**Лекция 3. Шифрование методом гаммирование. Модульное гаммирование. Случайные и псевдослучайные гаммы. Нулевая вертикальная биграмма(НВБ).**

**Гамма** - в криптографии - псевдослучайная числовая последовательность, вырабатываемая по определенному алгоритму и используемая для зашифрования открытых данных и расшифрования зашифрованных данных.

**Гаммирование** - преобразование исходного (открытого) текста, при котором символы исходного текста складываются (по модулю, равному мощности алфавита или по модулю 2) с символами последовательности, вырабатываемой по определенному правилу.

В шифрах символы исходного сообщения заменяются числами, которые складываются по модулю с числами гаммы. Ключом шифра является гамма, символы которой последовательно повторяются.

Перед шифрованием символы сообщения и гаммы заменяются их номерами в алфавите и само кодирование выполняется по формуле

***Ci = (Ti+Gi) mod N***

**Примечания:**

а) ***mod*** - операция целочисленного деления, вычисляющая остаток от деления. Например, ***18 mod 5 = 3***

или ***48 mod 44 = 4***. Данная операция доступна в Windows-калькуляторе в режиме "Инженерный".

б) ***N*** равен количеству символов применяемого алфавита.

в) ***Ci***, ***Ti*** и ***Gi*** - номера ***i***-х символов, соответственно, шифрограммы, шифруемого текста и гаммы

г) если ***Ci*** будет равно нулю, то его следует приравнять ***N***.

Создание шифрограммы завершается заменой полученных чисел ***Ci*** на соответствующие буквы алфавита.

**Пример**.- «КАФЕДРА СИСТЕМ ИНФОРМАТИКИ», используемая гамма - «СИМВОЛ».



Рис. 1. Схема шифрования гаммированием по модулю ***N***

В данной теме используется алфавит, состоящий из 44 символов

**Таблица 1. *Алфавит «Русские буквы, цифры и пробел» (44 символа)***

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5  | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 |
| А | Б | В | Г | Д | Е | Ё | Ж | З | И | Й | К | Л | М | Н | О | П | Р | С | Т | У | Ф | Х |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 | 33 | 34 | 35 | 36 | 7 | 38 | 39 | 40 | 41 | 42 | 43 | 44 |
| Ц | Ч | Ш | Щ | Ъ | Ы | Ь | Э | Ю | Я | пробел | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |

Дешифрирование выполняется по формуле

***Ti = (Ci-Gi+N) mod N*** ,

где ***Ti*** – это символы исходного сообщения, ***Ci*** – символы зашифрованного сообщения, ***Gi*** – символы гаммы.

**Примечание:**

если ***Ti=0***, то его следует взять равным ***N***.

В примере ниже зашифрованное выше сообщение вновь приводится к исходному виду



Рис. 2. Схема дешифрирования гаммированием по модулю ***N***

**Случайные и псевдослучайные гаммы**

Секретные ключи представляют собой основу криптографических преобразований, для которых, следуя правилу Керкхофа, стойкость хорошей шифровальной системы определяется лишь секретностью ключа. Однако в практике создание, распределение и хранение ключей редко были сложными технически, хотя и дорогими задачами.
Основная проблема классической криптографии долгое время заключалась в трудности генерирования непредсказуемых двоичных последовательностей большой длины с применением короткого случайного ключа. Для ее решения широко используются генераторы двоичных псевдослучайных последовательностей. Существенный прогресс в разработке и анализе этих генераторов был достигнут лишь к началу шестидесятых годов. Поэтому в данной главе рассмотрены правила получения ключей и генерации на их основе длинных псевдослучайных последовательностей, используемых криптографическими системами для преобразования сообщения в шифровку. Получаемые программно из ключа, случайные или псевдослучайные ряды чисел называются на жаргоне отечественных криптографов гаммой, по названию у - буквы греческого алфавита, которой в математических записях обозначаются случайные величины. Интересно отметить, что в книге "Незнакомцы на мосту", написанной адвокатом разведчика Абеля, приводится термин гамма, который специалисты ЦРУ пометили комментарием - "музыкальное упражнение?", то есть в пятидесятые годы они не знали его смысла. Получение и размножение реализаций настоящих случайных рядов опасно, сложно и накладно. Физическое моделирование случайности с помощью таких физических явлений, как радиоактивное излучение, дробовой шум в электронной лампе или туннельный пробой полупроводникового стабилитрона не дают настоящих случайных процессов. Хотя известны случаи удачных применений их в генерации ключей, например, в российском криптографическом устройстве КРИПТОН. Поэтому вместо физических процессов для генерации гаммы применяют программы для ЭВМ, которые хотя и называются генераторами случайных чисел, но на самом деле выдающие детерминированные числовые ряды, которые только кажутся случайными по своим свойствам. От них требуется, чтобы, даже зная закон формирования, но не зная ключа в виде начальных условий, никто не смог бы отличить числовой ряд от случайного, как будто он получен бросанием идеальных игральных костей. Можно сформулировать три основных требования к криптографически стойкому генератору псевдослучайной последовательности или гаммы:

 Период гаммы должен быть достаточно большим для шифрования сообщений различной длины.

Гамма должна быть трудно предсказуемой. Это значит, что если известны тип генератора и кусок гаммы, то невозможно предсказать следующий за этим куском бит гаммы с вероятностью выше х. Если криптоаналитику станет известна какая-то часть гаммы, он все же не сможет определить биты, предшествующие ей или следующие за ней.
Генерирование гаммы не должно быть связано с большими техническими и организационными трудностями.

Самая важная характеристика генератора псевдослучайных чисел - информационная длина периода, после которого числа либо начнут просто повторяться, либо их можно будет предсказывать. Эта длина фактически определяет возможное число ключей системы и зависит от алгоритма получения псевдослучайных чисел. Требуемую длину периода определяет степень секретности данных. Чем длиннее ключ, тем труднее его подобрать. Однако не только длина ключа гарантирует его стойкость к взлому. В том случае, если содержание шифрованного сообщения жизненно важно для государства и им заинтересуется национальная служба безопасности, то заранее нужно быть готовым к неудаче в столь неравном состязании. Люди из спецслужб легко найдут требуемый ключ своими специфическими неджентльменскими методами, далекими от математики и криптографии. Скорее всего, ключ им даст сам владелец на блюдечке с голубой каемкой и будет этому искренне рад.

**Вторая** проблема состоит в следующем: на основании чего можно сделать заключение, что гамма конкретного генератора является непредсказуемой? Пока в мире нет еще универсальных и практически проверяемых критериев, позволяющих утверждать это. Неизвестна и общая теория криптоанализа, которая могла бы быть применена для такого доказательства, за исключением все возрастающего количества конкретных способов анализа, выработанных для различных практических целей. Интуитивно случайность воспринимается как непредсказуемость. Чтобы гамма считалось случайной, как минимум необходимо, чтобы ее период был очень большим, а различные комбинации бит определенной длины равномерно распределялись по всей ее длине. Итак, второе требование к ряду заключается в подтверждаемом статистически подобии его свойств настоящей случайной выборки. Каждый порядок элементов гаммы должен быть так же случаен, как и любой другой. Это требование статистики можно толковать и как сложность закона формирования ряда псевдослучайных чисел. Практически, если по достаточно длинной реализации этот закон вскрыть не удается ни на статистическом уровне, ни аналитически, то этим нужно удовлетвориться. Чем длиннее требуемая длина ряда, тем жестче к нему требования. Теперь подробнее расскажем, как вскрывались скрытые закономерности в последовательностях чисел. С древнейших времен люди наблюдали и изучали периодически повторяющиеся процессы, как фазы Луны, движения планет, чередования времен года, но не все такие цикличности выражены явно. Например, солнечные пятна, наблюдаемые невооруженным глазом с начала нашей эры и в телескопы с начала XVII века, дают пример скрытой периодичности в II лет, впервые обнаруженной Генрихом Швабе лишь в 1843 году. А вот среднегодовые температуры и изменение климата Земли связаны с циклами в 19 лет. Работы Винера и Хинчина поставили анализ периодичностей с головы на ноги. Ими предложено оценивать спектр случайных колебаний значений элементов гаммы как преобразование Фурье функции автокорреляции. При этом шумоподобному равномерному спектру гаммы без скрытых периодичностей соответствует автокорреляционная функция в виде одиночного выброса в нуле, то есть так называемая дельта-функция. Этот результат можно интерпретировать как непохожесть последовательности на себя при любом ее сдвиге.

И, **третье** требование связано с возможностью практической реализации генератора в виде программы или электронного устройства, быстродействием, необходимым для применения в современных коммуникациях, а также удобством его практического использования.