

# 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 делом 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
<b>Глава 1</b>	
<b>ОСНОВЫ КРИПТОГРАФИИ .....</b>	<b>15</b>
1-1 Основные понятия криптографии .....	16
• Термины криптографии .....	20
• Связь между ключами $E_k$ и $D_k$ .....	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
<b>Глава 2</b>	
<b>ОДНОКЛЮЧЕВОЙ ШИФР .....</b>	<b>45</b>
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
<b>2-6 Шифры 3-DES и AES .....</b>	<b>78</b>
• Общие сведения о шифре AES.....	83
<b>Пример использования упрощённого DES .....</b>	<b>87</b>
• 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 .....

#### **3-2 Простые числа и факторизация .....**

- Тест на простоту..... 131

#### **3-3 Модульная арифметика .....**

- Сложение по модулю и вычитание по модулю..... 139
- Умножение по модулю и деление по модулю .....

#### **3-4 Малая теорема Ферма и теорема Эйлера .....**

- 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 .....**

- Шифрование и расшифрование RSA .....
- Метод генерирования ключей RSA..... 167

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

## Глава 4

### **КАК ИСПОЛЬЗУЮТ ШИФР НА ПРАКТИКЕ?..... 187**

<b>4-1 Гибридные криптосистемы .....</b>	<b>188</b>
<b>4-2 Хеш-функция и код аутентификации сообщения ....</b>	<b>192</b>
• 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
<b>4-3 Цифровая подпись .....</b>	<b>202</b>
• Защита от отказа.....	202
• Устройство цифровой подписи .....	203
• Атака посредника.....	205
• Защита от атаки посредника .....	206
• Сертификат и удостоверяющий центр.....	206
<b>4-4 Инфраструктура открытых ключей (ИОК).....</b>	<b>208</b>
<b>Доказательство с нулевым разглашением .....</b>	<b>219</b>
<b>Разъяснение некоторых терминов .....</b>	<b>225</b>
<b>Список использованной литературы .....</b>	<b>227</b>
<b>Предметный указатель .....</b>	<b>228</b>

# ΠΡΟΛΟΓ





Полицейский участок № 78  
в каком-то городе

отдел



Мегуро Рика

БРАТЕЦ,  
НУ КУПИ!

Мегуро  
помощник инспектора

НЕТ!  
КОМПЬЮТЕР  
ДЛЯ ШКОЛЬНИ-  
ЦЫ - СЛИШКОМ  
БОЛЬШАЯ  
РОСКОШЬ!



ОН НУЖЕН  
МНЕ ДЛЯ ИЗУЧЕНИЯ  
МАТЕМАТИКИ!

$$ax + by = \gcd(a, b)$$

$$a^{p-1} \equiv 1 \pmod{p}$$

$$\varphi(p) = p - 1$$



ХОЧУ!











※ Изображена енотовидная собака тануки.

МЕСТО ХРАНЕНИЯ  
КАРТИНЫ БЫЛО  
НАДЕЖНО ЗАШИФРОВА-  
НО - ПОСТОРОННИЕ  
О НЁМ УЗНАТЬ НИКАК  
НЕ МОГЛИ!



Катартамитанахтарантаттастаята  
тантааятаияяттаомстакталадтааета.



ОТЛИЧНО!  
МОЛОДЦЫ!



КАКОЙ  
УЖАС...



ЩЁЛК

ЭТО НЕЛЬЗЯ  
ДАЖЕ НАЗВАТЬ  
БЕЗОПАСНОСТЬЮ!



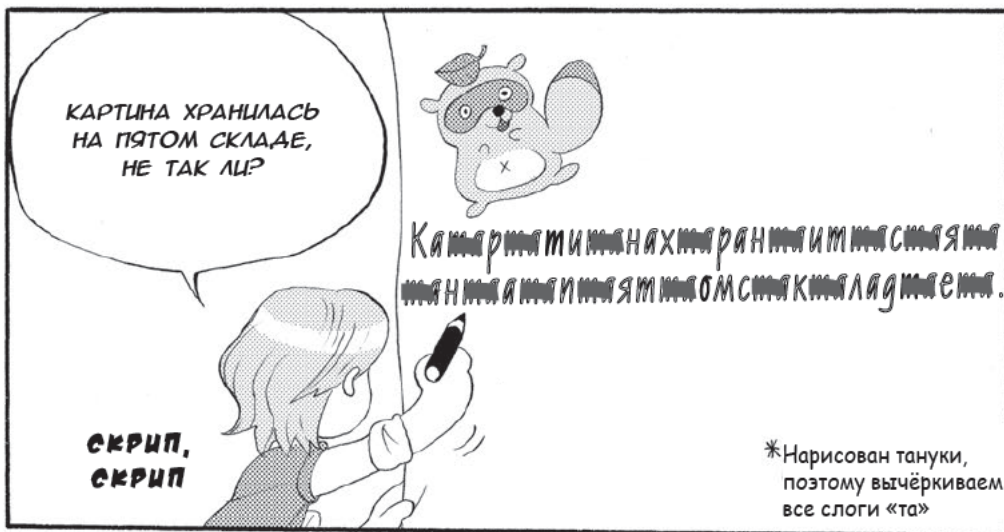
КТО?!

КТО ВЫ  
ТАКАЯ?!

ЩЁЛК

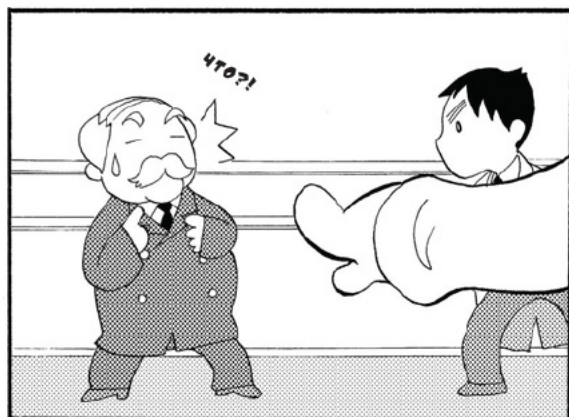
ЩЁЛК. ЩЁЛК

ЁМЗАА РЮ,  
КОРРЕСПОНДЕНТ  
"ВЕЧЕРНЕЙ ГАЗЕТЫ"!

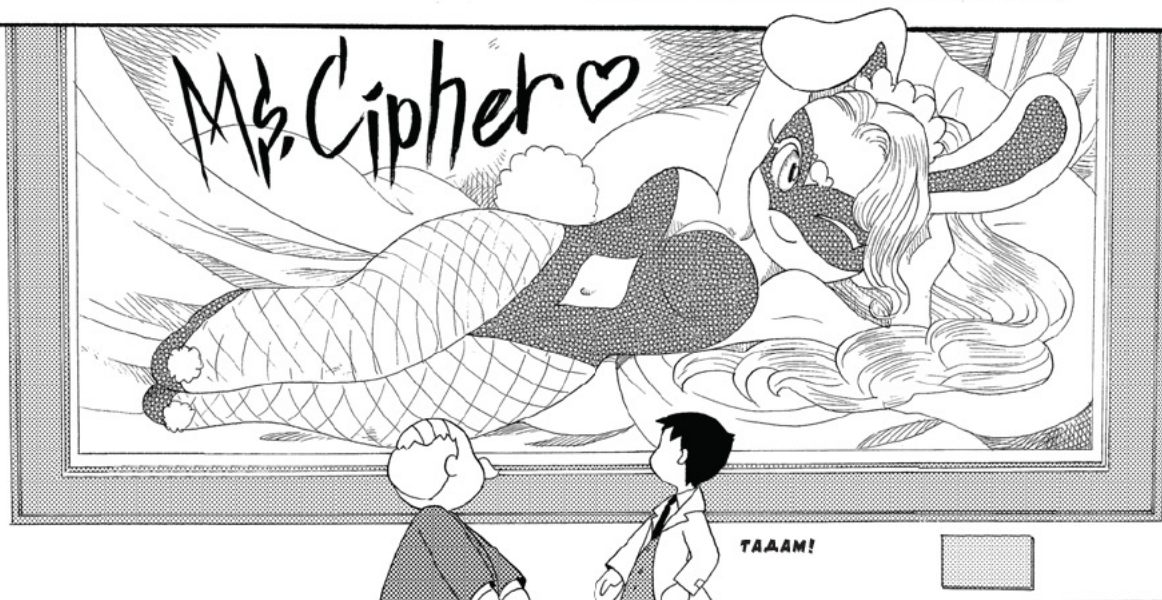


ШУХ










ГЛЫГ



НЕ НА КАРТИНУ  
НАДО СМОТРЕТЬ,  
А НА ЕЁ ТАБЛИЧКУ!

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

Спокойной ночи ♥



ВЕСЁЛЫЙ САЙФЕР?!




ХМ...

ЧТО БЫ  
ЭТО ЗНАЧИЛО?



УГУ!

Я ТОЖЕ  
СЕЙЧАС  
ОБ ЭТОМ  
ПОДУМАЛ.



СТРАННО КАК-ТО,  
"СПОКОЙНОЙ НОЧИ".  
СЕЙЧАС ВЕАЬ  
АЕНЬ.

ВАМ!

НЕТ, Я НЕ  
ОБ ЭТОМ!



Это я украла картину.  
В следующий раз  
украду VDVCURU.

ЧТО ОЗНАЧАЕТ  
ЭТО VDVCURU?

У МЕНЯ  
С АНГЛИЙСКИМ  
НЕ ОЧЕНЬ...

Эх...

ЭТО ЖЕ ШИФР!  
УКАЗАНА ВЕЩЬ,  
КОТОРАЯ  
БУДЕТ УКРАДЕНА  
СЛЕДУЮЩЕЙ.

НО ЭТО ЯВНО  
НЕ ШИФР "ТАНУКИ":  
ВЫЧЕРКИВАНИЕ БУКВ  
НЕ ДАЁТ НИЧЕГО  
ОСМЫСЛЕННОГО.

ДАВАЙТЕ ТОГДА  
ИЗУЧИМ  
КРИПТОЛОГИЮ  
И ПОКАЖЕМ  
ЭТОМУ  
ВЕСЁЛОМУ  
САЙФЕРУ!

(ОБРОД)

ЭТО ЖЕ  
НЕ ШПИОНСКИЙ РОМАН...  
КАКОЙ НАМ ПРОК  
ОТ ЭТИХ ШИФРОВ?



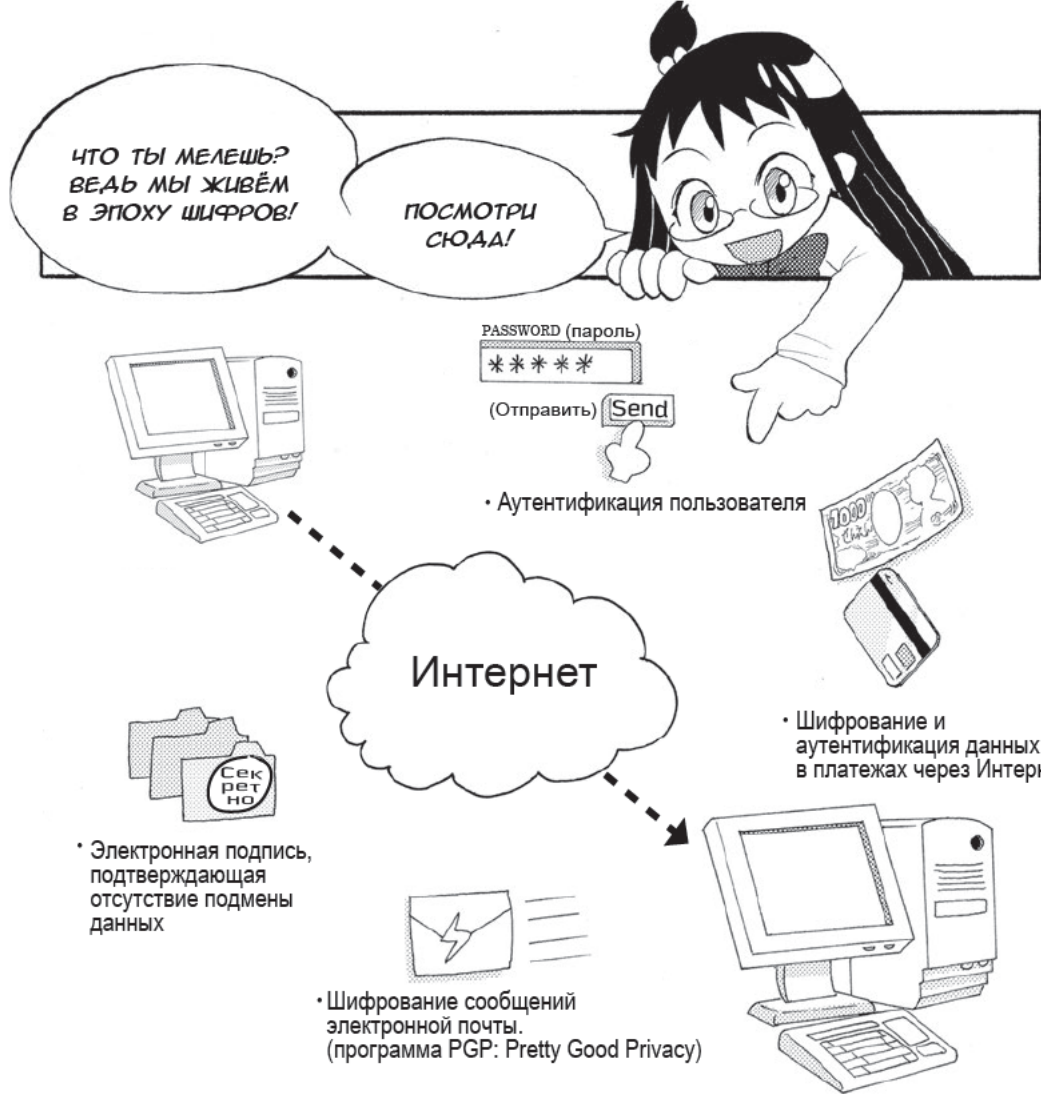


Рис. 0.1. Роль криптографии в современном обществе

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





хи, хи, хи... ПОАМЕНЮ-КА Я ДАННЫЕ...

Ева



Алиса



Неавторизованный получатель (перехватчик)

БОБ  
Я ЛЮБЛЮ ТЕБЯ, АЛИСА ♥



Отправитель



Получатель

КАК?!  
ЗНАЧИТ, БОБ МЕНЯ  
НЕНАВЦАИТ?!

Рис. 0.2. Перехват сообщения и подмена данных



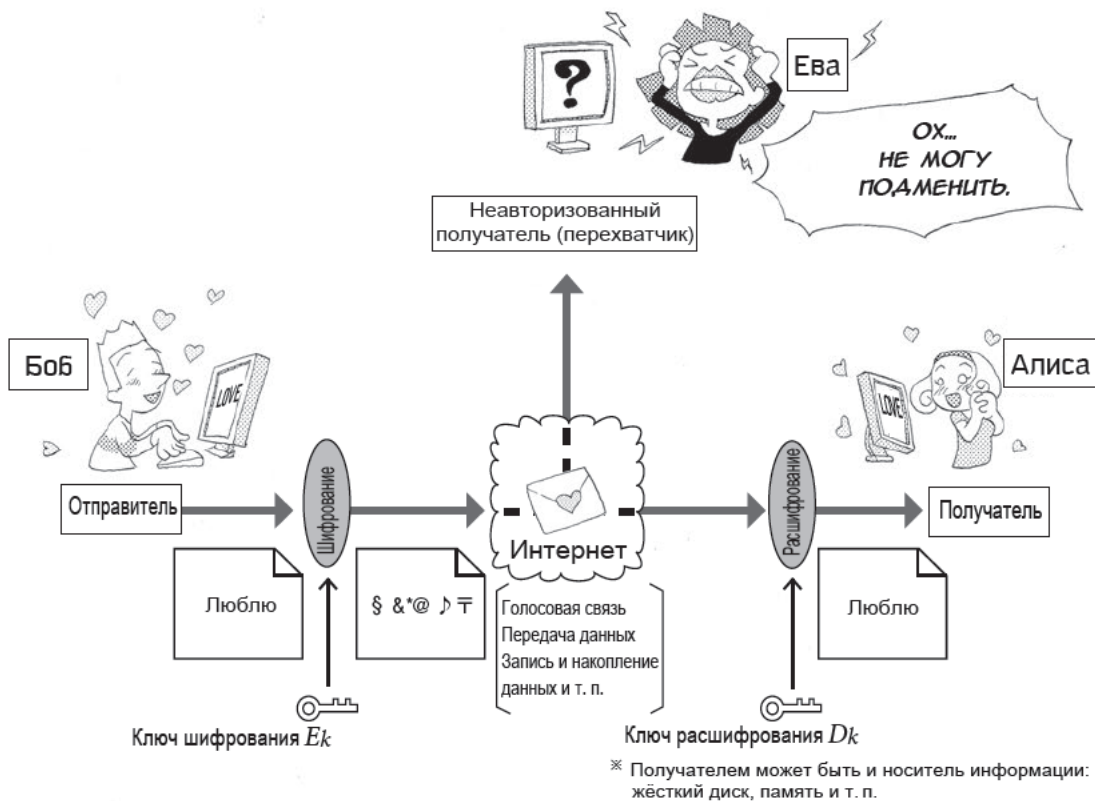
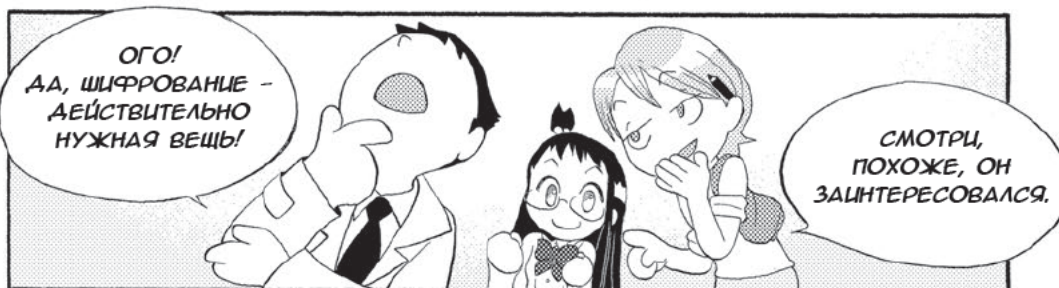
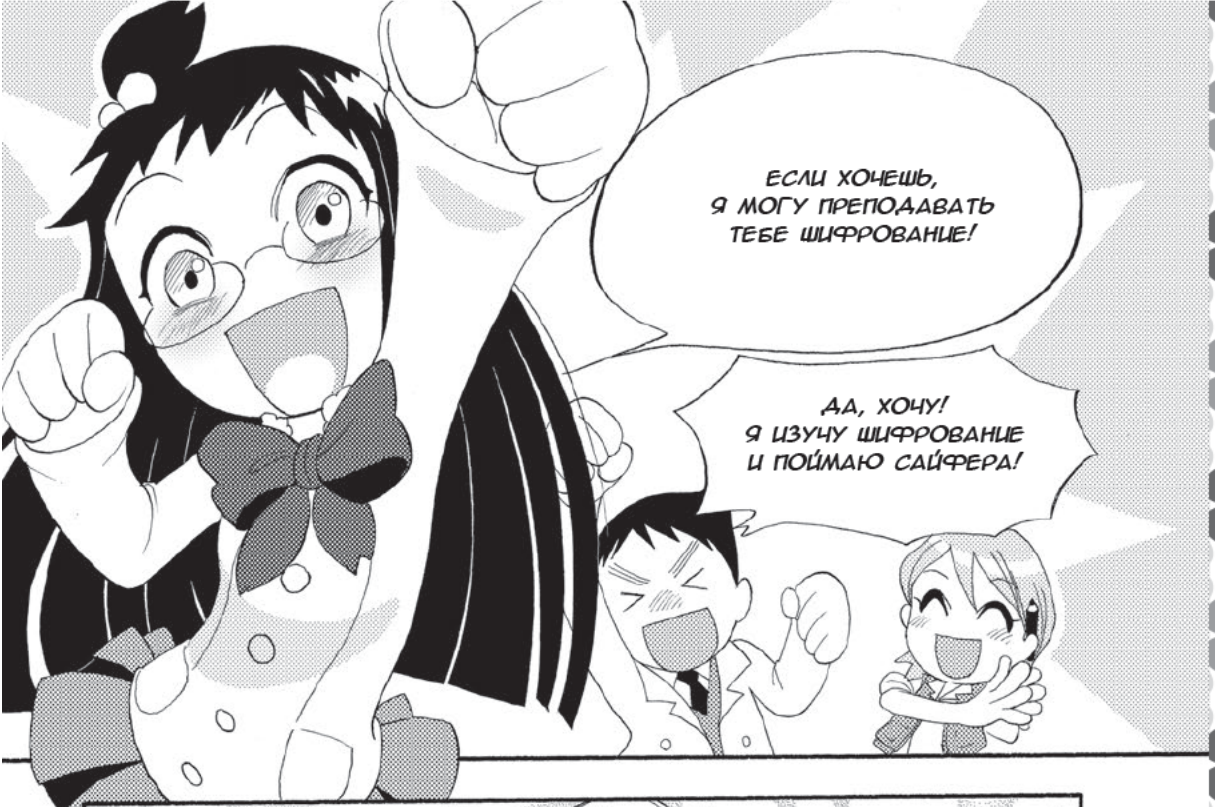


Рис. 0.3. Модель шифрования (криптосистема)







ГЛАВА 1

ОСНОВЫ  
КРИПТОГРАФИИ



1-1 Основные понятия криптографии



ИТАК,  
ПРИСТУПАЕМ  
К УЧЁБЕ!!



КСТАТИ!

YES!



...ЧТО ДЕЛАЕТ  
ГАЗЕТЧИК В СЛЕД-  
СТВЕННО-ОПЕРА-  
ТИВНОЙ  
ГРУППЕ?

Я БУДУ  
ОСВЕЩАТЬ ХОД  
РАССЛЕДОВАНИЯ!



Конец ознакомительного фрагмента.

Приобрести книгу можно

в интернет-магазине

«Электронный универс»

[e-Univers.ru](http://e-Univers.ru)