МИНОБРНАУКИ РОССИИ

Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет «Московский институт электронной техники»
Кафедра «Информационная безопасность»

РЕФЕРАТ

ПО ДИСЦИПЛИНЕ

«ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

ТЕМА: «МЕТОДЫ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ»

Студент ИБ-21 учебной группы _____ (Иванов И.И.)
подпись *(фамилия, инициалы)*

2024 г.

ПЕРЕЧЕНЬ УЛОВНЫХ ОБОЗНАЧЕНИЙ И СОКРАЩЕНИЙ

Исходное сообщение или Открытый текст – сообщение, текст которого необходимо сделать непонятным для посторонних.

Шифрование (зашифрование) данных – процесс преобразования открытых данных (исходного сообщения) в зашифрованные данные (шифротекст, криптограмму) при помощи шифра.

Шифр – совокупность обратимых преобразований множества возможных отрытых данных (исходного сообщения) во множество возможных шифротекстов, осуществляемых по определённым правилам с применением ключей.

Ключ – конкретное секретное состояние некоторого параметра (параметров), обеспечивающее выбор одного преобразования из совокупности возможных для используемого метода шифрования.

Дешифрование – метод извлечения информации из зашифрованных данных (криптограммы) без знания криптографического ключа.

Расшифрование – метод извлечения информации из зашифрованных данных (криптограммы), зная криптографический ключ.

АС – Автоматизированная система.

ЭВМ – электронная вычислительная машина.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Одним из важнейших методов защиты информации является её криптографическое преобразование.

В современном мире в результате бурного развития вычислительной техники, когда информация не то, что есть на каждом углу, а буквально везде, в том числе и конфиденциальная, как никогда важны методы криптографической защиты информации. Во многих прикладных областях основной задачей становится обеспечение целостности информации, под которой понимается гарантия поступления информации из достоверного источника и в неискажённом виде. В век цифровизации наши данные регулярно обрабатываются в различных центрах обработки данных, простых персональных компьютерах, передаваясь по различным каналам связи. Разумеется, столь большой поток важных данных для злоумышленников как красная тряпка для быков. Получив доступ к личным, приватным данным преступник может их использовать в своих корыстных целях. И ведь такой существенной информацией для преступной деятельности могут выступать не только документы или данные о субъекте из АС банковских расчётов или иной финансовой организации. Люди регулярно обмениваются сообщениями, в которых может содержаться разного уровня пользы информация – те же паспорта, выписки со счетов, информационная утечка из организаций о будущем крахе/подъёме акций в цене, да и в конце концов – фото, которые злоумышленники могут использовать для шантажа. Так же никто не отменял возможности фишинга в результате утечек открытых данных. Всё, что объединяет эти все случаи – открытость данных. Не важно каким образом злоумышленник получил доступ к данным. Важно то, что в результате получения доступа к потоку данных, он (злоумышленник) получил готовые (открытые) данные. Ему не нужно долго думать о том, как их прочитать и использовать – они уже готовы. И тут на помощь всем приходит наука, появившаяся как следствие математического анализа данных, под названием криптография, а вместе с ней и криптоанализ.

Именно благодаря криптографии мы можем спокойно обмениваться информацией по различным каналам связи. Наши данные защищены от прочтения при простом перехвате. Криптография помогает обеспечить безопасность нашей информации, то есть обеспечить такие свойства как: конфиденциальность, доступность и целостность. Современная криптография также предоставляет ресурсы для решения задачи аутентификации и невозможности отказа сторон от авторства. Кроме того, решение проблемы управления ключами тоже возложено на средства современной криптографии.

В рамках данной работы я поставил для себя следующие цели:

- Разобрать теоретическую базу, необходимую для понимания и ознакомления с последующими главами и результатами данной работы;

- Классифицировать методы криптографического преобразования информации;

- Указать на отличительные особенности различных методов криптографического преобразования информации;

- Сформулировать ряд требований к криптографическому преобразованию и самому алгоритму его исполнения, обеспечивающим эффективный уровень защиты информации в АС;

- Выделить популярный в современном мире метод криптографической защиты информации.

В ходе работы будем использовать и анализировать различные учебные пособия, нормативные акты, со списком которых можно ознакомится в соответствующей части реферата.

Актуальность данной темы обеспечивается тем «бесконечным» потоком данных, информации, которой мы на ежедневной основе пользуемся, применяя средства ЭВМ для поиска, получения и передачи информации. Все эти данные должны быть защищены на достаточном уровне, их информационная безопасность должна быть обеспечена, чему и способствует использование различных методов криптографической защиты информации.

1 Теоретическая база для криптографии

Согласно [1], метод криптографии можно определить, как некоторое множество отображений одного пространства (пространства возможных сообщений) в другое пространство (пространство возможных криптограмм). Каждое конкретное отображение из этого множества соответствует шифрованию при помощи конкретного ключа.

Пользуясь описанием из [2], можно заявить, что криптографические методы защиты информации в АС могут применяться для защиты информации, обрабатываемой в ЭВМ и передаваемой по линиям связи. Поэтому криптографические методы могут использоваться как внутри отдельных устройств или звеньев системы, так и на различных участках линий связи.

Сам процесс шифрования заключается в проведении обратимых математических, логических, комбинаторных и других преобразований исходной информации, в результате которых зашифрованная информация представляет собой хаотический набор букв, цифр, других символов и (или) двоичных кодов.

Для шифрования информации используется алгоритм преобразования (шифр) и ключ. Как правило, алгоритм для определённого метода шифрования является неизменным. Исходными данными для алгоритма служат информация, подлежащая процессу зашифрования, и ключ шифрования. Ключ содержит управляющую информацию, которая определяет выбор преобразования на определённых шагах алгоритма и величины аргументов, используемых при реализации алгоритма шифрования. Ключ, как элемент системы криптографической защиты информации, должен периодически обновляться. Именно это обеспечивает оригинальное представление защищаемой информации при использовании одного и того же алгоритма. Знание ключа позволяет просто и надёжно расшифровать криптограмму. Однако без знания ключа эта процедура часто обращается в практически невыполнимую даже при условии того, что сам алгоритм шифрования известен.

Сам процесс криптографического закрытия информации может осуществляться как программно, так и аппаратно. Однако аппаратная реализация алгоритмов и методов криптографического преобразования информации обладает рядом преимуществ, главное из которых – высокая производительность.

Вывод по разделу

Таким образом, мы разъяснили необходимую нам теоретическую базу, что позволяет нам перейти к следующей главе.

2 Методы криптографического преобразования информации

Известны различные подходы к классификации методов криптографического преобразования информации. Основываясь на сведениях из [3], в данной работе мы будем разделять методы криптографического преобразования по виду воздействия на исходную информацию (рисунок 1).

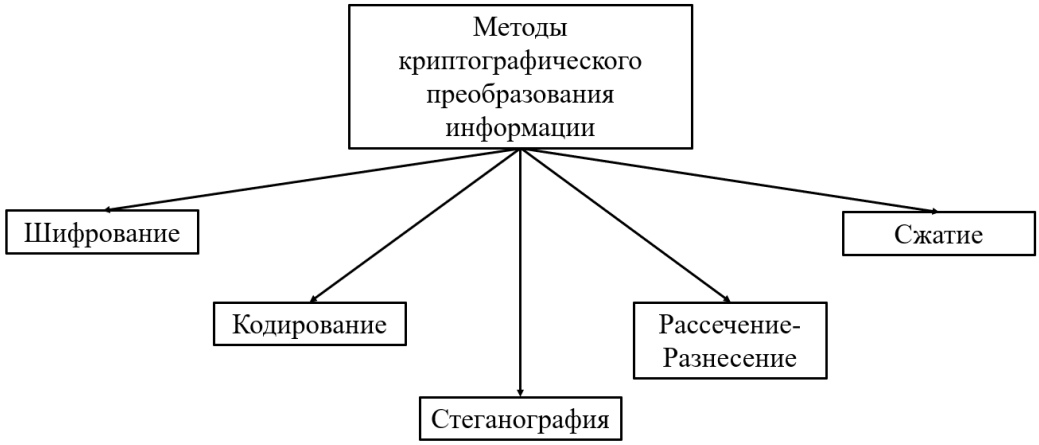

Рисунок 1 – Классификация методов криптографического преобразования информации

Классифицировав методы криптографического преобразования информации, теперь мы можем их описать, указать на их особенности, отличающие их от всех остальных представленных методов.

Сжатие информации – преобразование информации с целью сокращения её объёма. Сжатая информация не может быть прочитана или использована без обратного преобразования.

Само по себе сжатие может быть отнесено к методам криптографического преобразования информации с определёнными оговорками. Учитывая доступность средств сжатия и обратного преобразования, этот метод не является надёжным для криптографического преобразования информации. Даже при условии, что алгоритмы сжатия будут засекречены, они могут быть сравнительно легко раскрыты статистическими методами обработки. Поэтому сжатые файлы с конфиденциальной информацией должны быть подвержены последующему шифрованию, с целью обеспечения безопасности данной информации.

Пользуясь [4], определим метод рассечения-разнесения и принцип его работы на небольшом примере. Рассечение-разнесение заключается в том, что массив защищаемых

данных делится (рассекается) на такие элементы, каждый из которых в отдельности не позволяет раскрыть содержание защищаемой информации. Выделяемые таким образом элементы данных разносятся по разным зонам ЗУ (запоминающего устройства) или вовсе располагаются на различных носителях.

Ключом такого метода является способ разбиения изначальных данных. Например, ключом для такого метода может быть числовой набор {5, 8, 2, 7, 4, 6, 3, 1}. Эти числа мы в таком же порядке размещаем вдоль исходного текста, ставя в соответствие каждому символу. По итогу мы получим 8 отдельных бессмысленных наборов символов, которые уже можно будет разнести по разным зонам ЗУ.

Теперь разберём метод стеганографии. Согласно [5], методы компьютерной стеганографии предназначены для скрытия факта передачи сообщения путем встраивания скрываемой информации во внешне безобидные данные (текстовые, графические, аудио- или видеофайлы) и включают в себя две группы методов, основанных:

- на использовании специальных свойств компьютерных форматов хранения и передачи данных;

- на избыточности аудио-, визуальной или текстовой информации с позиции психофизиологических особенностей восприятия человека.

Следовательно, в отличие от остальных методов криптографического преобразования информации, методы ***стеганографии*** позволяют скрыть не только смысл хранящейся или передаваемой информации, но и сам факт хранения или передачи закрытой информации. В компьютерных сетях стеганография имеет некоторые перспективы на использование. В основе всех методов стеганографии лежит маскирование закрытой информации среди открытых файлов. Появление обработки мультимедийных файлов в АС открыло практически неограниченные возможности для применения стеганографии.

Существует несколько методов скрытой передачи информации. В частности, стеганография может быть применена с помощью такой вспомогательной информации, как графическая или звуковая (аудио) информация, представленная в числовом виде. Так, например, в графических объектах наименьший элемент изображения (из числового вида) может кодироваться одним байтом. В младшие биты определённых байтов (самый первый бит в байте) помещают биты скрытого файла в соответствии с алгоритмом криптографического преобразования. Правильно подобранный алгоритм и само изображение позволят сделать так, что по итогу этих преобразований скрытых данных на фоне изображения практически не видно. Невооруженным глазом их не заметить. Изображение, полученное непосредственно по в ходе преобразования, оказывается трудно отличимым от исходного. Зачастую, найти такие данные помогут только специализированные инструменты, но тем не менее это всё ещё

остаётся очень трудной задачей даже при наличии такого инструментария. Как правило, за основу такого метода берут изображение местности, снимок со спутника, фото самолёта и тому подобные, поскольку они лучше всего подходят под эти цели.

С помощью средств стеганографии можно замаскировать текст, изображение, речь, цифровую подпись, зашифрованное сообщение. Комплексное использование стеганографии и шифрования на порядок увеличивает сложность решения задачи обнаружения и дешифрования информации.

Разберёмся, что понимается под термином кодирование. Содержанием процесса кодирования информации является замена смысловых конструкций исходной информации (слов или целых предложений) кодами. В качестве самих кодов могут использоваться сочетания букв, цифр, букв и цифр. При кодировании и обратном преобразовании (декодировании) используются специальные таблицы (алфавиты и т.п.) или словари.

Алфавит кодирования – это множество используемых для кодирования знаков.

Кодирование информации целесообразно применять в системах с ограниченным набором смысловых конструкций. Такой вид криптографического преобразования применим, например, в командных линиях АС или в ЭВМ. Например, ЭВМ не воспринимает символы как таковые, он понимает только числа. Поэтому символы необходимо закодировать таким образом, чтобы с ними могла работать ЭВМ. В таком случае отдельное внимает стоит уделить кодированию ASCII и двоичному кодированию.

ASCII (American Standard Code for Information Interchange) — это таблица кодировки символов, в которой каждой латинской букве, числу, знаку или управляющему символу соответствует определенное число. В стандартной таблице ASCII 128 символов, пронумерованных от 0 до 127. В случае необходимости кодировки большего числа символов чаще всего применяют либо расширенную ASCII таблицу, либо стандарт кодирования символов Unicode. Сама ASCII таблица восьмибитная (т. к. $2^8 = 128$, следовательно можно зашифровать 128 символов). Как следствие, её удобно представить в виде таблицы с восьмью строками (рисунок 2).

	.0	.1	.2	.3	.4	.5	.6	.7	.8	.9	.A	.B	.C	.D	.E	.F
0.	NUL	SOH	STX	ETX	EOT	ENQ	ACK	BEL	BS	HT	LF	VT	FF	CR	SO	SI
1.	DLE	DC1	DC2	DC3	DC4	NAK	SYN	ETB	CAN	EM	SUB	ESC	FS	GS	RS	US
2.		!	"	#	$	%	&	'	(	)	*	+	,	-	.	/
3.	0	1	2	3	4	5	6	7	8	9	:	;	<	=	>	?
4.	@	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
5.	P	Q	R	S	T	U	V	W	X	Y	Z	[	\	]	^	_
6.	`	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
7.	p	q	r	s	t	u	v	w	x	y	z	{	|	}	~	DEL

Рисунок 2 – Кодовая таблица ASCII

Десятичное представление символов из ASCII таблицы удобно для понимания человеком, однако для последующего использования такой информации на ЭВМ, она преобразуется в двоичный код, поскольку именно в двоичных данных ЭВМ воспринимает и обрабатывает информацию. Преобразование закодированного символа десятичным числом (или любым другим числом в любой другой системе счисления) в двоичный код происходит переводом данного числа в двоичную систему счисления. Например: $48_{10} = 110000_2$, $41_{16} = 65_{10} = 1000001_2$.

Недостатками кодирования конфиденциальной информации является необходимость хранения и распространения кодировочных таблиц, которые необходимо регулярно менять, чтобы избежать возможного раскрытия кодов статистическими методами обработки перехваченных сообщений.

Как пример исторического соблюдения правила регулярной смены шифров можно назвать наиболее распространённую и известную даже в кинематографе шифровальную машину «Энигма», пользуясь которой во время Второй мировой войны гитлеровские радисты передавали актуальную и секретную информацию о военных действиях и планах. Именно регулярная смена шифра позволяла сохранять конфиденциальность передаваемой информации.

Выделяют так же и посимвольное кодирование – каждому известному символу ограниченной системы символов в сопоставление ставится иной символ из этого же набора в случайном или специально определённом порядке. В таком случае это уже отдельный случай, описывающийся собственным термином. Такой метод криптографического преобразования называется – шифрование. Хоть мы уже и определили понятие «шифрование данных», однако как метод, шифрование определяется чуть-чуть иначе:

Шифрование – замена символов исходного сообщения посредством использования конкретного алгоритма их замены (шифра).

У самого шифрования имеются свои способы, которые можно классифицировать. В качестве первичного признака для классификации – тип преобразования, осуществляемого с исходного сообщения при шифровании.

Шифр замены – символы исходного сообщения заменяются некоторыми эквивалентами, согласно алфавиту или таблице.

Шифр перестановки – символы исходного сообщения переставляются по определённому алгоритму внутри определённого блока символов. То есть изменяется лишь порядок следования символов исходного сообщения.

Гаммирование (gamma xoring) – процесс «наложения» гамма-последовательности на открытый текст. Обычно применяется в варианте двоичных данных при помощи оператора XOR $\oplus$.

Гамма-последовательность или просто гамма – обычно этот термин применяется в отношении псевдослучайных элементов, которые генерируются по определённому закону и алгоритму.

Композиционный шифр – комбинирование использование двух или более шифров для последовательного шифрования исходного сообщения.

Таким образом, все шифры можно разделить на три класса, в результате которого образуется первый уровень классификации шифров (рисунок 3).

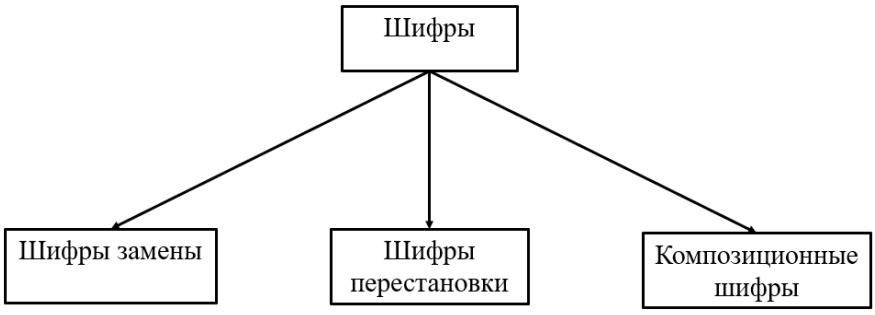

Рисунок 3 – Основные классы шифров

В современной криптографии широко используется деление шифров по типу ключей. Если ключ зашифрования совпадает с ключом расшифрования, шифры называют симметричными. Асимметричными в ином случае.

При симметричном шифровании используется один ключ (секретный), с помощью которого отправитель А зашифровывает открытый текст, а получатель Б – расшифровывает.

Очевидно, что для выбранного ключа и алгоритма, преобразование должно быть обратимым, то есть существует некоторое преобразование, которое при выбранном ключе вернёт открытый текст. При этом сам ключ передаётся от отправителя А к получателю Б отдельно по (защищенному или очень надёжному) каналу связи. Использование одного ключа приводит к повышению скорости передачи информации, однако это влечёт за собой потери в надежности такого шифрования в связи с потенциальным перехватом ключа шифрования злоумышленником. Принцип симметричного шифрования изображен на схеме (рисунок 4).

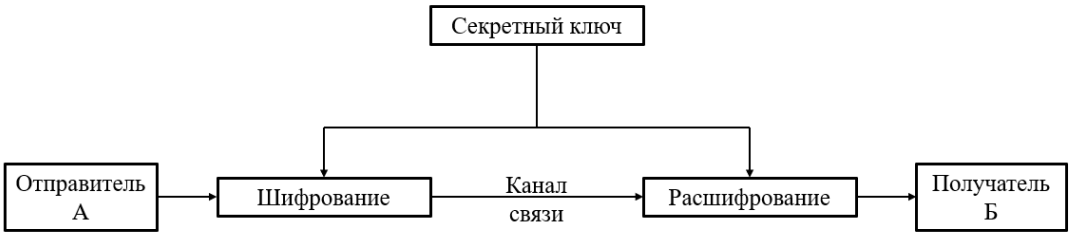

Рисунок 4 – Симметричное шифрование

Симметричные шифры подразделяют на поточные и блочные.

В случае с поточными преобразованиями – на протяжении работы со всем исходным текстом его символы последовательно заменяются по порядку их расположения, а символ зашифрованного текста, в который превращается исходный символ, непосредственно зависит от ключа и расположения исходного символа в потоке открытого текста. Такое шифрование обеспечивает скорость обработки информации с последующим её шифрованием, соизмеримую со скоростью поступления этой информации, вне зависимости от размеров получаемых данных.

При блочном преобразовании текст предварительно разбивается на блоки равной фиксированной длины, которые затем зашифровываются как отдельные элементы. Отдельные блоки информации обычно занимают от 4 до 32 байт. Шифрование может как иметь, так и не иметь взаимную зависимость блоков при преобразовании. В случае шифрования независимыми блоками, шифротекст остаётся уязвим к атаке методами выявления статистических зависимостей, поэтому шифрование с зависимыми от предыдущих блоками является более надёжным.

Асимметричное шифрование, в свою очередь, хоть и сложнее, но зато намного надёжнее. Для того, чтобы реализовать асимметричное шифрование необходимы два взаимосвязанных ключа: открытый и секретный. Получатель всем сообщает свой открытый

ключ, при помощи которого другие могут зашифровать сообщение, отправляемое ему. Получив сообщение, тот расшифровывает его при помощи своего секретного ключа, который он ни в коем случае никому не должен сообщать. То есть отличительная особенность такого метода шифрования заключается в разделении ключей для зашифрования и расшифрования. При этом ключ зашифрования не требуется засекречивать. Открытый ключ может быть общедоступным, а как итог содержаться в публичных записях (справочниках) совместно с публичными идентифицирующими данными его владельца. Принцип асимметричного шифрования изображен на схеме (рисунок 5).

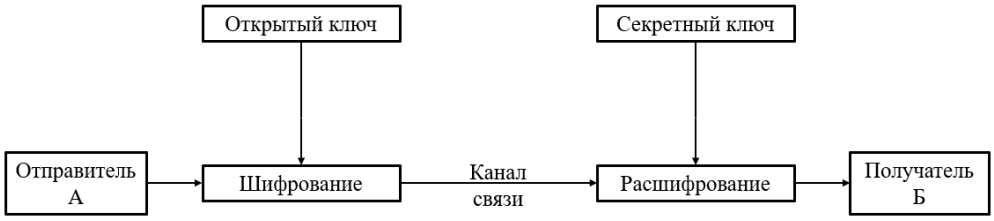

Рисунок 5 – Асимметричное шифрование

Основное преимущество асимметричного шифрования перед симметричным состоит в отсутствии необходимости передачи секретного ключа, как следствие пропадает угроза перехвата злоумышленником секретного ключа по техническим каналам связи. А недостаток такого шифрования заключается в трудоёмкости его реализации. Сложные вычисления взаимосвязанных ключей приводят к замедлению процесса зашифрования и расшифрования текста. Даже при использовании передовых ЭВМ этот процесс может занимать значительное количество времени.

Сами механизмы использования асимметричных шифров предполагают использование различных методов замены, поэтому само деление шифров по типу ключей целесообразно производить в классе шифров замены.

Вывод по разделу

В этой главе мы разделили методы криптографического преобразования по виду воздействия на исходную информацию, указали на их особенности, разобрав каждый из них и выделив (если было возможным) важные подразделения этих методов.

3 Требования к криптографическому преобразованию и алгоритму его исполнения

Для того, чтобы криптографическое преобразование обеспечивало эффективную защиту информации в АС, оно должно удовлетворять ряду требований. Эти требования были выявлены и выражены в процессе практического применения криптографии, а часть их вовсе основана на технически-экономических соображениях. Основываясь на [2, 6], их можно сформулировать следующим образом:

- Сложность и стойкость криптографического закрытия должны выбираться в зависимости от объёма и степени секретности данных;

- Надежность закрытия должна быть такой, чтобы секретность не нарушалась даже в том случае, когда злоумышленнику становится известен метод закрытия;

- Метод закрытия, набор используемых ключей и механизм их распределения не должны быть слишком сложными, так как в противном случае потребуются большие затраты вычислительных и временных ресурсов;

- Выполнение процедур прямого и обратного преобразований должно быть формальным. Эти процедуры не должны зависеть от длины сообщений;

- Ошибки, возникающие в процессе выполнения преобразования, не должны распространятся по системе;

- Вносимая процедурами защиты избыточность в массивы хранимых и обрабатываемых данных должна быть минимальной.

Кроме того, непосредственно к самим алгоритмам шифрования так же сформулирована система требований, которым они должны соответствовать:

- Зашифрованный текст должен поддаваться чтению только при наличии ключа шифрования (доступ только после идентификации и аутентификации пользователя);

- Число операций для определения использованного ключа шифрования по фрагменту криптограммы и соответствующим ей исходным данным должно быть не меньше общего числа возможных ключей;

- Знание механизма работы алгоритма шифрования не должно влиять на его надежность;

- Незначительные изменения ключа шифрования должны приводить к существенному изменению вида зашифрованных данных;

- Незначительные изменения шифруемых данных должны приводить к существенному изменению итогового вида зашифрованных данных даже при использовании одного и того же ключа;

- Длина зашифрованного текста должна быть равна длине исходного текста, любой ключ из множества возможных должен обеспечивать надёжную защиту информации;

- Алгоритм должен допускать как программную, так и аппаратную реализацию.

Вывод по разделу

Подытоживая главу, можно заявить, что, используя [2, 6], мы сформулировали необходимые требования к криптографическому преобразованию и алгоритму его исполнения, выполнив которые можно считать, что преобразование обеспечивает эффективную защиту информации в АС.

4 Популярный в современном мире метод криптографической защиты информации

В современном мире особое место в мире криптографии занимает криптосистема RSA, название которой образовано из первых букв фамилий предложивших её авторов (Rivest R., Shamir A., Adleman L.). Согласно [3], система относится к блочным экспоненциальным системам асимметричного шифрования, так как каждый блок M открытого текста рассматривается как целое число в интервале (0, n – 1) и преобразуется в блок C следующим открытым преобразованием – формула (1):

$$C = E(e,n)(M) = M^e \bmod n, \quad (1)$$

где *E (e, n)* – преобразование шифрования;

а *(e, n)* – ключ зашифрования.

При расшифровании блок открытого текста расшифруется аналогичным образом – формула (2):

$$M = D(d,n)(C) = C^d \bmod n, \quad (2)$$

где *D (e, n)* – преобразование шифрования;

а *(d, n)* – ключ расшифрования.

В основе самого метода лежит достаточно сложное теоретическое обоснование. Но базово стоит понимать, несколько фактов. Числа *e* и *d* связаны с *n* определённой зависимостью, а также существуют рекомендации по выбору ключевых элементов на основе простых чисел (их нахождение занимает значительное количество времени у компьютера, если идёт речь о больших простых числах, например, больше 2^{31}). Если взять пару простых чисел p и q, определить на их основе $n = p * q$, то можно определить пару чисел e и d, удовлетворяющим заданным условиям. Если сделать открытой пару чисел *(e, n)*, а ключ d держать в секрете, то полученная система будет являться RSA-криптосистемой открытого шифрования.

Как и со всеми другими методами криптографической защиты информации, максимальная защита шифруемой информации гарантируется при качественном соблюдении сохранности/секретности ключа, в данном случае – ключа расшифрования или исходных простых чисел, благодаря которым и получаются ключи для RSA-шифрования. На практике наибольший успех среди всех атак на RSA криптосистемы имеют те атаки, что нацелены на незащищённые этапы управления ключами системы. Сама по себе криптосистема RSA достаточно надежна при использовании ключа достаточной длины. Банально 256-битный ключ методом грубой силы не приносит никакой пользы, так как существующее число возможных комбинаций – примерно 10^{77}. Даже самым мощным суперкомпьютерам потребуются миллиарды лет на перебор всех вариантов. То есть, теоретически – взлом возможен, однако практически – нереален.

Область применения криптосистемы RSA достаточно широка. Она используется в программных и аппаратных средствах, на различных платформах и в целом во многих отраслях. В наше время криптосистема RSA встраивается во множество коммерческих комплексов, число которых лишь увеличивается. Она используется в операционных системах Microsoft, Apple, Novell и других. Примером аппаратной реализации RSA-шифрования являются защищенные телефоны, сетевые платы Ethernet, смарт-карты, криптографическое оборудование от фирмы THALES. Кроме этого, данный алгоритм входит в состав всех основных протоколов для защищённых коммуникаций Internet, в том числе S/MIME, SSL и S/WAN, а также во множестве различных учреждений, начиная от корпораций и заканчивая государственными лабораториями и правительственными службами.

Вывод по разделу

В данной главе мы разобрались с одним из самых популярных методов криптографической защиты информации в современном мире – алгоритм RSA. Разобрали его принцип действия, привели небольшую теоретическую основу этого алгоритма, рассмотрели его стойкость с практической точки зрения, а также затронули область применения алгоритма RSA.

ЗАКЛЮЧЕНИЕ

По итогам данной работы было проведено непосредственное изучение материала для его анализа и подведения необходимых итогов по изучаемым пунктам. Мы выяснили, что криптография и её методы преобразования информации носят важную роль в современном мире, но более подробно изучили именно вопрос методологии в криптографии.

Ознакомившись с необходимой в данной области теоретической справкой на достаточном нам уровне, мы классифицировали методы криптографического преобразования информации, указали их особенности.

На основе полученных в ходе исследования данных, сформулировали ряд требований к криптографическому преобразованию и самому алгоритму его исполнения, обеспечивающим эффективный уровень защиты информации в АС, приняв во внимание особенности практической реализации данных методов

Мы также выделили и ознакомились с одним из самых популярных и часто используемых методов криптографической защиты информации – алгоритм RSA.

Как итог – все цели, поставленные в введении, были выполнены.

Результаты данной работы может быть использована в просветительской деятельности за счёт емкости излагаемого в ней материала. Не смотря на некоторую возможную краткость в рассказе, данная работа раскрывает саму суть и объясняет основные моменты в методологии криптографической защиты информации, даёт понимание самих методов и их классификации. Этот реферат может являться кратким экскурсом или введением в криптографическую методологию для студентов в рамках курса по «основам информационной безопасности».

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Хорев, А.А. Лекции по дисциплине «Основы информационной безопасности» [Мультимедиа] – М. : МИЭТ, 2024.
2. Воеводин, В. А. Программно-аппаратные средства защиты информации : учебное пособие / В. А. Воеводин, А. В. Душкин, А. Н. Петухов, А. А. Хорев ; под ред. А. А. Хорева. – М. : МИЭТ, 2021. – 280 с. : ил.
3. Бутакова, Н. Г. Криптографическая защита информации : учебное пособие / Н. Г. Бутакова, В. А. Семененко, Н. В. Федоров. – М. : МГИУ, 2011. – 316 с.
4. Шурховецкий, Г. Н. Защита информации в облачных технологиях методом рассечения-разнесения / Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки №3 – 03.2021 г. [Электронный ресурс]. – Режим доступа: http://www.nauteh-journal.ru/files/74a28f6b-ed66-4a65-b123-6fa94f03a586 (дата обращения: 13.11.2024)
5. ФСТЭК РФ. «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных»: [утверждена Заместителем директора ФСТЭК России 15 февраля 2008 г.] [Электронный ресурс]. – Режим доступа: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/bazovaya-model-ot-15-fevralya-2008-g (дата обращения: 13.11.2024)
6. Афанасьева, Д. В. Средства криптографической защиты информации [Электронный ресурс] / Д. В. Афанасьева, А. А. Абидарова ; Известия ТулГУ. Технические науки. Вып. №3 – 2019 г. – Режим доступа: https://cyberleninka.ru/article/n/sredstva-kriptograficheskoy-zaschity-informatsii (дата обращения: 13.11.2024)