DOI 10.17223/20710410/4/9

УДК 519.7

МЕТОД АВТОМАТИЧЕСКОЙ ШИФРАЦИИ СООБЩЕНИЙ[1]

А. Д. Закревский

Объединенный институт проблем информатики НАН Беларуси, г. Минск, Беларусь

E-mail: zakrevskij@tut.by

Эта статья написана в 1959 г., публикуется впервые и исключительно в интересах исторической точности, без редакторской правки и с сохранением терминологии того времени. В ней для шифрования сообщений предложено использовать конечные автоматы с функцией выходов, биективной в каждом состоянии.

Ключевые слова: *конечный автомат, шифрование сообщений*[2].

Предлагаемая работа относится к области криптографии — науки о способах шифрации сообщений, которые могут быть перехвачены противником, и о способах расшифровки перехваченных сообщений при отсутствии ключа шифра.

Естественно, что получаемые криптографией существенные результаты являются секретными, поэтому о характере и эффективности развитых к настоящему времени методов криптографии автор может судить лишь из немногочисленных косвенных источников [1 – 3]. Тем не менее, представляется очевидным, что в последнее время развитие криптографии происходит на базе теории информации и теории автоматов. Неудивительно, что, по свидетельству Уивера [1], крупные теоретические исследования в области криптографии проводились американским математиком Шенноном — одним из основоположников теории информации (разумеется, эти работы Шеннона засекречены).

Излагаемые в данной работе результаты получены автором при рассмотрении общей теории цифровых автоматов. При исследовании класса таких автоматов, которые преобразуют информацию без её потерь, оказалось, что эти автоматы представляют эффективные шифровальные устройства, удовлетворяя требованиям простоты, автоматичности, быстродействия и высокой секретности шифра.

Область применения этих шифровальных устройств может быть весьма широка, охватывая различные системы связи, предназначенные для передачи как осведомительной, так и управляющей информации и связывающие как людей, так и автоматическую аппаратуру.

§ 1

Любое сообщение можно представить конечной последовательностью символов — значений, принимаемых некоторой случайной дискретной переменной x в дискретные моменты времени.

Если сообщение может попасть в руки противника, который может извлечь из него для себя пользу, то сообщение шифруется так, чтобы противник вообще не смог его расшифровать или, по крайней мере, смог его расшифровать только длительный промежуток времени спустя, когда сообщение потеряло бы уже свою ценность.

[1] Печатается по рукописи автора 1959 г. в авторской редакции. (*Прим. ред.*)

[2] Аннотация и ключевые слова написаны редакцией. (*Прим. ред.*)

Процесс шифрации сообщения, выражающийся заменой одной последовательности символов на другую, определяется выбором способа шифрации и ключа шифра, различие между которыми станет ясным при рассмотрении примеров шифрации. Можно сказать, что способ шифрации определяет общие правила шифрации, а ключ шифра конкретизирует их. В ряде случаев допускается, что противник может знать способ шифрации перехваченного им сообщения, но он не должен обладать ключом шифра.

При дальнейшем изложении мы всегда будем предполагать, что противнику известен способ шифрации и неизвестен ключ шифра.

Расшифровку сообщения по имеющемуся ключу будем называть дешифрацией. Оперативность шифрованной связи очевидно зависит от скорости дешифрации сообщений.

Качество шифрации будет тем выше, чем больше отношение времени, затрачиваемого на расшифровку сообщения противником, которому неизвестен ключ шифра, но известен способ шифрации, к суммарному времени, затрачиваемому на шифрацию и дешифрацию сообщения по известному ключу. При этом предполагается, что затраты средств в единицу времени (количество и квалификация людей и стоимость аппаратуры) одинаковы для обеих сторон.

Так как, вообще говоря, задача расшифровки сообщения при неизвестном ключе является задачей определения ключа и решение её усложняется при повышении качества шифрации, последнее можно ориентировочно оценивать минимальной длиной последовательности, представляющей сообщение, при которой (длине) сообщение может быть расшифровано без ключа.

Простейшим способом шифрации (в дальнейшем будем называть его элементарным (шифр Э)) является взаимно-однозначная замена всех символов последовательности.

Конкретная информация о том, на какие символы заменяются символы последовательности, содержится в ключе шифра. Например, по ключу

$$(\text{а} \sim \text{С},\ \text{Ю} \sim \text{Т},\ \text{К} \sim .,\ ...)$$

при шифрации символ «а» заменяется символом «С», символ «Ю» — символом «Т», символ «К» — символом «.» и т. д., при дешифрации производится обратная замена.

Задача расшифровки сообщения при отсутствии ключа может показаться чрезвычайно сложной. В самом деле, если n — число различных символов последовательности, то существует $n!$ различных ключей шифра Э и простой перебор этих ключей может оказаться практически неосуществимым (например, при $n = 40$ число ключей превышает 10^{47}).

В действительности эта задача весьма легко решается статистическими методами. Дело в том, что язык и характер сообщения находят своё отражение в статистической структуре представляющей сообщение последовательности.

Например, каждый письменный язык характеризуется определёнными, ему только свойственными, относительными частотами отдельных символов — букв, знаков препинания, пропусков между словами — и определёнными относительными частотами групп символов. Без риска сделать ошибку можно утверждать, что, выбирая наугад группу из трёх рядом расположенных символов в произвольном русском тексте, можно относительно часто встречаться с группой «про», реже с «тюл», ещё реже с «щер», исключительно редко с «ееe» и никогда (если в тексте нет опечаток) не встретиться с «ыыы».

Характер сообщения может, в частности, отражаться относительными частотами слов. Маловероятна, например, встреча в математическом тексте, посвящённом дока-

зательству некоей теоремы, слова «парнокопытное», характерного для зоологического текста.

Статистические характеристики последовательности мало нарушаются при описанном элементарном способе шифрации. В результате статистического анализа зашифрованной последовательности могут быть определены относительные частоты отдельных символов и их сравнение с относительными частотами незашифрованных последовательностей, представляющих сообщения на том же языке, позволит найти ключ шифра. Если последовательность достаточно длинна, то полученный в результате статистического анализа последовательности набор достаточно точно определённых относительных частот символов может сравниваться с наборами относительных частот символов, характеризующими различные языки, что даёт возможность нахождения как языка сообщения, так и ключа шифра, то есть решения задачи расшифровки.

Учёт статистических связей между соседними символами также облегчает расшифровку.

Чтобы разрушить статистические связи между соседними символами последовательности, применяется перестановка символов в группах длины m, порядок перестановок определяется ключом. В этом случае при дешифрации неизбежна теоретически минимальная задержка в m тактов (за один такт принимаем время приёма одного символа). Число различных перестановок m символов равно $m!$, сочетание шифра Э с перестановками даёт $n! \cdot m!$ различных ключей.

Расшифровка сообщения при этом способе затрудняется. Однако статистические характеристики сообщения при его шифрации разрушаются далеко не полностью, что даёт возможность, воспользовавшись ими при расшифровке, добиться успеха.

Другим из известных автору способов шифрации является следующее развитие элементарного способа шифрации: при шифрации последовательности происходит замена не отдельных символов, а целых групп — слов, их корней, окончаний, целых выражений и т. д. — на группы стандартной длины (например, на группы из пяти цифр). Ключами являются так называемые шифровальные книги, устанавливающие определённое соответствие между группами символов в незашифрованной и зашифрованной последовательностях. Число возможных ключей при этом способе можно ориентировочно оценить числом $M!$, где M — число групп, внесённых в кодовую книгу. Недостатком этого способа является сложность пользования им, приводящая к большим потерям времени на шифрацию и дешифрацию. В то же время статистический анализ может оказаться эффективным орудием расшифровки и в этом случае.

Общей характерной чертой известных автору по косвенным данным способов шифрации является их сложность и уязвимость со стороны статистического анализа, тем большая, чем проще шифр.

Особо важные сообщения шифруются очень сложным способом с высокой надёжностью шифра, но при этом и на дешифровку сообщений адресатом уходит много времени. Срочные сообщения поэтому таким способом шифровать нельзя, и к ним применяется более простой шифр; чем более срочное сообщение и чем меньше у адресата средств дешифрации, тем проще должен быть способ шифрации и тем ненадёжнее, следовательно, шифр.

В пределе этот принцип может привести к полному отказу от шифрации в тех случаях, когда затрата времени на дешифрацию нетерпима (например, при атаке, когда на первый план выступают требования быстрого и точного обмена осведомительной и управляющей информацией между частями). Просачивание информации в руки про-

тивника, которым в данном случае пренебрегают, может дать противнику некоторые преимущества, иногда довольно значительные.

§ 2

Расшифровка представляющей некоторое сообщение последовательности, зашифрованной по шифру Э, не представляет большого труда лишь тогда, когда последовательность достаточно длинна, чтобы статистический метод её анализа мог дать ощутимые результаты.

Минимальную длину последовательности, которая, будучи зашифрована по шифру Э, может быть расшифрована без ключа на базе статистического анализа, обозначим через $L(\text{Э})$ (очевидно, что величину $L(\text{Э})$ можно определить только ориентировочно).

Если длина зашифрованной по шифру Э последовательности $l << L(\text{Э})$, то сообщение практически расшифровать невозможно.

Если сообщение представлено длинной по сравнению с $L(\text{Э})$ последовательностью, то оно может быть разбито на отрезки не более чем по l символов каждый, которые можно зашифровать различными ключами.

Малый размер отрезков, на протяжении которых ключ фиксирован, не позволит противнику найти ключи, или, что то же самое, расшифровать сообщение с помощью статистических методов, теряющих в данном случае свою силу. Поэтому смена ключей является испытанным средством повышения секретности сообщения, тем более эффективным, чем чаще она производится.

Набор ключей и порядок их смены могут быть определены заранее, образуя обобщённый ключ, настолько сложный, что его раскрытие может оказаться практически невозможным.

Перейдём к рассмотрению такого способа шифрации, при котором заранее определён набор ключей с присвоенными им номерами, а порядок смены ключей определяется передачей по линии связи соответствующих этим номерам символов. Пусть последние являются одновременно символами шифруемой последовательности, в этом случае смена ключей будет происходить с частотой передачи символов.

Этот способ шифрации можно реализовать, применяя автоматическое устройство — шифратор, которое может находиться в одном из нескольких состояний, переходы между которыми будут соответствовать смене элементарных ключей, поставленных, в свою очередь, в соответствие состояниям автомата.

Порядок смены состояний автомата представим матрицей (z_{ik}):

$$\begin{pmatrix} z_{11} & z_{12} & \dots & z_{1m} \\ z_{21} & z_{22} & \dots & z_{2m} \\ \dots & \dots & \dots & \dots \\ z_{n1} & z_{n2} & \dots & z_{nm} \end{pmatrix},$$

строки i которой поставлены во взаимно-однозначное соответствие с символами поступающей на вход автомата последовательности, столбцы k — с состояниями автомата. Будем считать, что номера столбцов матрицы совпадают с номерами соответствующих им состояний автомата, а номера строк — с соответствующими им символами входной последовательности.

Элемент матрицы z_{ik} представляет номер состояния автомата, в которое он переходит из состояния k, если на его вход поступает символ i. Совокупность всех элементов

матрицы полностью определяет порядок смены состояний для любой заданной последовательности входных символов, поэтому матрицу (z_{ik}) назовём *матрицей переходов*.

Другой существенной характеристикой автомата является матрица (y_{ik}), представляющая множество элементарных ключей и определяющая в любой момент времени выходной символ как функцию входного символа и состояния автомата:

$$\begin{pmatrix} y_{11} & y_{12} & \dots & y_{1m} \\ y_{21} & y_{22} & \dots & y_{2m} \\ \dots & \dots & \dots & \dots \\ y_{n1} & y_{n2} & \dots & y_{nm} \end{pmatrix}.$$

Находясь в определённом состоянии, автомат вполне определённо преобразует поступающий на его вход символ в некий выходной символ, и это преобразование определяется соответствующим данному состоянию автомата элементарным ключом. Вместе с тем автомат переходит в другое состояние, определяемое как его предыдущим состоянием, так и входным символом, передаваемым по линии связи в зашифрованном виде.

Следующий символ последовательности будет зашифрован уже по другому элементарному ключу, соответствующему новому состоянию автомата, затем автомат может перейти в следующее состояние и т. д. Таким образом смена ключей производится автоматически каждый такт, в течение которого шифруется и передаётся один символ.

В результате последовательности входных символов и последовательности выходных символов оказываются взаимно-однозначно связаны, т. е. выходная последовательность представляет зашифрованную входную последовательность.

Пример 1. Рассмотрим автомат с алфавитом входных и выходных символов {а, б, в, г}, с матрицей (z_{ik}):

$i\backslash k$	0	1	2	3	4	5	6	7
а	2	0	1	2	3	0	2	0
б	7	1	5	4	4	6	1	4
в	5	4	4	0	1	5	7	6
г	3	6	6	7	7	0	5	5

и матрицей (y_{ik}):

$i\backslash k$	0	1	2	3	4	5	6	7
а	б	б	а	г	г	в	в	а
б	в	а	г	в	а	г	б	б
в	а	в	б	б	б	а	г	г
г	г	г	в	а	в	б	а	в

Допустим, что автомат находится в состоянии 0, затем на его вход подаётся последовательность символов

а б б а в г а б в г г г а б а б ...

Какова будет последовательность выходных символов?

Первый символ «а» поступает на автомат, когда тот находится в состоянии 0, соответствующим этому состоянию элементарным ключом он преобразуется в символ «б». Элемент $z_{\text{а}0}$ равен 2, поэтому автомат переходит в состояние 2 и т. д. В результате на выходе появляется последовательность:

б г г в б в а в г а б г г г в в ...,

представляющая зашифрованную входную последовательность.

Расшифровка подобных последовательностей весьма затруднительна и может оказаться практически невыполнимой, так как расшифровка сообщения может проводиться успешно лишь при получении определённых сведений о порядке смены ключей, а последний определяется последовательностью, которую требуется расшифровать. Так как смена ключей производится каждый такт, то становится невозможным применение статистического анализа для нахождения элементарных ключей на отрезках последовательности, на которых ключ не меняется — длина таких отрезков сокращается до одного символа.

Хаотическая в целом смена ключей приводит к тому, что относительные частоты различных символов и групп выходной последовательности окажутся в весьма сложной зависимости от подобных статистических характеристик входной последовательности. Представляется возможным с помощью соответствующего подбора набора элементарных ключей и матрицы переходов добиться распределения относительных частот, достаточно близкого к равномерному. В этом случае полностью или в весьма значительной степени теряет свою силу метод анализа относительных частот символов и групп, используемый обычно на первом (и наиболее важном) этапе расшифровки.

§ 3

Степень секретности шифра, определяемая трудностями расшифровки сообщения при отсутствии ключа, может быть количественно оценена методами теории информации.

Пусть n — число различных символов (строк матрицы), m — число состояний автомата (столбцов матрицы). Так как в каждом столбце матрицы (y_{ik}) допускаются все возможные перестановки n символов, а какие-либо связи между столбцами не накладываются, то существует $\mathfrak{A}_y = (n!)^m$ различных допустимых матриц (y_{ik}).

Число различных матриц (z_{ik}), элементами которых служат номера состояний (столбцов), в которые переходит автомат, равно $\mathfrak{A}_z = m^{nm}$, но не все они могут представлять шифраторы. Ограничиваясь поэтому рассмотрением класса сильно-связных автоматов, характерным свойством которых является возможность перехода из любого состояния в любое (реализуемая при подаче соответствующей последовательности символов на вход автомата), воспользуемся грубой оценкой нижнего предела числа различных соответствующих этим автоматам матриц (z_{ik}). Мы не выйдем за пределы данного класса, рассматривая матрицы с заранее заданными элементами одной из строк, обеспечивающей сильную связность представляемого матрицей автомата (например, каждый элемент этой строки может представлять номер следующего столбца, а элемент последнего столбца — номер начального). С учётом всевозможных комбинаций значений других элементов получим искомый нижний предел $m^{(n-1)m}$, т. е. $m^{(n-1)m} < \mathfrak{A}_z < m^{nm}$.

В итоге, число различных шифраторов $\mathfrak{A}_m > (n!)^m \cdot m^{(n-1)m}$, а стоящая перед расшифровщиком неопределённость может быть оценена количественной мерой, предлагаемой теорией информации, — энтропией, определяемой двоичным логарифмом числа возможных вариантов (если они равновероятны):

$$H_m = \log_2 \mathfrak{A}_m \approx m \cdot \log_2(n!) + m \cdot (n-1) \cdot \log_2 m.$$

Пример 2. Пусть число различных символов, образующих подаваемую на вход шифратора последовательность, равно 64, а число состояний автомата — 32. Тогда $H_m \approx 18\,000$ дв. единиц, т. е. если ключ неизвестен, то его придётся искать среди $2^{18\,000} \approx 10^{5\,400}$ других ключей, что, скорее всего, окажется практически невыполнимой задачей.

Очевидно, что методы расшифровки последовательности должны основываться на её статистическом анализе, позволяющем за счёт избыточности сообщения, не уничтожающейся при шифрации, а принимающей более скрытую форму, т. е. также шифруемой, получать информацию как о самом сообщении, так и о ключе шифра.

Очевидно также, что количество информации, которую можно таким образом получить, представляет монотонно возрастающую функцию от длины анализируемой зашифрованной последовательности. Следовательно, расшифровка сообщения становится в принципе возможна лишь при достижении некоторой «критической» длины последовательности, зашифрованной автоматом Ш: $l \approx L(\text{Ш})$.

Величина $L(\text{Ш})$ определяется скоростью накопления информации о шифре при анализе зашифрованной последовательности и энтропией шифра: анализируемая последовательность достигает размера $L(\text{Ш})$, когда количество накопленной информации о шифре достигает значения априорной энтропии шифра H_m.

В отличие от развитых к настоящему времени статистических методов теории связи при процессе расшифровки весьма большое внимание уделяется семантической стороне сообщения, и это позволяет в какой-то мере увеличивать скорость накопления информации о шифре при расшифровке. Эффективной контрмерой всегда может служить увеличение энтропии шифра путём увеличения числа состояний автомата-шифратора или другими способами, на которых мы остановимся в дальнейшем.

Представление о трудностях расшифровки можно получить, познакомившись с попытками решения в некоторой степени аналогичной задачи, рассмотренной Муром [4].

Определить логическую структуру (т. е. найти матрицы (y_{ik}) и (z_{ik})) автомата с n состояниями, m входными и p выходными символами, имея возможность последовательно подавать любые символы на вход и наблюдать соответствующие по времени выходные символы.

Полученный Муром результат говорит, что для решения такой экспериментальной задачи потребуется подача на вход последовательности, длина которой имеет порядок $n^{nm+2} \cdot p^n/n!$, указывающий на практическую невозможность решения задачи уже при $n = m = p = 8$: для подачи соответствующей последовательности с частотой 1 миллион символов в секунду потребуется около 10^{50} лет.

Задача расшифровки легче в том отношении, что на матрицы (y_{ik}) и (z_{ik}) наложены некоторые условия, например, в одном столбце матрицы (y_{ik}) не может быть двух одинаковых символов. Но она значительно сложнее в другом отношении: при эксперименте доступны лишь выходные символы автомата-шифратора, а о характере входных последовательностей могут быть сделаны лишь весьма общие предположения.

§ 4

Дешифрация полученной адресатом последовательности, зашифрованной автоматом Ш, может производиться автоматически, с помощью автомата-дешифратора Д, матрицы (y'_{ik}) и (z'_{ik}) которого взаимно-однозначно связаны с соответствующими матрицами автомата-шифратора Ш.

Установим это соответствие.

Потребуем, чтобы автомат Д производил дешифрацию последовательности, пропущенной через автомат Ш, если состояние автомата Д в любой момент времени совпадает с состоянием автомата Ш в этот же момент времени. Получаем

$$\left.\begin{array}{l} y_{ik} = j \\ y'_{jk} = i \end{array}\right\} (k = 1, 2, \ldots, n). \tag{1}$$

Теперь обеспечим синхронное изменение состояний автоматов Ш и Д:

$$z'_{ik} = z_{jk}\ (k = 1, 2, \ldots, n), \tag{2}$$

где i и j связаны системой (1).

Пример 3. Автомат, являющийся дешифратором по отношению к автомату-шифратору, рассмотренному в примере § 2, обладает следующими матрицами (z'_{ik}) и (y'_{ik}):

$i\backslash k$	0	1	2	3	4	5	6	7
а	5	1	1	7	4	5	5	0
б	2	0	4	0	1	0	1	4
в	7	4	6	4	7	0	2	5
г	3	6	5	2	3	6	7	6

$i\backslash k$	0	1	2	3	4	5	6	7
а	в	б	а	г	б	в	г	а
б	а	а	в	в	в	г	б	б
в	б	в	г	б	г	а	а	г
г	г	г	б	а	а	б	в	в

,

получаемыми из матриц (z_{ik}) и (y_{ik}) по соотношениям (1) и (2). Нетрудно убедиться, что подаваемая на вход автомата Д последовательность

б г г в б в а в г а б г г г в в ...

преобразуется автоматом в последовательность

а б б а в г а б в г г г а б а б ...,

т. е. автомат производит требуемую дешифрацию.

Симметрия соотношений (1) и (2) относительно индексов i и j обеспечивает следующее ценное с практической точки зрения свойство соответствующих автоматов Ш и Д: они могут меняться своими ролями — автомат Д может служить шифратором, а автомат Ш — дешифратором, что даёт возможность вести дуплексную связь без дублирования шифровальной аппаратуры.

§ 5

Энтропию преобразования последовательности при шифрации можно повысить с помощью последовательного соединения автоматов

$$\longrightarrow \text{Ш}_1 \longrightarrow \text{Ш}_2 \longrightarrow \ldots \longrightarrow \text{Ш}_n \longrightarrow \boxed{\text{канал связи}} \longrightarrow \text{Д}_n \longrightarrow \ldots \longrightarrow \text{Д}_2 \longrightarrow \text{Д}_1 \longrightarrow,$$

где энтропия преобразования последовательности цепью последовательно соединённых автоматов Ш_1, Ш_2, ..., Ш_n равна сумме энтропий преобразования отдельных автоматов:

$$H(\sum_{i=1}^{n} \text{Ш}_i) = \sum_{i=1}^{n} H(\text{Ш}_i).$$

Отметим симметричный характер цепи и некоммутативность операторов преобразования Ш_i, так как цепь

$$\longrightarrow \text{Ш}_k \longrightarrow \text{Ш}_{k+1} \longrightarrow$$

не эквивалентна, в общем случае, цепи

$$\longrightarrow \text{Ш}_{k+1} \longrightarrow \text{Ш}_k \longrightarrow .$$

Из симметричности цепи и некоммутативности операторов Ш_i следует некоммутативность операторов Д_i.

Другими способами повышения энтропии шифрации последовательности могут служить:

а) разбавление шифруемой последовательности не несущими семантической информации символами;

б) периодическая смена матриц шифра, в частности, новые матрицы могут целиком передаваться по каналу связи, зашифрованные предыдущими матрицами. Периоды смены матриц T, измеряемые количеством передаваемых за период символов, должны удовлетворять неравенству $T << L(\text{Ш})$.

Представляется, однако, что вряд ли эти способы потребуются — секретность зашифрованного автоматом Ш сообщения может быть без этого достаточно высока.

§ 6

Помехоустойчивость шифруемой по данному методу системы связи может быть обеспечена применением обычных корректирующих кодов (типа кода Хэмминга). В противном случае система может оказаться весьма чувствительной к воздействию помех. Методом повышения помехоустойчивости системы может также служить периодическое (или апериодическое) восстановление автоматов Ш и Д, причём роль восстановителей могут играть одиночные символы или группы символов.

Влияние помехи на канал связи между автоматами Ш и Д выразится в нарушении синхронности изменения соответствующих состояний автоматов Ш и Д. Символы-восстановители, подаваемые на вход автоматов, будут восстанавливать нарушенное соответствие.

Такой символ можно освободить от других нагрузок, связанных с переносом семантической информации, и представляя его лишь в одной определённой строке матриц (y_{ik}) и (y'_{ik}) (во всех столбцах), единообразно заполнить номером какого-либо состояния соответствующие символу-восстановителю строки матриц (z_{ik}) и (z'_{ik}).

Частоту разбавления этими символами последовательности, несущей информацию, можно регулировать в зависимости от эффективности помех, имея в виду, что повышение этой частоты влечёт снижение секретности шифра.

§ 7

В этой работе не рассматриваются методы синтеза автоматов по заданным матрицам (y_{ik}) и (z_{ik}). Этим вопросам, представляющим самостоятельный интерес, посвящён целый ряд опубликованных работ [5 – 7], ими занимаются, в частности, и в нашей лаборатории.

Приведём лишь некоторые результаты проведённых исследований.

Синтез автоматов Ш и Д по заданным матрицам производится без особого труда как с применением релейно-контактных схем, так и с применением электронных схем.

Быстродействие релейно-контактных автоматов Ш и Д имеет порядок 10 симв./с, электронных автоматов — 10^5 симв./с, если пользоваться стандартными дешёвыми элементами.

Автоматы Ш и Д просты в производстве и эксплуатации и обеспечивают полную автоматичность шифрации и дешифрации. Цепи, структура которых определяется

матрицами (y_{ik}) и (z_{ik}), могут быть сконцентрированы в небольшом сменном блоке пассивного действия, смена которого соответствует смене ключа шифра (таким блоком, в частности, может служить обычная перфокарта).

Такая система шифрации обладает высокой секретностью, так как наличие у противника полной информации о способе шифра (даже наличие у него экземпляров применяемых автоматов Ш и Д) не позволяет производить расшифровку перехваченных сообщений, если неизвестны применявшиеся при их шифрации матрицы.

Дешифрация сообщений автоматом Д с соответствующим сменным блоком производится без задержки.

Простота, быстродействие и полная автоматичность шифрации позволяют расширить сферу её применения. Можно рекомендовать предлагаемый метод шифрации к использованию в каналах связи, по которым происходит обмен осведомительной и управляющей информацией не только между людьми, но и между человеком и автоматическим устройством и между автоматическими взаимодействующими системами. Такая шифрация может обеспечить, с одной стороны, помехоустойчивость телеуправляющих систем, с другой стороны, секретность идущей от автоматов осведомительной информации.

ДОБАВЛЕНИЕ

Уже после написания этой статьи автор ознакомился с обстоятельной работой К. Шеннона (*C. E. Shannon.* Communication theory of secrecy systems. Bell S. T. J. 28. 1949. P. 656–715).

Сравнение излагаемого в нашей работе метода с методами, приводимыми в статье Шеннона, показывает, что он может быть эффективным, так как удовлетворяет выдвигаемым в работе Шеннона критериям:

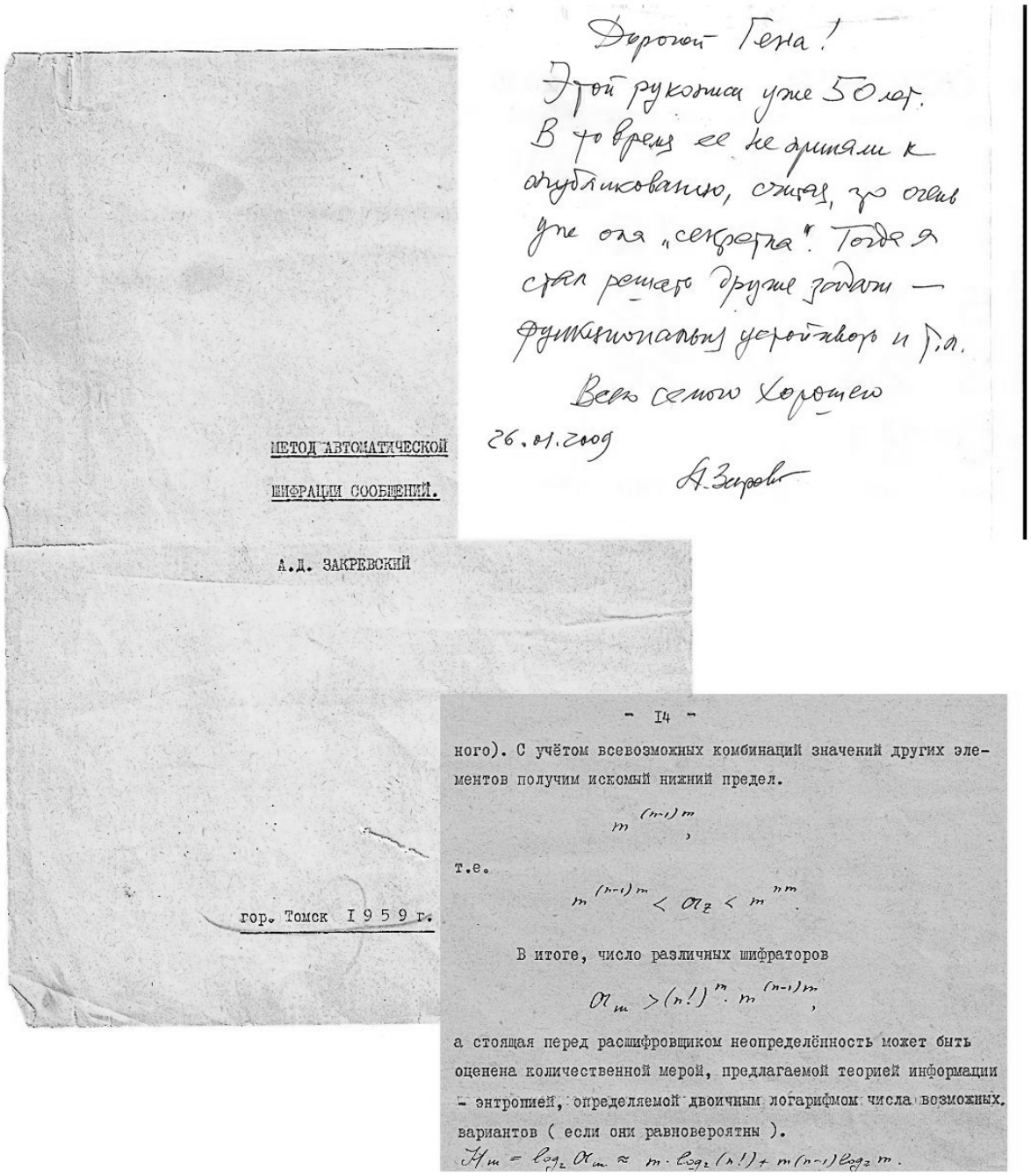
1. Процессы шифрации и дешифрации просты в том смысле, что они полностью автоматизированы.
2. Размер ключа (матриц (y_{ik}) и (z_{ik})) довольно мал.
3. Сложность преобразования высока, и трудности расшифровки криптограммы противником велики, в чём можно убедиться сравнением задачи с аналогичной задачей, рассмотренной Муром [4].
4. Борьба с помехами может вестись простым способом — добавлением в криптограмму восстанавливающих символов, долю которых в общем числе символов можно регулировать в зависимости от эффективности помех.
5. Повышение секретности шифра может проводиться разбавлением сообщения символами, не несущими информации, но при этом увеличивается размер криптограммы.

   Сохраняя последний, секретность шифра можно повышать, последовательно соединяя автоматы-шифраторы.
6. К достоинствам метода можно отнести также практическое отсутствие задержки при дешифрации (величина задержки не превышает периода следования символов).

ЛИТЕРАТУРА

1. *Уивер У.* Перевод // Сборник «Машинный перевод». М.: ИЛ, 1957.
2. *Винер Н.* Кибернетика и общество. М.: ИЛ, 1958.
3. *Гольдман.* Теория информации. М.: ИЛ, 1958.

4. *Мур Т.* Эксперименты с последовательностными автоматами // Сборник «Автоматы». М.: ИЛ, 1956.
5. *Huffman D.* The synthesis of sequential switching circuits // J. of the Franklin Inst. 1954. Т. 257. № 3. P. 161–190, № 4. P. 275–303.
6. *Трахтенброт Б. А.* Синтез логических сетей, операторы которых описаны средствами исчисления одноместных предикатов // ДАН СССР. 1958. Т. 118. № 4. С. 646–649.
7. *Цейтлин М. Л.* Матричный метод синтеза электронно-импульсных и релейно-контактных (непримитивных) схем // ДАН СССР. 1957. Т. 117. № 6.



Дорогой Гена!
Этой рукописи уже 50 лет.
В то время ее не решился к опубликованию, считая, что очень уже она „секретна". Тогда я стал решать другие задачи — функциональных устройств и т.п.
Всего самого хорошего
26.01.2009
А. Закревский

МЕТОД АВТОМАТИЧЕСКОЙ
ШИФРАЦИИ СООБЩЕНИЙ.

А.Д. ЗАКРЕВСКИЙ

гор. Томск 1959 г.

- I4 -

ного). С учётом всевозможных комбинаций значений других элементов получим искомый нижний предел.

$$m^{(n-1)m},$$

т.е.

$$m^{(n-1)m} < \alpha_2 < m^{nm}.$$

В итоге, число различных шифраторов

$$\alpha_m > (n!)^m \cdot m^{(n-1)m},$$

а стоящая перед расшифровщиком неопределённость может быть оценена количественной мерой, предлагаемой теорией информации – энтропией, определяемой двоичным логарифмом числа возможных вариантов (если они равновероятны).

$$H_m = \log_2 \alpha_m \approx m \cdot \log_2 (n!) + m(n-1)\log_2 m.$$

Фрагменты рукописи А. Д. Закревского с автографом автора