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


Полицейский участок № 78
в каком-то городе
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!

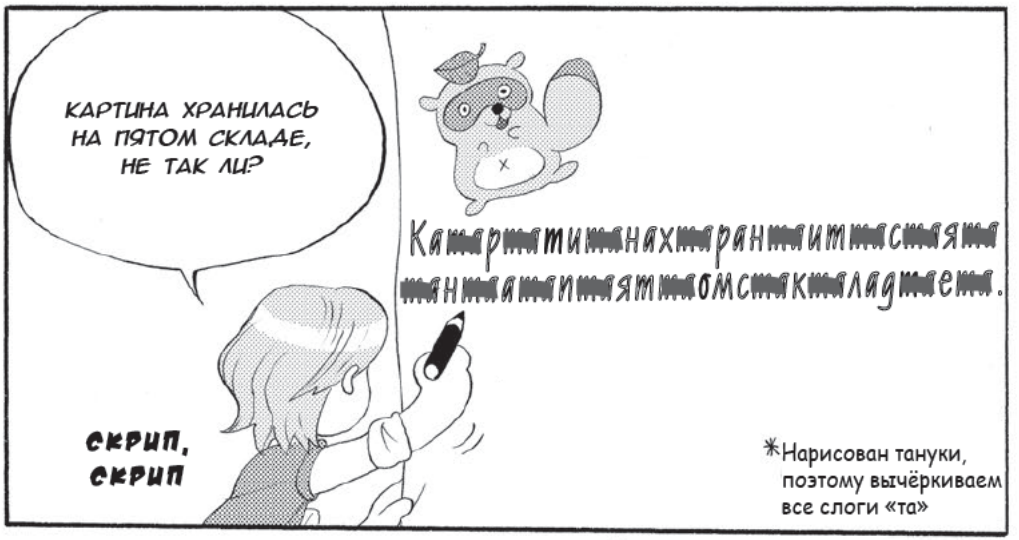

ДЛЯ ЭТОГО И ОБЫЧНЫХ СЧЁТОВ ДОСТАТОЧНО!
ГРР
ХВАТЬ
ТРР, ТРР
ТРР, ТРР
КЛАЦ
78-ОЙ УЧАСТОК, СЛУШАЮ ВАС.
ЧТО?! ПОХИТИЛИ?!
ПФУ!
ФИ!

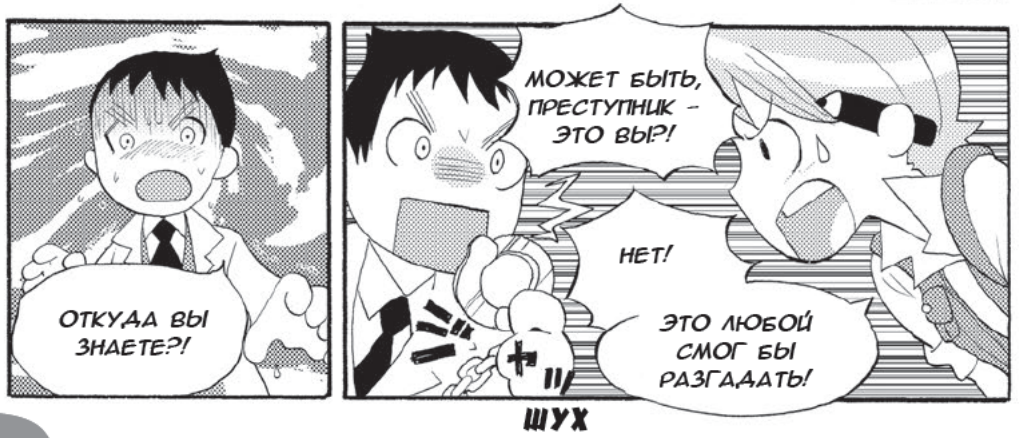

Музей исскуств «Мраморный»
ВИУ
ВИУ
ПРОВЕРЬТЕ ЗАПАДНОЕ КРЫЛО!
ПЕРЕКРОЙТЕ ВОН ТОТ ВЫХОД!
ВОСТОЧНОЕ КРЫЛО!
ОХ, ОХ...


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

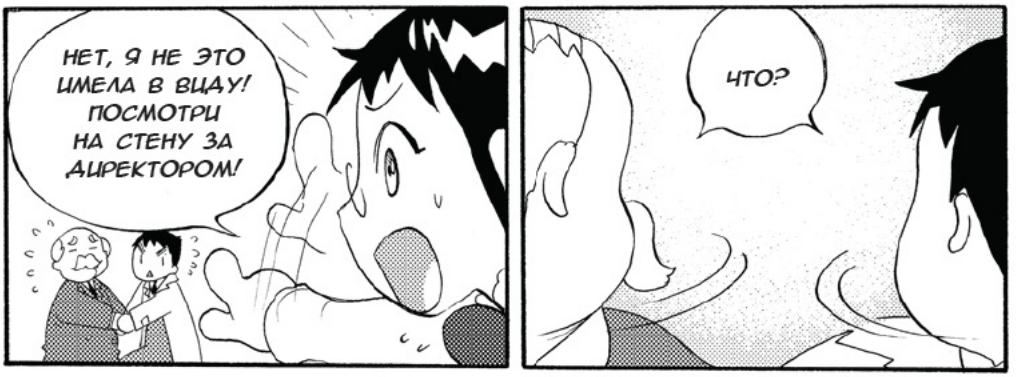
※ Изображена енотовидная собака тануки.

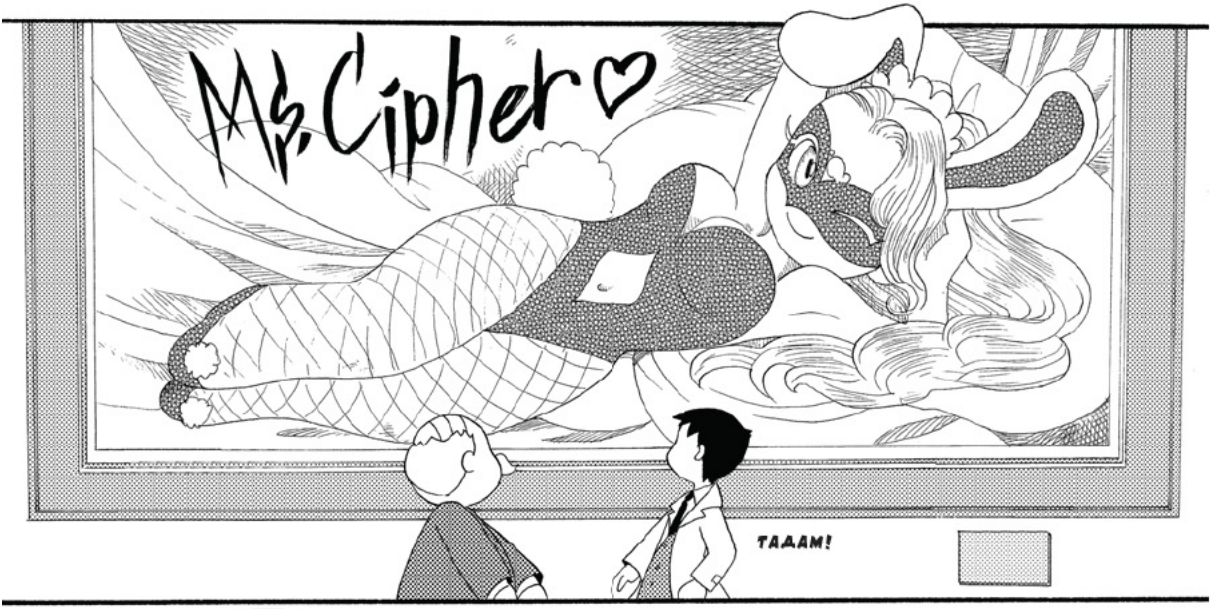

КАК?! ГАЗЕТЧИКИ УЖЕ ВСЁ ПРОНЮХАЛИ?
ЧТО БЫЛО НЕ ТАК С БЕЗОПАСНОСТЬЮ?!
ПАРОЛЬ И ШИФР НИКУДА НЕ ГОДЯТСЯ!
ЧТО?! ПОЧЕМУ?!

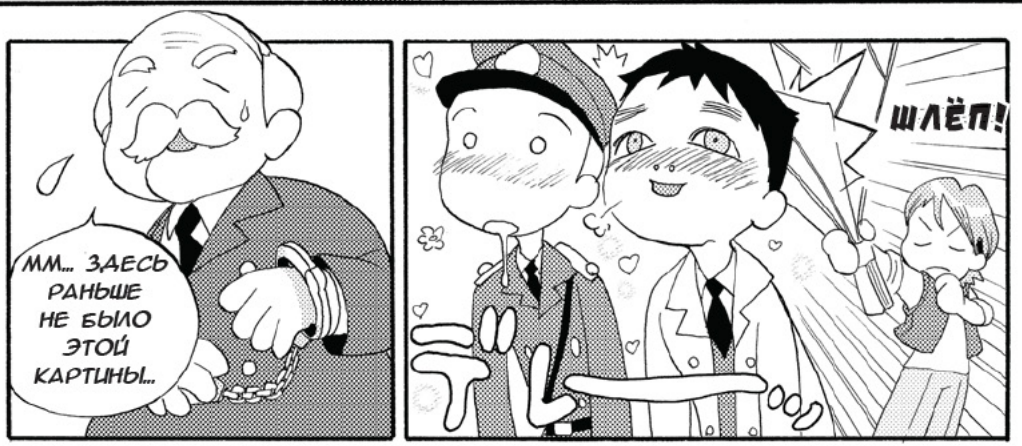

КАРТИНА ХРАНИЛАСЬ НА ПЯТОМ СКЛАДЕ, НЕ ТАК ЛИ?
Картина хранилась на пятом складе.
СКРИП, СКРИП
*Нарисован тануки, поэтому вычёркиваем все слоги «та»


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!

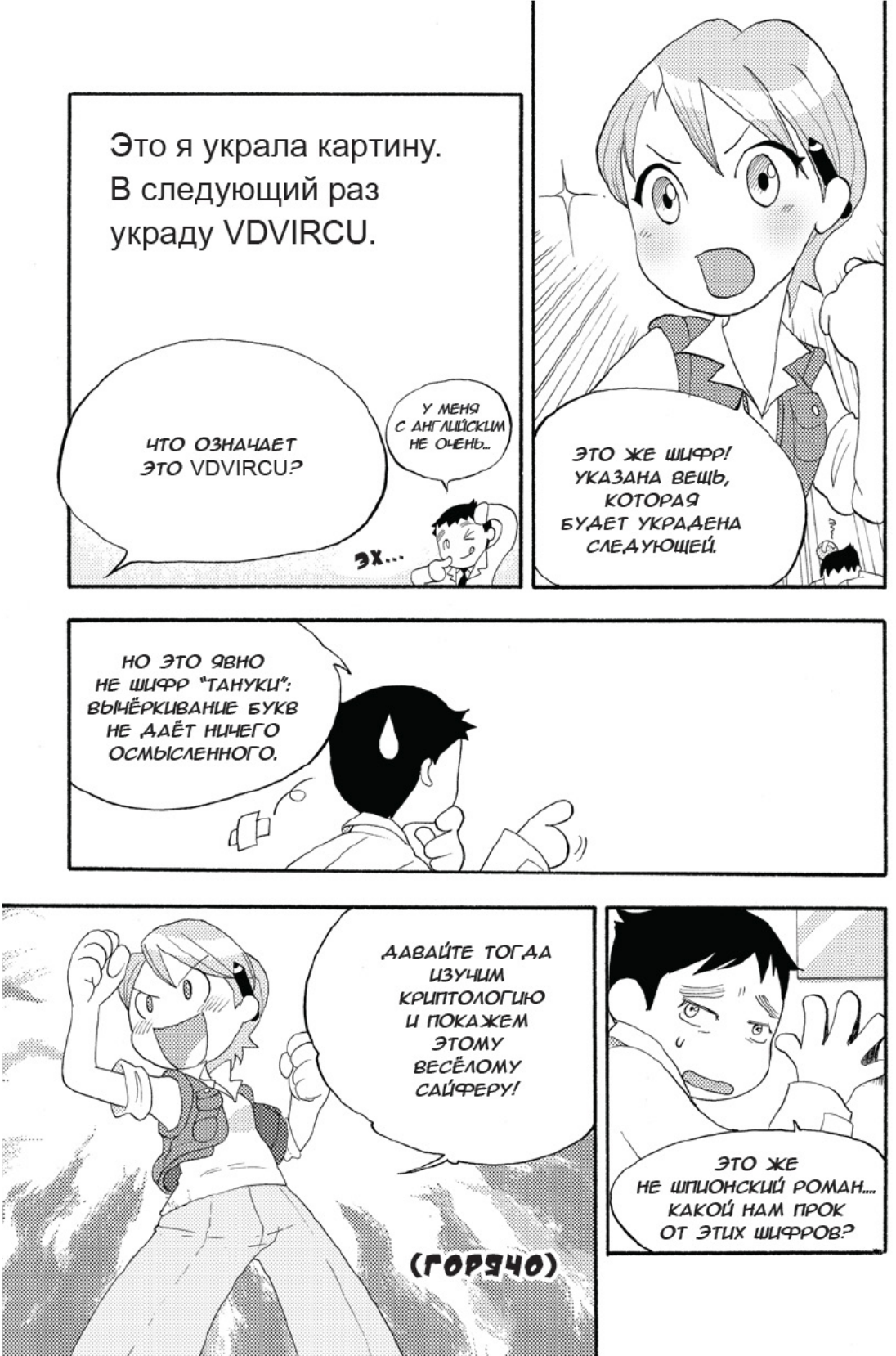

НЕТ, Я НЕ ЭТО ИМЕЛА В ВИДУ! ПОСМОТРИ НА СТЕНУ ЗА ДИРЕКТОРОМ!
ЧТО?


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.
ЭТО ЖЕ НЕ ШПИОНСКИЙ РОМАН... КАКОЙ НАМ ПРОК ОТ ЭТИХ ШИФРОВ?
ДАВАЙТЕ ТОГДА ИЗУЧИМ КРИПТОЛОГИЮ И ПОКАЖЕМ ЭТОМУ ВЕСЁЛОМУ САЙФЕРУ!
(ГОРЯЧО)

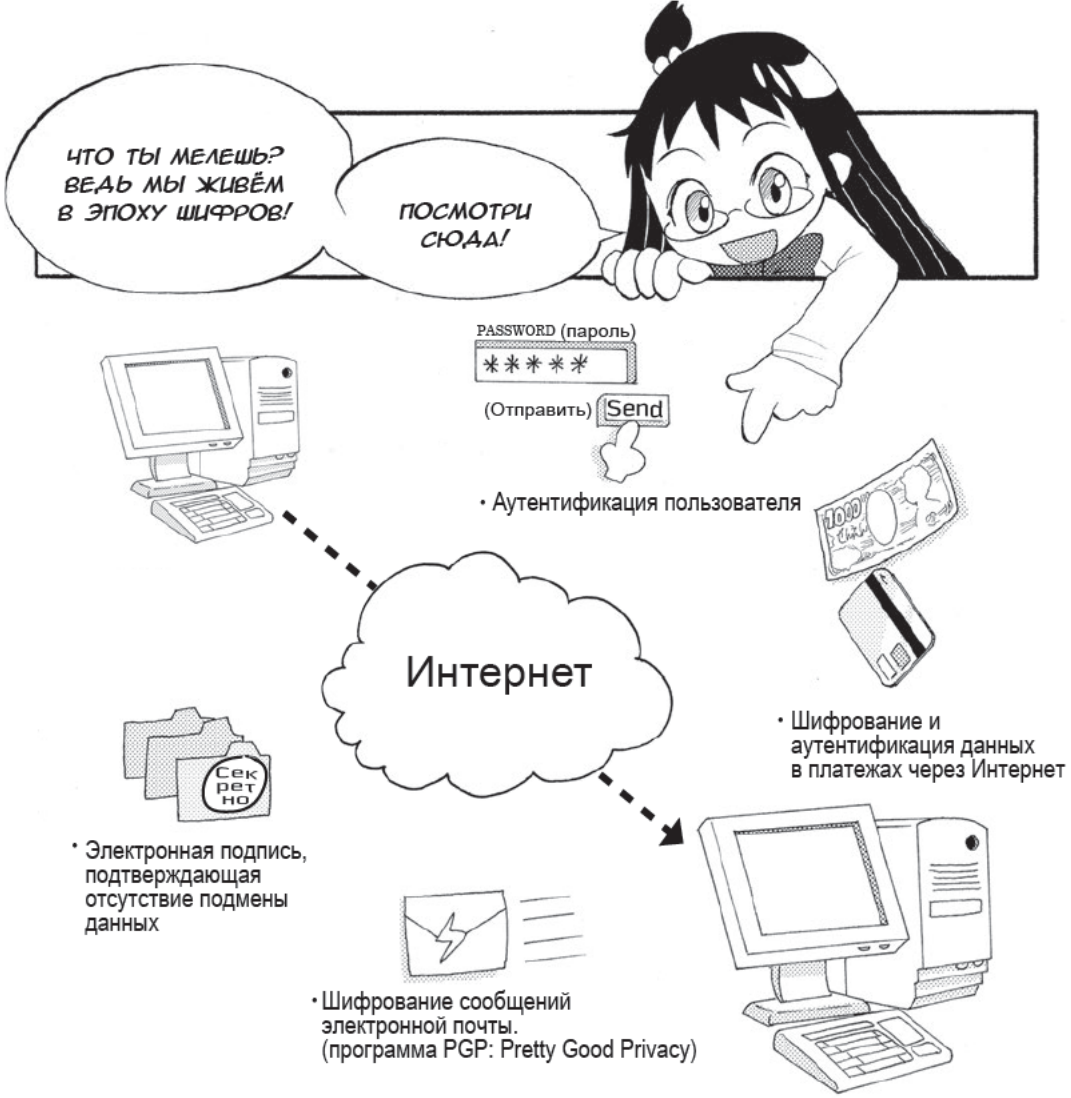


Рис. 0.1. Роль криптографии в современном обществе

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

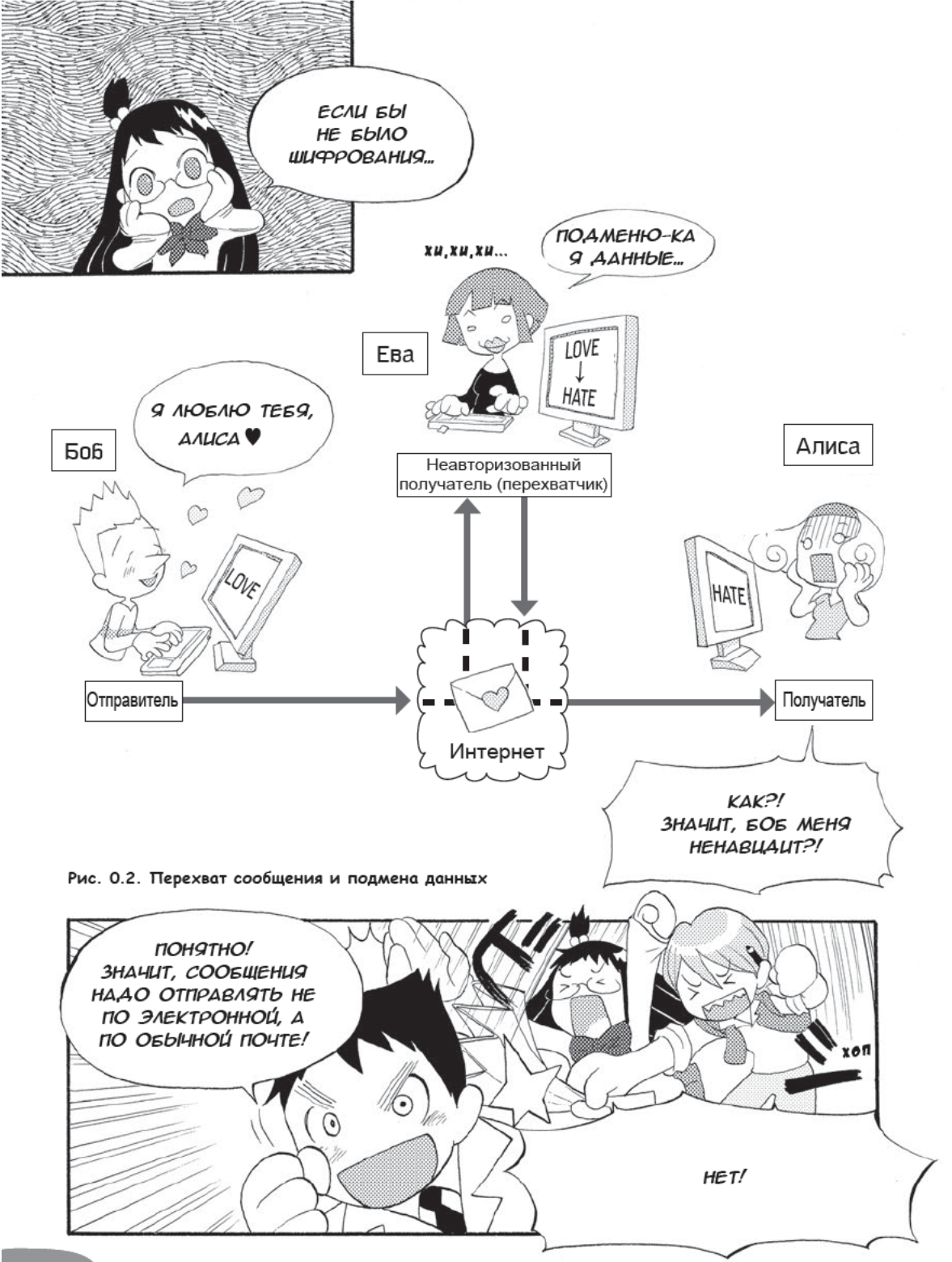


Рис. 0.2. Перехват сообщения и подмена данных

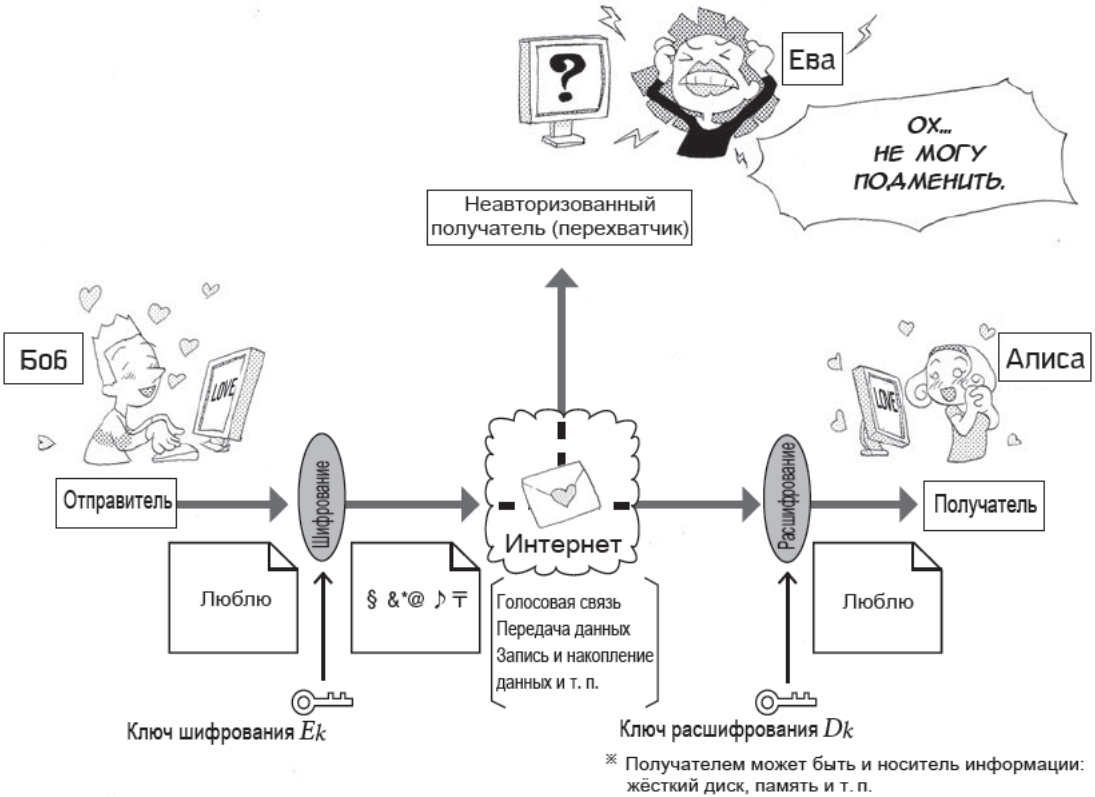
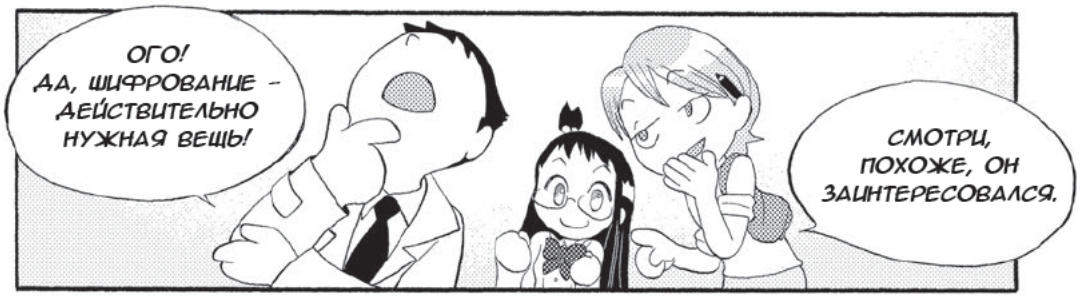


Рис. 0.3. Модель шифрования (криптосистема)




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