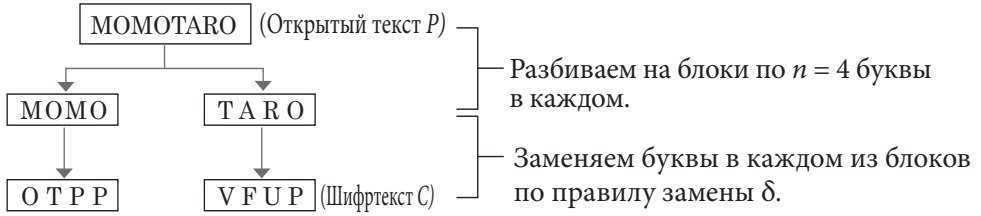
Разбив открытый текст на блоки по n букв в каждом, изменяют величину сдвига в зависимости от позиции каждой буквы внутри блока. Можно сказать, что шифр Виженера является расширением шифра Цезаря.

Положим $n = 4$ и определим правило замены δ следующим образом.

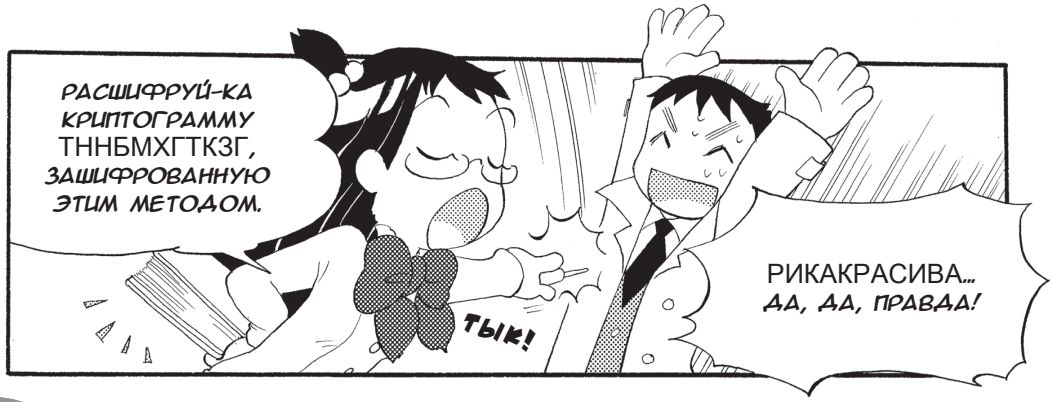
1-я буква → сдвиг = 2
2-я буква → сдвиг = 5
3-я буква → сдвиг = 3
4-я буква → сдвиг = 1

Правило замены δ

В этом случае мы получим следующий шифртекст.



В данном шифре ключ шифрования – это длина блока и правило замены, то есть последовательность величин сдвига.



✤ Шифр перестановки

Разбив открытый текст на блоки по n букв в каждом, меняют местами буквы в каждом из блоков.

Положим $n = 4$ и определим правило перестановки τ следующим образом.

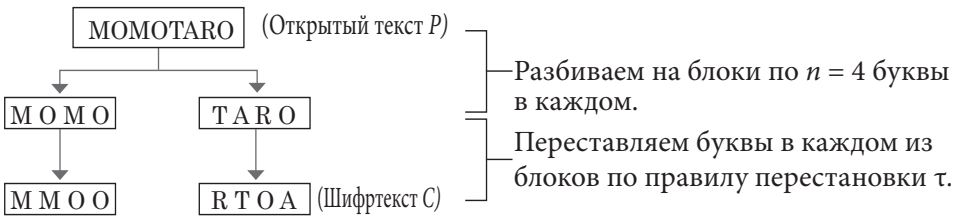
$$\tau = \begin{pmatrix} 1234 \\ 2413 \end{pmatrix}$$

Верхняя формула означает, что перестановка осуществляется следующим образом.

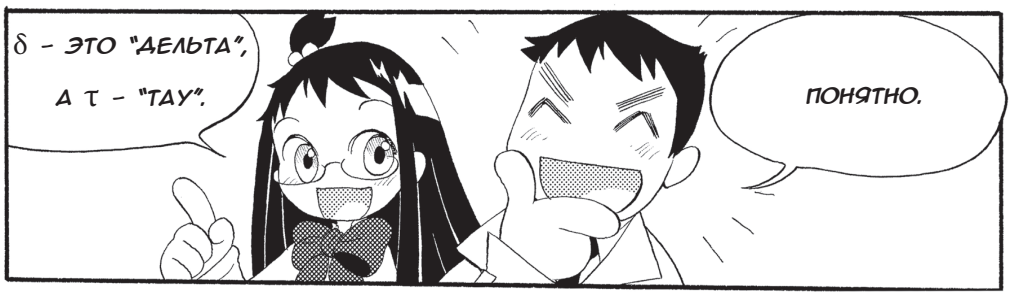
1-я буква → 2-я буква
2-я буква → 4-я буква
3-я буква → 1-я буква
4-я буква → 3-я буква

Правило перестановки τ

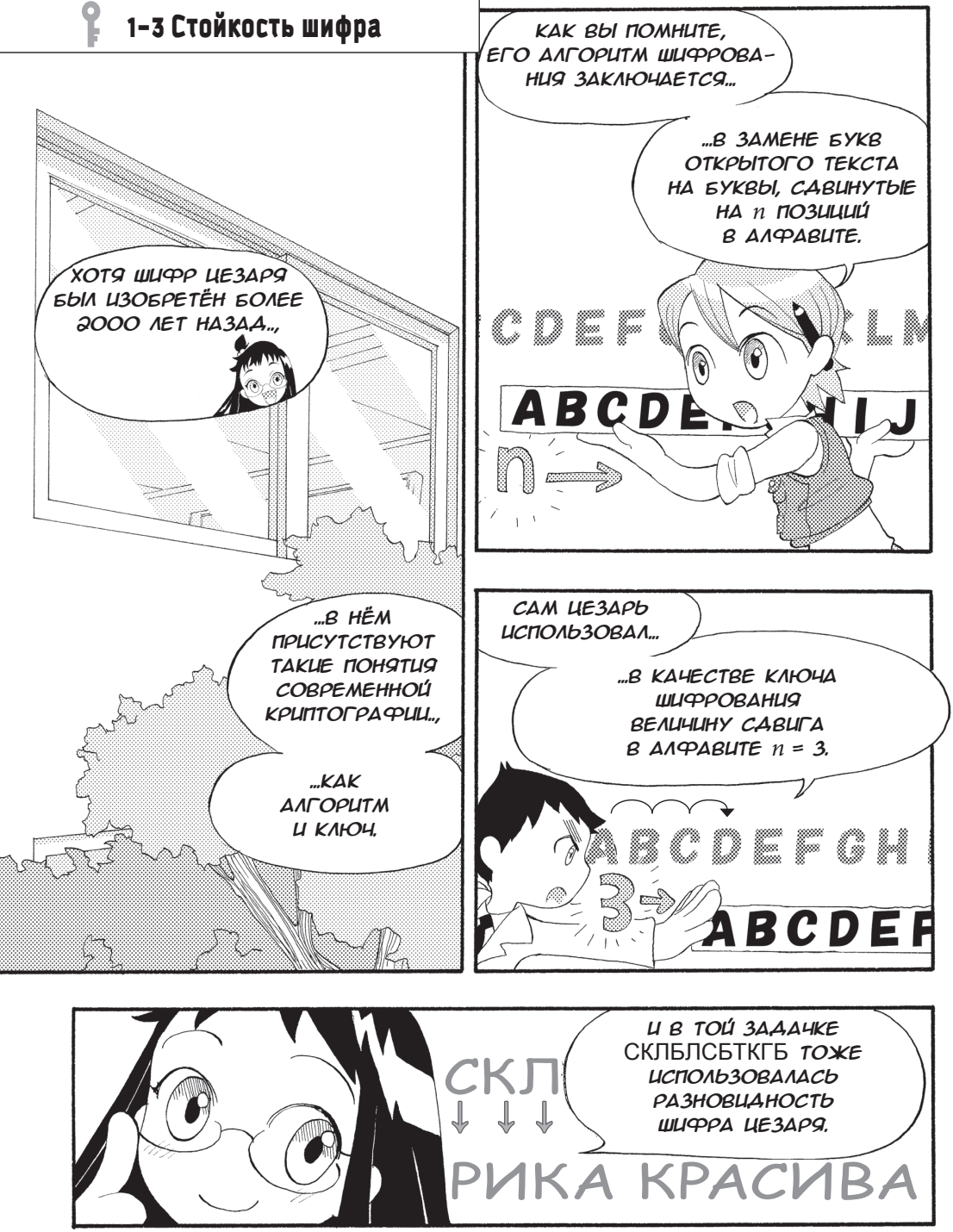
В этом случае мы получим следующий шифртекст.

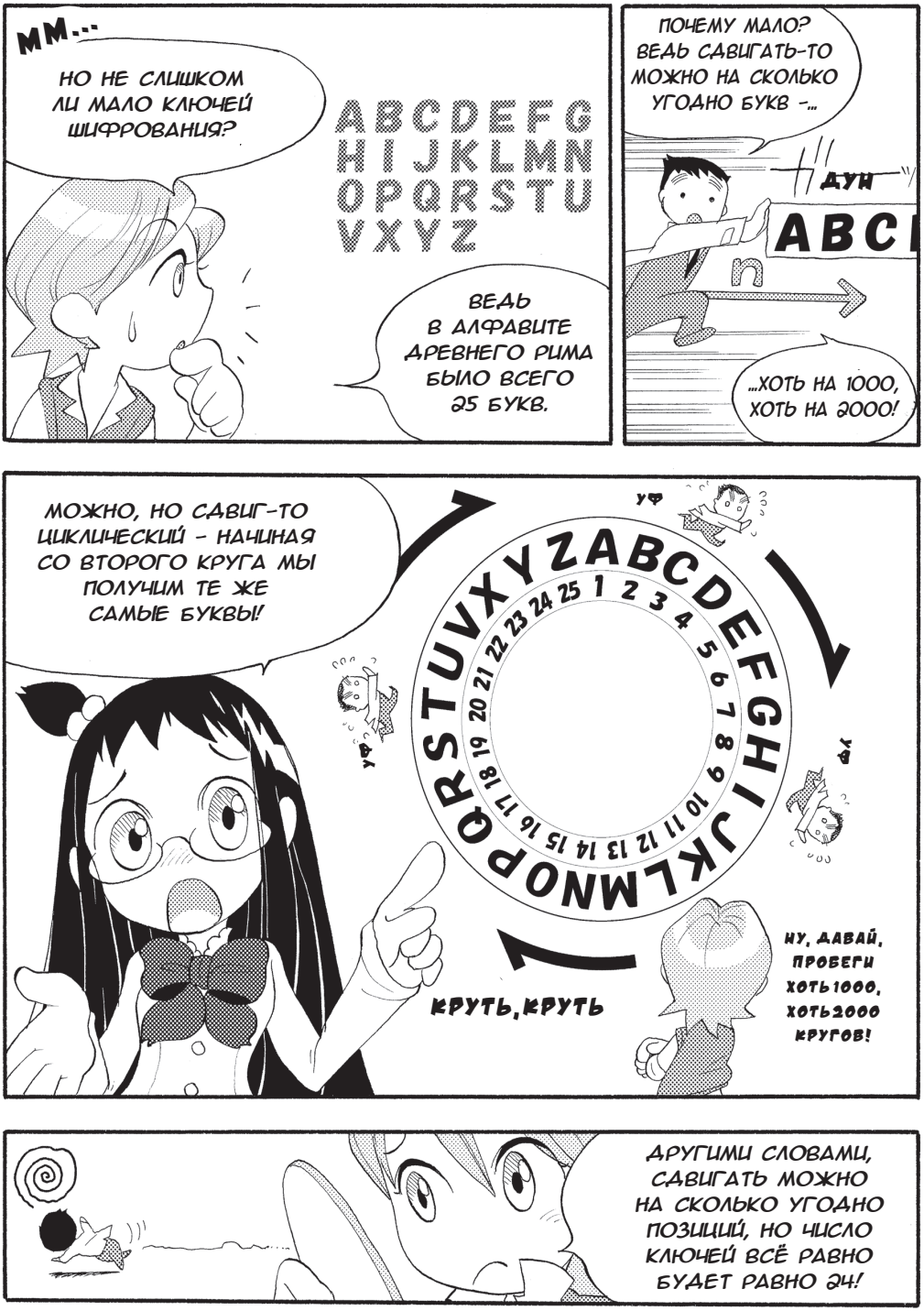


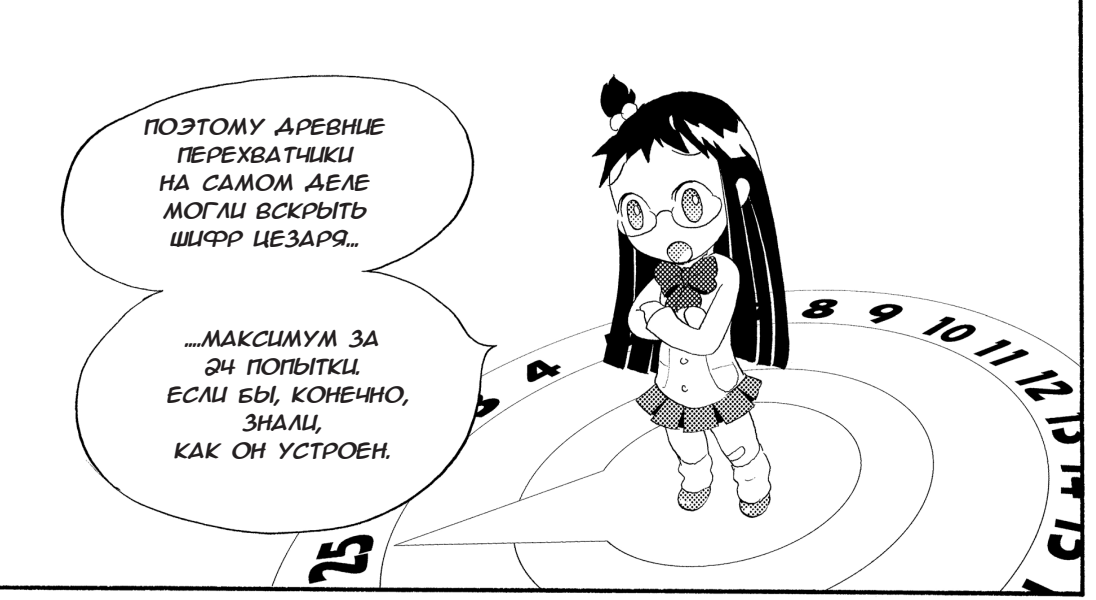
В данном шифре алгоритм шифрования – изменение порядка следования букв, а ключ шифрования – длина блока и правило перестановки.



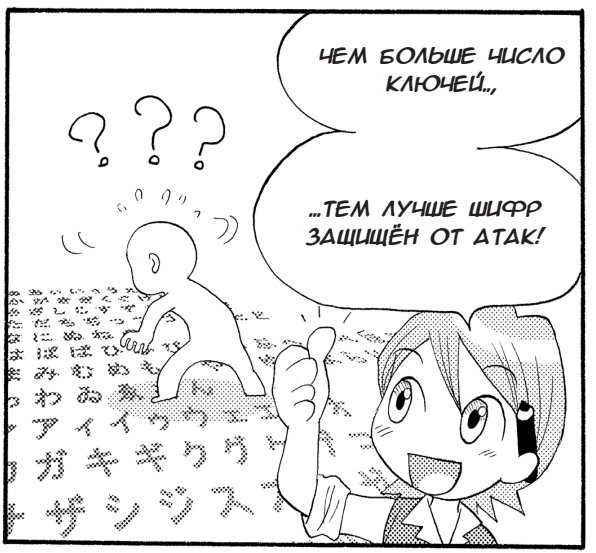
1-3 Стойкость шифра




ММ...
НО НЕ СЛИШКОМ ЛИ МАЛО КЛЮЧЕЙ ШИФРОВАНИЯ?
A B C D E F G
H I J K L M N
O P Q R S T U
V X Y Z
ВЕДЬ В АЛФАВИТЕ ДРЕВНЕГО РИМА БЫЛО ВСЕГО 25 БУКВ.
ПОЧЕМУ МАЛО? ВЕДЬ САВИГАТЬ-ТО МОЖНО НА СКОЛЬКО УГОДНО БУКВ -...
ДУН
A B C
...ХОТЬ НА 1000, ХОТЬ НА 2000!
МОЖНО, НО САВИГ-ТО ЦИКЛИЧЕСКИЙ - НАЧИНАЯ СО ВТОРОГО КРУГА МЫ ПОЛУЧИМ ТЕ ЖЕ САМЫЕ БУКВЫ!
УФ
УФ
УФ
A B C D E F G H I J K L M N O P Q R S T U V X Y Z
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
КРУТЬ, КРУТЬ
НУ, ДАВАЙ, ПРОБЕГИ ХОТЬ 1000, ХОТЬ 2000 КРУГОВ!
ДРУГИМИ СЛОВАМИ, САВИГАТЬ МОЖНО НА СКОЛЬКО УГОДНО ПОЗИЦИЙ, НО ЧИСЛО КЛЮЧЕЙ ВСЁ РАВНО БУДЕТ РАВНО 24!


ПОЭТОМУ ДРЕВНИЕ ПЕРЕХВАТЧИКИ НА САМОМ ДЕЛЕ МОГЛИ ВСКРЫТЬ ШИФР ЦЕЗАРЯ...
....МАКСИМУМ ЗА 24 ПОПЫТКИ. ЕСЛИ БЫ, КОНЕЧНО, ЗНАЛИ, КАК ОН УСТРОЕН.
25
8 9 10 11 12


НО ЕСЛИ ИСПОЛЬЗОВАТЬ, НАПРИМЕР, ЗНАКИ ЯПОНСКОГО ЯЗЫКА...
АГА!
ЭВРИКА!
...АЛФАВИТЫ ХИРАГАНУ, КАТАКАНУ И ИЕРОГЛИФЫ В ПРИДАЧУ, – ТО ЧИСЛО КЛЮЧЕЙ ПРЕВЫСИТ 10 ТЫСЯЧ!


ЧЕМ БОЛЬШЕ ЧИСЛО КЛЮЧЕЙ...,
...ТЕМ ЛУЧШЕ ШИФР ЗАЩИЩЁН ОТ АТАК!


ИТАК, ТЕПЕРЬ МЫ ПОСМОТРИМ ЧИСЛО КЛЮЧЕЙ В ДРУГИХ ШИФРАХ.

✤ Число ключей шифра одноалфавитной замены

Будем считать, что в этом и в последующих шифрах используется английский алфавит, состоящий из 26 букв. Общее число ключей шифра замены будет равно числу перестановок множества из 26 букв, рассчитываемому по следующей формуле:

$$P_{26} = 26! = 26 \times 25 \times 24 \times \cdots \times 3 \times 2 \times 1 \approx 4.03291461 \times 10^{26}.$$

Перестановкой (Permutation) *n* элементов называется любой упорядоченный набор этих элементов. Полученное выше значение является довольно большим: время поиска ключа (временная сложность криптоанализа) на компьютере, перебирающем 100 млн перестановок в секунду, может составить до 128 млрд лет.

Таким образом, хотя теоретически ключ найти возможно, практически шифр одноалфавитной замены считается вычислительно стойким.

Однако известно, что этот шифр уязвим для частотного криптоанализа, использующего такую его особенность, как совпадение частот появления букв в открытом тексте и шифртексте.

В связи с этим с практической точки зрения вычислительно криптостойким считается шифр одноалфавитной замены с одноразовым ключом (one time pad).

Теперь поговорим о разделе математики под названием комбинаторика. Кроме вышеописанной перестановки, существуют также понятия размещения и сочетания. Размещение из *n* по *r* – это упорядоченный набор *r* элементов, выбранных из множества *n* различных элементов. Таким образом, перестановка тоже является частным случаем размещения. Число размещений вычисляется по нижеприведённой формуле.

$${}_nA_r = n \times (n-1) \times (n-2) \times \cdots\cdots \times (n-r+1) = \frac{n!}{(n-r)\ !}.$$

Сочетание из *n* по *r* – это набор *r* элементов, выбранных из множества *n* различных элементов. Оно обозначается заглавной буквой *C*, от слова Combination.

$${}_nC_r = \frac{{}_nP_r}{r!} = \frac{n!}{(n-r)\ !\ r!}.$$

Различие между размещением и сочетанием заключается в том, что в размещении важен порядок следования элементов, поэтому AB и BA будут разными размещениями, а сочетание – это способ выбора элементов из множества, а порядок их следования здесь не важен, поэтому AB и BA будут одинаковыми сочетаниями. Кстати, восклицательный знак (!) – это факториал. Знак факториала после *n* означает произведение всех чисел от 1 до *n* включительно.

$$n! = n \times (n-1)\ \cdots\cdots \times 3 \times 2 \times 1.$$

✤ Число ключей шифра многоалфавитной замены

Примем длину одного блока равной n буквам. Так как сдвиги букв в блоке нам неизвестны, мы должны будем перебрать 26 значений сдвига 1-й позиции, для каждого из значений сдвига 1-й позиции – по 26 значений сдвига 2-й позиции, для каждого из значений сдвига 2-й позиции – по 26 значений сдвига 3-й позиции и так далее до n-й позиции в блоке. Общее число ключей будет следующим.

$$\underbrace{26 \times 26 \times \cdots \times 26 \times 26}_{n \text{ множителей}} = 26^n$$

Для $n = 4$ получим следующее.

$$\underbrace{26 \times 26 \times 26 \times 26}_{4 \text{ множителя}} = 26^4$$

$$26^4 = 456\,976$$

При увеличении n количество ключей резко увеличивается. Так, для $n = 10$ оно превысит 140 трлн.

✤ Число ключей шифра перестановки

Приняв длину одного блока равной n буквам, получим следующее.

$$P_n = n \times (n-1) \times (n-2) \times \cdots \times 3 \times 2 \times 1 = n!$$

Для блока, состоящего из 4 букв ($n = 4$), общее число ключей Ek будет следующим:

$$4! = 4 \times 3 \times 2 \times 1 = 24.$$

При увеличении n число ключей будет возрастать, повышая тем самым стойкость шифра. Так, для $n = 26$ число ключей будет таким же, как для шифра одноалфавитной замены.