Введение

Проблема защиты информации путем ее преобразования, исключающего ее прочтение посторонним лицом волновала человеческий ум с давних времен. История криптографии - ровесница истории человеческого языка. Более того, первоначально письменность сама по себе была криптографической системой, так как в древних обществах ею владели только избранные. Священные книги Древнего Египта, Древней Индии тому примеры.

С широким распространением письменности криптография стала формироваться как самостоятельная наука. Первые криптосистемы встречаются уже в начале нашей эры. Так, Цезарь в своей переписке использовал уже более менее систематический шифр, получивший его имя.

Бурное развитие криптографические системы получили в годы первой и второй мировых войн. Начиная с послевоенного времени и по нынешний день появление вычислительных средств ускорило разработку и совершенствование криптографических методов.

Проблема использования криптографических методов в информационных системах (ИС) стала в настоящий момент особо актуальна.

С одной стороны, расширилось использование компьютерных сетей, в частности глобальной сети Интернет, по которым передаются большие объемы информации государственного, военного, коммерческого и частного характера, не допускающего возможность доступа к ней посторонних лиц.

С другой стороны, появление новых мощных компьютеров, технологий сетевых и нейронных вычислений сделало возможным дискредитацию криптографических систем еще недавно считавшихся практически не раскрываемыми.

Основываясь на этих заключениях, было принято решение проверить а как же в нашем современном обществе происходит кодирование информации, и как это кодирование используется человеком для получения знаний о потребляемых услугах и товарах.

Цель данной работы: установление подлинности школьных учебников, путем обработки их штрих-кода и его расшифровки.

Достижение этой цели будет реализовано через следующие задачи:

- анализ влияния кодирования на деятельность человека;
- исследование известных способов кодирования информации;
- анализ штрих-кодовой информации и ее значения в жизни человека;
- проверка подлинности учебников, через раскодировку их штрих-кода.

Методы решения основных задач: - анализ, - исследование, - синтез.

§1. История криптографии

Читая современные публикации, посвященные криптографии, может сложиться впечатление, что она зародилась вскоре после изобретения компьютера и долгое время использовалась лишь для военных нужд. Действительно, появление компьютеров очень преобразило криптографию, но считать XX век ее началом, безусловно, не стоит. Люди стремились максимально защитить свои секреты всегда, поэтому еще до нашей эры не только придумывались, но и довольно широко применялись разные алгоритмы шифрования.

По прошествии многих лет уже трудно достоверно определить дату зарождения шифрования. Вполне возможно, что она лишь немного "моложе" даты возникновения письменности.

Многие из древних рецептов, научных трактатов и религиозных текстов записывались не открытым текстом, а путем его преобразований по некоторым жестко фиксированным правилам. Чаще всего такие правила представляли собой то, что сегодня называют *шифрами замены.* Общий принцип для них сводится к тому, что все буквы исходного (открытого) текста при записи *заменяются другими буквами из того же алфавита.* Правила замены могут быть самими разными. В простейшем случае использовалось смещение на некоторое фиксированное количество символов вперед. Слово ZERO после шифрования будет представлено (в соответствии с тем же алгоритмом замены) последовательностью символов CHUS.

У такого алгоритма есть одно достоинство: он прост настолько, что для его реализации не требуется вообще никаких устройств. Процедуру шифрования можно проводить в уме, что называется, "на лету". Однако, с другой стороны, такая простота обусловливает целый ряд недостатков:

• Длина зашифрованного сообщения равна длине исходного текста.

• Ключом алгоритма является число N — величина сдвига на какое-то количество символов. Это число целое и не может быть больше A — 1, где A — общее количество букв в алфавите. Следовательно, возможных значений числа N достаточно мало. Например, для латинского алфавита максимальное N — 26 — 1 = 25. Даже без компьютера можно последовательно перепробовать все возможные значения N и найти нужное значение в течение получаса или быстрее — все зависит от сообщения, алфавита, вели чины N и темперамента подбирающего человека.

• Значение сдвига N — постоянно на протяжении все го послания. Учитывая, что начало или конец сообщения чаще всего стандартные ("Здравствуй!", "Привет!", "Пока!" и т.п.), а длина слов исходного текста равна длине слов зашифрованного текста, величина N легко вычисляется и без перебора — достаточно лишь установить соответствие любых двух слов из исходного и зашифрованного текста, как N будет известно.

• Любому символу исходного текста *строго соответствует один и тот же символ* зашифрованного текста на протяжении всего сообщения. Разные буквы встречаются в текстах с разной частотой, и для всех языков уже давно созданы статистические таблицы с указанием этих частот. Чем более длинный текст вы шифруете, тем больше частота встречаемости букв в нем соответствует эталонной, что также упрощает задачу поиска N. Такой способ атаки (попытки расшифровать текст) является классическим и называется *частотный анализ.*

Как можно видеть, древние варианты шифра замены интересны лишь с теоретической стороны: на них четко прослеживаются типичные недостатки элементарных схем шифрования и поясняются принципы простейших методов криптоанализа.

§2. Анализ известных шифров информации

Шифр Цезаря

Шифрование текста используется человечеством с того самого момента, как появилась первая секретная информация, т.е. такая, доступ к которой должен быть ограничен. Это было очень давно – так, один из самых первых известных методов шифрования носит имя римского императора Юлия Цезаря (I век до н.э.), который если и не сам изобрел его, то активно им пользовался.

Этот метод основан на замене каждой буквы шифруемого текста на другую путем смещения в алфавите от исходной буквы на фиксированное количество символов, причем алфавит читается по кругу. Регистр символов не учитывается. Так, например, слово *байт* при смещении на два символа вправо кодируется словом *гвлт*.

Используя метод Цезаря, закодируем название науки *криптографии* – будет считать, что каждая буква исходного текста заменяется третьей после нее буквой – шифр будет выглядеть следующим образом – *нултхсёугчлв*.

А теперь усложним задание, и зашифруем четверостишие Омара Хайяма, используя следующий ключ для шифровки: сдвигаемся на семь символов влево по алфавиту:

Чтоб мудро жизнь прожить, знать надобно немало,
Два важных принципа запомни для начала:
Ты лучше голодай, чем что попало есть,
И лучше будь один, чем вместе с кем попало.

Получим следующий текст:

Рлзь ёмейз авбжу ийзавлу, бжцлу жщэзьжз жюёщез,
Эыщ ыщажфо ийцывещ бцизёжв эеш жщрщещ:
Лф емрсю ъзезэщг, рюё рлз изищез юклу

В емрсю ьмэу зэвж, рюё ыёюклю к дюё изищез.

Квадрат Полибия

История свидетельствует, что в Древней Греции применялась система передачи секретных сообщений на основе так называемого *квадрата Полибия*. Для латинского алфавита он представлял собой квадрат из клеток 6*6, в котором первые вертикальная и горизонтальная строки были заполнены цифрами от 1 до 5, а оставшиеся 25 клеток — буквами:

				/J	

Согласно этой системе, каждая буква сообщения заменялась парой цифр. Букве А соответствовал код 1:1, а К — 2:5 и т.д.

Практически схема могла быть реализована, к примеру, так. На вышке стоят два дозорных — слева и справа. Им необходимо передать сообщение DIMICANDUM! *(оборона,* лат.), что означало приказ занять оборону. Дозорный слева (если смотреть на него спереди) поднимает один флаг (днем) или факел (ночью). Дозорный справа синхронно с ним поднимает 4 флага (факела). Так они передают код 1:4, соответствующий первой букве слова — О. Затем процедура повторяется для оставшихся букв.

Такой способ передачи данных был лучше системы условных сигналов в силу своей универсальности. С его помощью можно было передавать абсолютно любую информацию.

На первый взгляд шифр кажется очень нестойким, но для его реальной оценки надо учесть два фактора:

1) возможность заполнить квадрат Полибия буквами произвольно, а не только строго по алфавиту;

2) возможность периодически заменять квадраты. Тогда анализ предыдущих сообщений ничего не даст, так как к моменту раскрытия шифра он уже будет заменен.

Кроме того, следует учитывать также тактику боя в античные времена, когда основной упор делался на лобовую атаку, а не на дешифрование сообщений.

Скорость передачи сообщений была невелика, но ее можно было увеличить путем введения сокращений. Например, команда DIMICANDUM сокращалась до DIM, что ускоряло ее передачу более чем втрое.

Шифр Вижинера

Шифр Вижинера представляет собой шифр Цезаря с переменной величиной сдвига. Величина сдвига задается некоторым ключевым словом. Например, ключевое слово ВАЗА означает следующую последовательность сдвигов букв исходного текста:

3 1 9 1 3 1 9 1 и т.д.

Попробуем зашифровать таким образом слова АЛГОРИТМ, ПРАВИЛА, ИНФОРМАЦИЯ, используя ключевое слово ВАГОН.

Получим, что при ключевом слове ВАГОН последовательность сдвигов букв при шифровании следующая: 3 1 4 16 15 3 1 4 16 15 и т.д. Это означает, что слово АЛГОРИТМ шифруется как ГМЖЮЯЛУР, слово ПРАВИЛА – как ТСДСЧОБ, слово ИНФОРМАЦИЯ – как ЛОШЮЯПБЪШН.

«Тарабарская грамота»

В России для дипломатической переписки использовалась тайнопись, которая называлась «тарабарская грамота». Попробуем рассмотреть шифрование таким способом.

Возьмем некоторый текст:

Пайцике тсют т «камащамлтой чмароке» - кайпонили, нмирепяшвейля ш Моллии цся цинсоракигелтой неменилти.

Обратим при расшифровке внимание на слово МОЛЛИИ в шифрограмме. Оно очень похоже на слово РОССИИ. Предположим, что Ш МОЛЛИИ – это В РОССИИ. Тогда можно заметить, что все гласные остались без изменения, т.е. они не шифруются. Посмотрим на согласные. Мы уже выяснили, что в шифрограмме М это Р, Ш – В, а Л – С. Выпишем все согласные буквы:

Примечание: в верхней строке записаны буквы в шифрограмме, в нижней – зашифрованные буквы.

Проанализировав табличку, можно увидеть «симметрию» (предпоследняя буква Ш означает вторую согласную букву В). Исследовав эту закономерность, можно установить следующее правило шифрования согласных букв: каждая согласная буква заменяется на «симметричную» ей букву в перечне всех согласных букв.

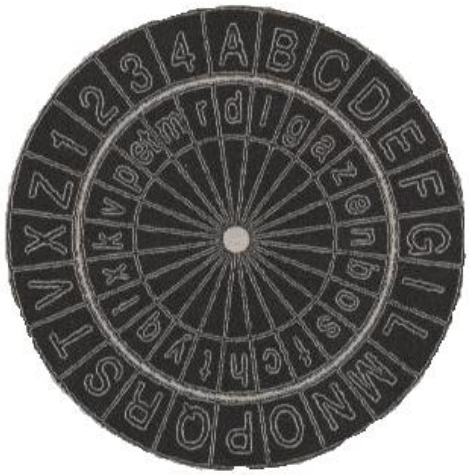
Эта табличка – ключ шифра – может быть оформлен короче:

В этом шифре каждая согласная меняется на букву, расположенную непосредственно над ней или под ней в таблице.

Диск Леона Альберти

Одним из наиболее уникальных приборов для шифрования текста был диск итальянского архитектора и философа Леона Альберти, созданный во второй половине XV века (см. рисунок).

Можно видеть, что диск состоит из двух частей: внутренней (подвижной) и внешней (неподвижной). Обе части делят на 24 сектора радиальные лучи.



Секторы внешней части диска заполняются по порядку двадцатью буквами латинского алфавита (за исключением шести из них: H, J, K, U, W, Y) и четырьмя арабскими цифрами (1-4). В секторы внутренней части тоже вписаны буквы латинского алфавита, но уже не в классическом порядке следования. При этом из них исключили три буквы: J, U, W — и добавили слог ET, который записали в одном секторе.

Обозначим алфавиты внешней и внутренней части диска как A_1 и A_2 соответственно и приступим к рассмотрению процедуры шифрования на конкретном примере.

Итак, XV век...Людовик хочет написать любовное послание Анжелике, однако его ревнивая жена по имени Мегера тоже умеет читать и щедро платит слугам за то, чтобы они давали ей ознакомиться с корреспонденцией мужа до отправки. Чтобы решить эту проблему, Людовик просит мастера изготовить... нет, не арбалет, а два одинаковых диска Альберти. Далее он передает один из них Анжелике и объясняет правила пользования.

На подвижном диске выбирается (и запоминается обоими участниками переписки) некоторая буква (так называемая "маркерная буква").

Для зашифрованного текста Людовик выбирает на внешнем диске любой сектор (букву) и поворачивает его так, чтобы этот сектор оказался напротив маркерной буквы. Он сообщает о своем выборе Анжелике, *записывая букву выбранного сектора первым, симво-*

лом сообщения. Диск фиксируется в таком положении. Для составления зашифрованного текста буквы, составляющие исходный (открытый) текст, берутся из внешнего диска и заменяются соответствующими им (противоположными) буквами внутреннего.

Ключом такого шифра (т.е. совокупностью всего того, что нужно знать, чтобы прочитать зашифрованный текст) является:

1) информация об алфавитах A_1 и A_2 (как правило, они не менялись);

2) маркерная буква;

3) соответствующая маркерной букве *в данном сообщении* буква внутреннего диска (S_1).

Описанная шифрсистема для того времени была очень надежной. Главным образом это обуславливали ее следующие свойства:

• Использовалась замена в пределах не одного, а двух алфавитов. Спустя годы подобные шифры получат название *многоалфавитных.*

• 4 цифры на диске вместо букв легли в основу гениальной идеи: они образовывали так называемые кодовые группы (Альберти использовал 336 групп, обозначаемых последовательностью цифр от 11 до 4444), с каждой из которых связывалось целое предложение. Например, "Дорогая Анжелика, Мегера уезжает завтра утром" соответствовало коду 13. Когда в открытом тексте встречалось такое предложение, оно целиком заменялось цифрами 13, которые далее шифровались буквами по внутреннему диску по общему правилу. Такой принцип получил название *перешифрование*..

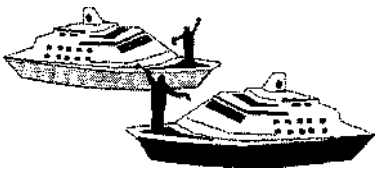
• Длина зашифрованного текста обычно меньше длины исходного, что затрудняет нахождения ключа методом частотного анализа.

К недостаткам можно отнести то, что две из трех составляющих ключа обычно были известны. Отсутствующие в алфавитах A_1 и A_2 буквы добавляли надежности, но создавали неудобства при работе. Хотя Альберти намеренно выбрал наименее значимые символы, порой результат дешифрования был неоднозначным, и его можно было трактовать только исходя из контекста.

§3. Кодирование информации в компьютерных технологиях

Для общения друг с другом мы используем код — русский язык. При разговоре этот код передается звуками, при письме — буквами. Водитель передает сигнал с помощью гудка или миганием фар. Вы встречаетесь с кодированием информации при переходе дороги в виде сигналов светофора. Таким образом, кодирование сводится к использованию совокупности символов по строго определенным правилам.

Кодировать информацию можно различными способами: устно; письменно; жестами или сигналами любой другой природы. Когда создается информационная модель объекта или явления, то их свойства, параметры, состояния, среда, действия могут отображаться также с помощью различных способов кодирования.



Люди всегда искали способы быстрого обмена сообщениями. Для этого посылали гонцов, использовали почтовых голубей. В древности, а у некоторых народов и сейчас, существовали различные способы оповещения о надвигающейся опасности: барабанным боем, дымом костров, флагами и т. д. Однако использование такого способа представления информации требует предварительной договоренности о понимании принимаемого сообщения. Например, что означает поднятая вверх правая рука регулировщика движения?

По мере развития техники появлялись разные способы кодирования информации. Во второй половине XIX века американский изобретатель Сэмюэль Морзе изобрел удивительный код, который служит человечеству до сих пор. Информация кодируется тремя символами: длинный сигнал (тире), короткий сигнал (точка), нет сигнала (пауза) — для разделения букв.

В качестве источников информации может выступать человек, техническое устройство, предметы, объекты неживой и живой природы. Получателей сообщений может быть несколько или один.

В процессе обмена информацией мы совершаем две операции: *кодирование и декодирование*. Первая связана с переходом от исходной формы представления информации в форму, удобную для хранения, передачи или обработки. А вторая — с обратным переходом к исходному представлению информации.

В настоящее время существуют разные способы кодирования и декодирования информации в компьютере. Выбор способа зависит от вида информации, которую необходимо кодировать: текст, число, графическое изображение или звук. Для чисел, кроме того, важную роль играет то, как будет использоваться число: в тексте, или в вычислениях, или в процессе ввода-вывода. Накладываются также особенности технической реализации.

Несмотря на особенности каждого вида информации, общим для них является использование при кодировании двоичной системы счисления, основанной на двух цифрах — 0 и 1. Эти два символа принято называть двоичными цифрами или битами. С помощью двух цифр 0 и 1 можно закодировать любое сообщение.

Инженеров такой способ кодирования привлек простотой технической реализации — есть сигнал или нет сигнала. Эти состояния легко различать. Недостаток двоичного кодирования

— длинные коды. Но в технике легче иметь дело с большим числом простых однотипных элементов, чем с небольшим числом сложных.

Рассмотрим основные способы кодирования информации в компьютере.

Кодирование текстовой информации

Нажатие клавиши на клавиатуре приводит к тому, что сигнал посылается в компьютер в виде двоичного числа, которое хранится в кодовой таблице. Кодовая таблица — это внутреннее представление символов в компьютере. Во всем мире в качестве стандарта принята таблица ASCII (American Standard Code for Information Interchange — Американский стандартный код для обмена информацией). Для хранения двоичного кода одного символа выделен 1 байт = 8 бит. Учитывая, что каждый бит принимает значение 0 или 1, количество их возможных сочетаний в байте равно 2^8=256. Значит, с помощью 1 байта можно получить 256 разных двоичных кодовых комбинаций и отобразить с их помощью 256 различных символов. Эти комбинации и составляют таблицу ASCII.

Например, вы нажимаете на клавиатуре латинскую букву 8. В этом случае в память компьютера записывается код 01010011. Для вывода буквы 8 на экран в компьютере происходит декодирование — по этому двоичному коду строится его изображение.

Цифры кодируются по этому стандарту при вводе-выводе и если они встречаются в тексте. Если они участвуют в вычислениях, то осуществляется их преобразование в другой двоичный код.

Кодирование чисел

Двоичная система счисления обладает такими же свойствами, что и десятичная, только для представления чисел используется не 10 цифр, а всего две. Соответственно и разряд числа называют не десятичным, а двоичным. Все же основные законы выполнения арифметических действий соблюдаются точно так же неукоснительно.

Для сравнения рассмотрим представление чисел в разных системах счисления как сумму слагаемых, в которых учтен вес каждого разряда.

В десятичной системе счисления

$435{,}67 = 4*10^2 + 3 * 10^1 + 5*10^0 + 6*10^{-1} + 7*10^{-2}$

В двоичной системе счисления

$$10110{,}101 = 1*2^4 + 0*2^3 + 1*2^2 + 1*2^1 + 0*2^0 + 1*2^{-1} + 0*2^{-2} + 1*2^{-3}$$

Для кодирования числа, участвующего в вычислениях, используется специальная система правил перевода из десятичной системы счисления в двоичную. В результате число будет записано двоичным кодом, т. е. представлено различным сочетанием всего двух цифр — 0 и 1.

Кодирование графической информации

Создавать и хранить графические объекты в компьютере можно двумя способами — как растровое изображение или как векторное изображение. Для каждого типа изображения используется свой способ кодирования.

Растровое изображение представляет собой совокупность точек, используемых для его отображения на экране монитора. Объем растрового изображения определяется умножением количества точек на информационный объем одной точки, который зависит от количества возможных цветов. Для черно-белого изображения информационный объем одной точки равен 1 биту, т.к. она может быть либо черной, либо белой, что можно закодировать двумя цифрами — 0 или 1.

Рассмотрим, сколько потребуется бит для отображения цветной точки: для 8 цветов — 3 бита; для 16 цветов — 4 бита; для 256 цветов — 8 битов (1 байт). В таблице показано кодирование цветовой палитры из 16 цветов. Разные цвета и их оттенки получаются за счет наличия или отсутствия трех основных цветов (красного, синего, зеленого) и их яркости. Каждая точка на экране кодируется с помощью 4 битов.

Цвет	Яр-	Крас-	Зеле-	Синий
Черный	0	0	0	0
Синий	0	0	0	1
Зеленый	0	0	1	0
Голубой	0	0	1	1
Красный	0	1	0	0
Фиолетовый	0	1	0	1
Коричневый	0	1	1	0
Белый	0	1	1	1
Серый	1	0	0	0
Светло-синий	1	0	0	1
Светло-зеленый	1	0	1	0
Светло-голубой	1	0	1	1
Светло-красный	1	1	0	0
Светло-фиолетовый	1	1	0	1
Желтый	1	1	1	0
Ярко-белый	1	1	1	1

Векторное изображение представляет собой графический объект, состоящий из элементарных отрезков и дуг. Положение этих элементарных объектов определяется координатами точек и длиной радиуса. Для каждой линии указывается ее тип (сплошная, пунктирная, штрих-пунктирная), толщина и цвет. Информация о векторном изображении кодируется как обычная буквенно-цифровая и обрабатывается специальными программами.

Кодирование звуковой информации

Звуковая информация может быть представлена последовательностью элементарных звуков (фонем) и пауз между ними. Каждый звук кодируется и хранится в памяти. Вывод звуков из компьютера осуществляется синтезатором речи, который считывает из памяти хранящийся код звука. Гораздо сложнее преобразовать речь человека в код, т. к. живая речь имеет

большое разнообразие оттенков. Каждое произнесенное слово должно сравниваться с предварительно занесенным в память компьютера эталоном, и при их совпадении происходит его распознавание и запись.

§4. Штрих-кодовое кодирование информации

Все видели на упаковке многих товаров ряд вертикальных полосок различной толщины, разделенных пустыми интервалами, под которыми написано число:

Такое изображение называется штриховым кодом, или штрих-кодом. Что же это такое и зачем это нужно? Начнем с числа.

В свое время производители товаров и торговые фирмы столкнулись с серьезной проблемой: товаров много (например, средний универмаг оперирует с десятью тысячами наименований), и к каждому - длинный сертификат - документ, в котором расписано, где сделан товар, на какой фирме, сколько весит, какие габариты и т.д. Поэтому придумали систему кодирования этой информации в виде последовательности цифр (и штрихового кода). Более 20 лет назад была создана глобальная международная организация - система товарных номеров EAN/UCC, образованная на основе Европейской (European Article Numbering Association – EAN International) и Северо-Американской (Uniform Code Council - UCC) ассоциаций товарной нумерации. В настоящее время система EAN/UCC объединяет национальные организации в 94 странах мира. Каждая страна имеет свой номер. Чаще всего коды стран - двузначные, но могут быть и трехзначными (например, страны СНГ имеют номера с 460-ю по 469-й, в т.ч. Россия - 460). Внутри каждой страны проводится нумерация предприятий - изготовителей товаров. В Российской Федерации национальной организацией товарной нумерации - членом EAN International является Ассоциация автоматической идентификации ЮНИСКАН/EAN РОССИЯ, которая насчитывает около 5000 предприятий-членов. Всем им присвоены уникальные идентификационные номера, которые начинаются с цифр 460 (EAN РОССИЯ). Регистрационный номер предприятия отображается на упаковке продукции в виде первых цифр кода EAN (например, 4600952). Следующие 5 цифр - это закодированная информация о товаре (имя товара, масса, состав, цвет и т.п.). Итак, всего всю необходимую информацию отражают 12 цифр. Но внимательный читатель, конечно, обнаружит, что на приведенном выше рисунке в числе не 12, а 13 цифр. Дело в том, что последняя, тринадцатая, цифра - контрольная.

При наличии на упаковке товаров закодированной информации о них можно автоматизировать процесс распознавания этой информации, если считывать ее специальным

устройством - сканером. Причем можно, конечно, использовать для распознавания информации о товаре указываемые на упаковке цифры. Но это потребовало бы применения сложной компьютерной технологии распознавания символов. Проще и надежнее это делать с использованием двоичного кодирования этой информации. Нет, речь не идет о том, чтобы представлять число-код в виде цифр двоичной системы счисления. Просто десятичный номер товара изображается на упаковке в виде тех самых вертикальных полосок различной толщины и интервалов между ними, а эта информация является двоичной, хотя на первый взгляд этого и не скажешь.

Если сделать тонкий срез этих полосок, то можно увидеть следующее (в увеличенном масштабе):

Эти полоски и пробелы графического изображения штрихового кода очень хорошо понятны специальным приборам - сканерам. Считывая эту информацию слева направо, сканер присваивает 1 первой встреченной черной полоске и 0 - первому промежутку. Следующие промежутки и штрихи считываются как последовательности одного, двух, трех или четырех нулей или единиц, в зависимости от ширины штриха иди промежутка. Следовательно, все изображение может быть представлено как последовательность битов:

10100001100101100001001100 1...

Эти биты и есть двоичное представление десятичного числа - кода товара. При считывании штрихового кода сканер из комбинации штрихов восстанавливает закодированный номер. Те, кто бывали в крупных магазинах, видели, как кассир, делая расчет, просто проносит товар, повернув его штрих-кодом вниз, над кассовым аппаратом, и на экране аппарата мгновенно выскакивает цена. Это происходит потому, что кассы со считывателями штрихового кода подключены к компьютеру, который обрабатывает считанную информацию. Кроме удобства работы кассира и "быстроты" обслуживания покупателя, такая автоматизированная система может обеспечить и учет объема продаж того или иного товара, уровень спроса на те или иные изделия, заблаговременно сделать заказ на склад для восполнения запасов товаров на полках торгового зала и т.п.

Некоторых покупателей смущает, если на штрих-коде - только собственно штрихи, а цифр нет. Это - не признак подделки. Для кассового аппарата цифры вообще не имеют значения, и, если места на товаре мало, их не ставят.

Не нужно пытать продавца и в том случае, если штрих-код узкий или короткий, или вообще "какой-то не такой". Обычно так бывает на мелких по размеру товарах. ЮНИСКАН разрешает производителям таковых использовать сокращенные варианты кодировки.

Есть способ, хотя и несколько трудоемкий, узнать по штрих-коду, поддельный ли то-

вар. Используя последнюю контрольную цифру можно проверить правильность кода товара. Итак, если вам крайне важно узнать, с чем вы имеете дело, нужно произвести следующие арифметические действия:

1. Сложить цифры, стоящие на четных позициях; для штрих-кода, изображенного на рисунке в начале статьи: 6+0+5+0+0+1 = 12.
2. Сумму умножить на 3: 12 * 3= 36.
3. Сложить цифры, стоящие на нечетных позициях (не учитывая контрольную цифру): 4+0+9+2++ 0+ 0= 15.
4. Сложить то, что получилось в результате второго и третьего действий: 36 + 15 = 51.
5. От результата отбросить первую цифру. Получится 1.
6. И отнять от 10 то, что получилось в пятом пункте: 10,- 1 = 9.

Этот результат должен совпадать с контрольной цифрой. Если нет - товар поддельный.

Метод, конечно, сложный. Однако, если вы покупаете дорогую вещь или есть сомнения, доброкачественный ли продукт питания перед вами, имеет смысл произвести эти в общем-то элементарные процедуры.

§5. Практическая часть

На основании всего выше изложенного и учитывая цель своей работы я могу теперь определить являются ли школьные учебники, по которым я обучаюсь лицензированными или контрафактными. Для этого я взяла:

1) Учебник по английскому языку «English Student’s Book» авторы О. В. Афанасьева, И. В. Михеева, издательство «Просвещение» , 2001:

- складываем цифры, стоящие на четных позициях для штрих-кода

7+5+9+1+2+5=29

- сумму умножаем на 3 – 29*3=87

- складываем цифры, стоящие на нечетных позициях (не учитывая последнюю цифру)

9+8+0+0+5+7=29

- складываем то, что получилось в результате сложений цифр

87+29=116

- от результата оставляем только последнюю цифру, получится 6

- от 10 отнимаем то, что получилось в пятом действии

10-6=4.

Этот результат совпал с контрольной цифрой. Значит, делаем вывод, что данный учебник лицензированный.

2) Учебник по литературе, автор Т. Ф. Курдюмова, издательство «Дрофа» ,2002

- складываем цифры, стоящие на четных позициях для штрих-кода 7+5+1+7+8+0=28
- сумму умножаем на 3 – 28*3=84
- складываем цифры, стоящие на нечетных позициях (не учитывая последнюю цифру) 9+8+7+0+5+5=34
- складываем то, что получилось в результате двух последних действий с цифрами 84+34=118
- от результата оставляем только последнюю цифру, получится 8
- от 10 отнимаем то, что получилось в пятом действии 10-8=2

Этот результат совпал с контрольной цифрой. Значит, делаем вывод, что данный учебник лицензированный.

3) Учебник по информатике автор Н. В. Макарова, издательство «Питер» , 2001

- складываем цифры, стоящие на четных позициях для штрих-кода 7+5+1+0+1+0=14
- сумму умножаем на 3 – 14*3=42
- складываем цифры, стоящие на нечетных позициях (не учитывая последнюю цифру) 9+8+3+4+0+5=29
- складываем то, что получилось в результате двух последних действий с цифрами 42+29=71
- от результата оставляем только последнюю цифру, получится 1
- от 10 отнимаем то, что получилось в пятом действии 10-1=9

Этот результат совпал с контрольной цифрой. Значит, делаем вывод, что данный учебник лицензированный.

4) Учебник по истории «История России» авторы А. А. Данилов, Л. Г. Косулина, издательство «Просвещение» , 2002

- складываем цифры, стоящие на четных позициях для штрих-кода 7+5+9+1+0+2=24
- сумму умножаем на 3 – 24*3=72
- складываем цифры, стоящие на нечетных позициях (не учитывая последнюю цифру) 9+8+0+0+4+1=22
- складываем то, что получилось в результате двух последних действий с цифрами 72+22=94
- от результата оставляем только последнюю цифру, получится 4
- от 10 отнимаем то, что получилось в пятом действии 10-4=6

Этот результат совпал с контрольной цифрой. Значит, делаем вывод, что данный учебник лицензированный.

5) Учебник по химии, авторы И. И. Новошинский, Н. С. Новошинская, издательство «ОНИКС» , 2006

- складываем цифры, стоящие на четных позициях для штрих-кода

7+5+8+0+2+4=26

- сумму умножаем на 3 – 26*3=78

- складываем цифры, стоящие на нечетных позициях (не учитывая последнюю цифру)

9+8+4+8+0+8=37

- складываем то, что получилось в результате двух последних действий с цифрами

78+37=115

- от результата оставляем только последнюю цифру, получится 5

- от 10 отнимаем то, что получилось в пятом действии 10-5=5

Этот результат совпал с контрольной цифрой. Значит, делаем вывод, что данный учебник лицензированный.

6) Учебник по основам безопасности и жизни деятельности, авторы М. П. Фролов, Е. Н. Литвинов, издательство «Астрель» , 2004

- складываем цифры, стоящие на четных позициях для штрих-кода 7+5+7+1+1+3=24

- сумму умножаем на 3 – 24*3=72

- складываем цифры, стоящие на нечетных позициях (не учитывая последнюю цифру) 9+8+1+0+1+3=22

- складываем то, что получилось в результате двух последних действий с цифрами

72+22=94

- от результата оставляем только последнюю цифру, получится 4

- от 10 отнимаем то, что получилось в пятом действии 10-4=6

Этот результат совпал с контрольной цифрой. Значит, делаем вывод, что данный учебник лицензированный.

7) Учебник по геометрии, авторы Л. С. Атанясян, издательство «Просвещение» , 2005

- складываем цифры, стоящие на четных позициях для штрих-кода 7+5+9+1+3+8=33

- сумму умножаем на 3 – 33*3=99

- складываем цифры, стоящие на нечетных позициях (не учитывая последнюю цифру) 9+8+0+0+4+9=30

- складываем то, что получилось в результате двух последних действий с цифрами

99+30=129

- от результата оставляем только последнюю цифру, получится 9

- от 10 отнимаем то, что получилось в пятом действии 10-9=1

Этот результат совпал с контрольной цифрой. Значит, делаем вывод, что данный учебник лицензированный.

8) Учебник по физике, автор А. В. Перышкин, издательство «Дрофа» , 2002

- складываем цифры, стоящие на четных позициях для штрих-кода

7+5+1+7+3+5=28

- сумму умножаем на 3 – 28*3=84

- складываем цифры, стоящие на нечетных позициях (не учитывая последнюю цифру) 9+8+7+0+5+5=34

- складываем то, что получилось в результате двух последних действий с цифрами

84+34=118

- от результата оставляем только последнюю цифру, получится 8

- от 10 отнимаем то, что получилось в пятом действии 10-8=2

Этот результат совпал с контрольной цифрой. Значит, делаем вывод, что данный учебник лицензированный.

9) Учебник по биологии, авторы Д. В. Колесов, Р. Д. Маш, И. Н. Беляев, издательство «Дрофа» , 2003

- складываем цифры, стоящие на четных позициях для штрих-кода

7+5+1+7+8=28

- сумму умножаем на 3 – 28*3=84

- складываем цифры, стоящие на нечетных позициях (не учитывая последнюю цифру)

9+8+7+7+3=34

- складываем то, что получилось в результате двух последних действий с цифрами

84+34=118

- от результата оставляем только последнюю цифру, получится 8

- от 10 отнимаем то, что получилось в пятом действии 10-8=2

Этот результат совпал с контрольной цифрой. Значит, делаем вывод, что данный учебник лицензированный.

10) Учебник по обществознанию, автор Л. Н. Боголюбова, издательство «Просвещение» , 2005

- складываем цифры, стоящие на четных позициях для штрих-кода

7+5+9+1+2+3=27

- сумму умножаем на 3 – 27*3=81

- складываем цифры, стоящие на нечетных позициях (не учитывая последнюю цифру)

9+8+0+0+4+3=24

- складываем то, что получилось в результате двух последних действий с цифрами

81+24=105

- от результата оставляем только последнюю цифру, получится 5

- от 10 отнимаем то, что получилось в пятом действии 10-5=5

Этот результат совпал с контрольной цифрой. Значит, делаем вывод, что данный учебник лицензированный.

Из всех расчетов можно сказать, что все учебники, по которым я обучаюсь, являются лицензированными. Поэтому мое здоровье не подвергается воздействию ядохимикатов, используемых при создании поддельных учебников. Бумага использована качественная - это продлевает «жизнь» учебника. Текст учебников напечатан без пунктуационных и орфографических ошибок. Рисунки и фотографии соответствуют тексту, который они иллюстрируют.

Заключение

Исследовав многие способы кодирования информации в деятельности человека, я нашла возможный способ определения подлинности любого товара. Проделав ряд расчетов, можно сказать, что все учебники, по которым я обучаюсь, являются лицензированными. Поэтому мое здоровье не подвергается воздействию ядохимикатов, используемых при создании поддельных учебников. Бумага использована качественная - это продлевает «жизнь» учебника. Текст учебников напечатан без пунктуационных и орфографических ошибок. Рисунки и фотографии соответствуют тексту, который они иллюстрируют.

Этой методикой подсчета овладеть очень легко. Научившись делать расчеты можно обезопасить себя от покупки поделанного товара, тем самым защитить свое здоровье, и не тратить дополнительные деньги на покупки новых более качественных товаров.

Конечно же на этом развитие криптографии не остановится, ее дальнейшее развитие для нашей страны будет реализовано в электронных паспортах личности.

Литература

1. Статья «История криптографии», «В мире информатики №15/ Информатика №47/2003»

2. Статья «Шифр Вижинера», «В мире информатики №53/ Информатика №6/2005»

3. Статья «Шифр Цезаря», «В мире информатики №1/ Информатика №34/2003»

4. Статья «Тарабарская грамота», «В мире информатики №77/ Информатика №18/2006»

5. Статья «Кодирование информации о товаре», «В мире информатики №55/ Информатика №8/2005»

6. Учебник «Информатика», под ред. Н. В. Макаровой, 7-8 класс, издательство «Питер», 2001

7. Баричев С. «Криптография без секретов»

Оглавление

Введение....3
§1. История криптографии....4
§2. Анализ известных шифров информации....5
Шифр Цезаря....5
Квадрат Полибия....6
Шифр Вижинера....7
«Тарабарская грамота»....7
Диск Леона Альберти....8
§3. Кодирование информации в компьютерных технологиях....9
Кодирование текстовой информации....11
Кодирование чисел....11
Кодирование графической информации....11
Кодирование звуковой информации....12
§4. Штрих-кодовое кодирование информации....13
§5. Практическая часть....15
Заключение....20
Литература....21