34. Основные концепции и понятия информационной безопасности. Модели безопасности. Симметричные криптосистемы. Блочные криптосистемы. Асимметричные криптосистемы. Схема шифрования RSA. Схема шифрования Эль-Гамаля. ***Информационная безопасность*** – состояние защищенности инф-и от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений.Субъекты информационных отношений: потребители информации, обладатели (держатели) информации, производители информации.

Защита информации – комплекс мероприятий, направленных на обеспечение информационной безопасности.

Свойства информации:

Конфиденциальность – с инфой может ознакомиться только ограниченный круг лиц, определенный ее владельцем. Важна для данных стратегических исследований, медицинских и страховых записей и т.п. ***Целостность*** – способность сохраняться в неискаженном виде. Важна для данных, связанных с функционированием объектов критических инфраструктур (управление воздушным движением, энергоснабжения), финансовых данных. ***Доступность*** – способность системы предоставлять временный беспрепятственный доступ к информации субъектам, обладающим соответствующими полномочиями. Важный атрибут для функционирования информационных систем, ориентированных на обслуживание клиетов. ***Достоверность*** – общая точность и полнота информации. ***Аутентичность*** – возможность достоверно установить автора сообщения. ***Апеллируемость*** – возможность доказать, что автором является именно данный человек и никто другой.

. Модели безопасности. Угрозы информационной безопасности.

Угроза информационной безопасности – потенциально возможное событие, процесс или явление, которое посредством воздействия на информацию может прямо или косвенно привести к нанесению ущерба интересам субъектов информационных отношений.

Атака – попытка реализации угрозы.

Нарушение – реализация угрозы.

Классификация угроз ИБ:

- По аспекту ИБ: угрозы конфиденциальности, целостности, доступности. Дополнительно: угрозы аутентичности и апеллируемости.
- По компонентам АИС, на которые нацелена угроза: данные, ПО, АО, поддерживающая инфраструктура.
- По расположению источника угроз: внутри или вне рассматриваемой АИС.
- По природе возникновения:
- Естественные (объективные) – угрозы, вызванные воздействиями на АИС и ее элементы объективных физических процессов или стихийных природных явлений, независящих от человека.
- Искусственные (субъективные) – угрозы, вызванные деятельностью человека. Могут быть непреднамеренными и преднамеренными.

Основные понятия криптографии

Криптология – наука, изучающая математические

методы защиты информации путем ее преобразования.

Криптография – совокупность методов преобразования данных, направленных на то, чтобы сделать эти данные бесполезными для противника.

Криптоанализ – наука о раскрытии исходного текста зашифрованного сообщения без доступа к ключу.

Криптосистема – информационная сиcетма, в которой обеспечивается безопасность передачи данных.

. **Симметричные криптосистемы.** Основной постулат: хранение ключа втайне.

- Сложность передачи обеим сторонам секретного ключа.

+ Обладают высоким быстродействием.

Симметричные криптосистемы:

1) Поточные.

2) Блочные.

В (1) на основе ключа вырабатывается некоторая последовательность – выходная гамма, которая затем накладывается на текст сообщения.

(2) разбивают текст сообщения на отдельные блоки, затем осуществляют преобразование этих блоков с использованием ключа.

Обобщенная схема (симметричной) криптосистемы:

M – открытый текст.

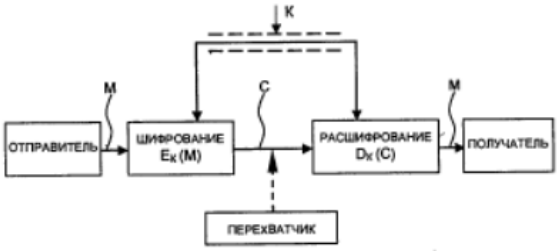


Рис.1.1. Обобщенная схема криптосистемы

K – секретный ключ (передается по закрытому каналу)

$E_k(M)$ – процесс зашифрования $D_k(M)$ – процесс расшифрования

Отправитель генерирует открытый текст исходного сообщения M, которое должно быть передано законному получателю по незащищенному каналу.

За каналом следит перехватчик.

Отправитель шифрует сообщение M с помощью криптографического преобразования E_K и получает шифротекст $C = E_K(M)$.

Законный получатель, приняв шифротекст C, расшифровывает его с помощью обратного преобразования $D = E_K^{-1}$ и получает исходное сообщение в виде открытого текста M.

$$D_K(C) = E_K^{-1}\left(E_K(M)\right) = M.$$

Криптоалгоритм – преобразование E_K из семейства криптографических преобразований.

Криптографический ключ K – параметр, с помощью которого выбирается отдельное используемое криптопреобразование.

Криптографическая система – это однопараметрическое семейство $(E_K)_{K\in\bar{K}}$ обратимых преобразований $E_K:\bar{M}\to\bar{C}$ из пространства сообщений $\bar{M}$ открытого текста в пространство $\bar{C}$ шифрованных текстов. Параметр К (ключ) выбирается из конечного множества $\bar{K}$, называемого пространством ключей.

Преобразование шифрования может быть симметричным или ассиметричным относительно преобразования расшифрования.

Плюсы:

- наиболее высокая скорость шифрования;
- с их помощью обеспечивается как конфиденциальность и подлинность, так и целостность.

Минус: проблема распределения ключей шифрования между пользователями.

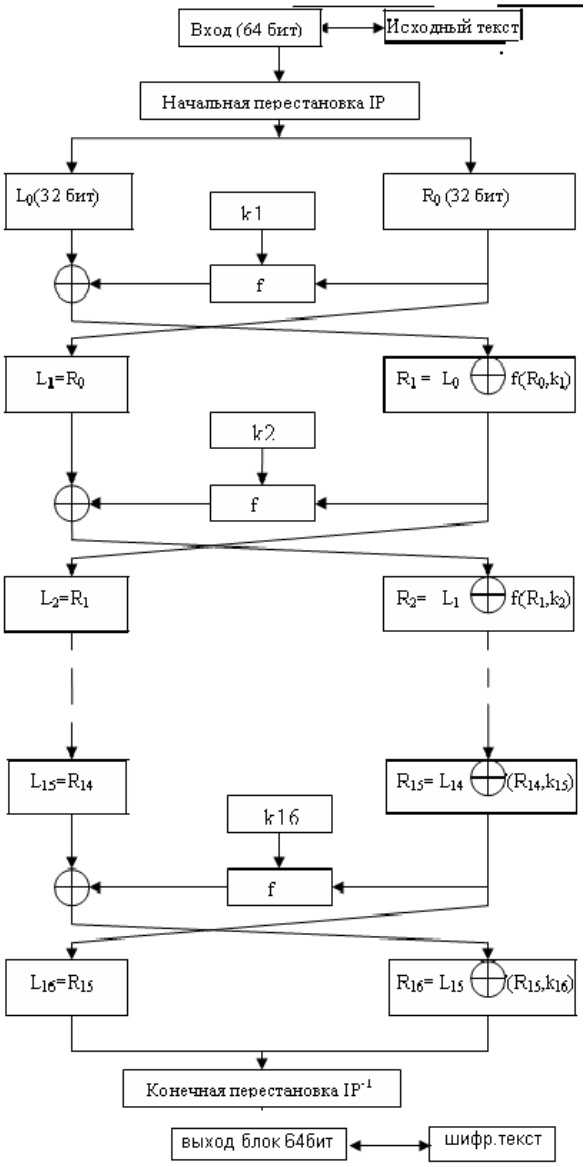
Имитовставка – разновидность контрольной суммы, некоторая эталонная характеристика сообщения, по которой осуществляется проверка целостности последнего.

3.Блочные криптосистемы. в практических шифрах необходимо использовать 2 общих принципа: Рассеивание – распространение влияния одного знака открытого текста на множество знаков шифротекста, что позволяет скрыть статистические свойства открытого текста. Перемешивание – использование таких шифрующих преобразований, которые усложняют восстановление взаимосвязи статистических свойств открытого и шифрованного текстов.

DES Основные достоинства DES:

1) Исп-ся только 1 ключ длиной 56 бит
2) Зашифровать сообщение с помощью одного пакета программ, для расшифрования можно исп-ть любой другой пакет программ сообветствующий стандарту DES
3) Относительная простота алгоритма обеспечивает высокую скорость обработки
4) Достаточно высокая стойкость алгоритма

Схема шифромания алгоритма DES:



Начальная перестановка

Исходный текст T (блок 64 бит) преобразуется с помощью начальной перестановки IP которая определяется таблицей.

16 циклов преобразования Фейстеля:

Разбить IP(T) на две части L_0, R_0, где L_0, R_0 — соответственно 32 старших битов и 32 младших битов блока T_0 IP(T)= L_0, R_0

Пусть $T_{i-1} = L_{i-1}R_{i-1}$ результат (i-1) итерации, тогда результат i-ой итерации $T_i = L_iR_i$ определяется: $R_i = L_{i-1} \oplus f(R_{i-1}, k_i)$

$L_i = R_{i-1}$

$R_i = L_{i-1} \oplus f(R_{i-1}, k_i)$

Левая половина L_i равна правой половине предыдущего вектора $L_{i-1}R_{i-1}$. А правая половина R_i — это битовое сложение L_{i-1} и $f(R_{i-1}, k_i)$ по модулю 2.

Основная функция шифрования

Аргументами функции f являются 32-битовый вектор R_{i-1} и 48-битовый ключ k_i, который является результатом преобразования 56-битового исходного ключа шифра k.

Для вычисления функции f последовательно используются

1. функция расширения E,
2. сложение по модулю 2 с ключом k_i
3. преобразование S, состоящее из 8 преобразований S-блоков S_1, S_2, …, S_8.
4. перестановка P.

Функция E расширяет 32-битовый вектор R_{i-1} до 48-битового вектора $E(R_{i-1})$ путём дублирования некоторых битов из R_{i-1}; порядок битов вектора $E(R_{i-1})$ указан в таблице.

Режимы работы блочных шифров

1) Электронная кодовая книга (ECB) – режим прост в обращении, но слабо защищен от возможных атак с удалениями и вставками. Ошибка, допущенная в одном символе шифротекста, влияет на целый блок в расшифрованном тексте.

2) Режим сцепления блоков шифротекста (CBC) – наилучший способ эксплуатации блочного шифра, т.к. предназначен для предотвращения потери в результате атаки с использованием удалений и вставок. Ошибочный бит шифротекста при расшифровании превращает в ошибочный блок, в котором он содержится, и следующий блок, что легко интерпретировать как атаку.

3) Обратная связь по выходу (OFB) – блочный шифр превращается в поточный. Ошибка в один бит в шифротексте даст только один ошибочный бит в расшифрованном тексте.

4) Обратная связь по шифротексту (CFB) – блочный шифр превращается в поточный. Ошибка в шифротексте влияет как на блок, в котором она допущена, так и на следующий блок.

ГОСТ 28147-89 — советский и российский стандарт симметричного шифрования, введённый в 1990 году, также является стандартом СНГ. Полное название — «ГОСТ 28147-89 Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования». Блочный шифроалгоритм.

Алгоритм шифрования данных представляет собой 64-битовый блочный алгоритм с 246-битовым ключом.

ГОСТ предусматривает три режима шифрования:

1) Простая замена.

2) Гаммирование.

3) Гаммирование с обратной связью.

В любом режиме размер блока – 64 бита, но в режимах гаммирования существует возможность обработки неполного блока данных размером менее 8 байт, что существенно при шифровании массивов данных произвольных размеров, меньше 8 байт, не кратных 8.

Обозначения:

$T_O, T_{Ш}$ – массивы открытых и закрытых данных.

$T_i^O, T_i^{Ш}$ – i-е по порядку 64-битовые блоки открытых и закрытых данных.

$$T_O = \left(T_1^O, \ldots, T_n^O\right), T_{Ш} = \left(T_1^{Ш}, \ldots, T_n^{Ш}\right), 1 \le i \le n$$

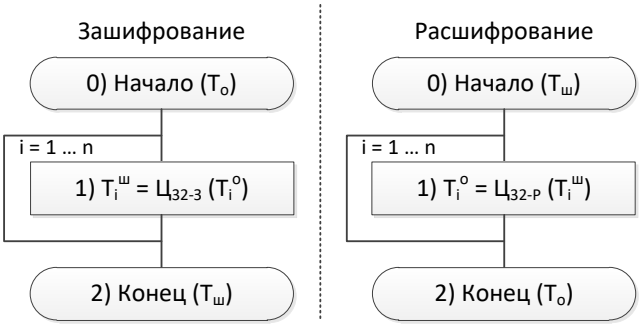
$$\left|T_i^O\right| = \left|T_i^{Ш}\right| = 64$$

$$1 \le i \le n, 1 \le \left|T_i^O\right| = \left|T_i^{Ш}\right| \le 64$$

n – число 64-битных блоков в массиве данных.

$Ц_X$ – цикл №X.

Простая замена



Размер массива данных должен быть кратен 64 битам и не должен изменяться.

Особенности режима простой замены:

1) Так как блоки данных шифруются независимо друг от друга и от их позиции в массиве, при зашифровании двух одинаковых блоков открытого текста получаются одинаковые блоки шифротекста и наоборот.

2) Если длина шифруемого массива не кратна 64 битам, возникает проблема, как дополнять последний блок.

Режим простой замены подходит для шифрования ключевой информации.

Гаммирование

Если размер блока меньше 64 бит, то усекаем гамма и складываем.

Хотя элементы гамма вырабатываются одинаковыми порциями в 64 бита, использоваться может и часть такого блока с размером, равным размеру шифрующего блока. Гамма получается с помощью некоторого алгоритмического рекуррентного генератора последовательности чисел (РГПЧ). Полученные блоки в 64 бита подвергаются преобразованию по циклу 32-3, т.е. зашифровываются в режиме простой замены. В результате получаются блоки гамма.

РГПЧ является рекуррентной функцией

$$\Omega_{i+1} = f(\Omega_i);$$

Ω_i - элементы рекуррентной последовательности

f – функция преобразования

$\Omega_0 = S$ - синхропосылка (начальное заполнение)

$$\Omega_0 = Ц_{32-3}(\Omega_0)$$

Таким образом, последовательность элементов гаммы для использования в режиме гаммирования однозначно определяется ключевыми данными и синхропосылками. Для обратимости процедуры шифрования в шифровании/дешифровании должна использоваться одна и та же синхропосылка. Это приводит к необходимости хранить или передавать синхропосылку по каналам связи вместе с зашифрованными данными. Либо можно создать алгоритм ее выработки.

Требования к РГПЧ:

1) Период повторения последовательности чисел, вырабатываемый РГПЧ, не должен сильно отличаться от максимально возможного при заданном размере блока значения 2^{64}.

2) Соседние значения, вырабатываемые РГПЧ должны отличаться друг от друга в каждом байте, иначе задача криптоаналитика будет упрощена.

3) РГПЧ должен быть достаточно просто реализуем как аппаратно, так и программно на наиболее распространенных типах процессоров.

Характеристики РГПЧ:

1) В 64-битовом блоке старшая и младшая части вырабатываются независимо друг от друга.

$$\Omega_i = (\Omega_i^0, \Omega_i^1)$$

$$|\Omega_i^0| = |\Omega_i^1| = 32$$

$$\Omega_{i+1}^0 = \hat{f}(\Omega_i^0)$$

$$\Omega_{i+1}^1 = \hat{f}\left(\Omega_i^1\right)$$

Т.е. фактически существует два различных РГПЧ для старшей и младшей половины блока.

2) Рекуррентные соотношения для старшей и младшей частей имеют вид:

$$\Omega_{i+1}^0 = \left(\Omega_i^0 + C_1\right) \bmod 2^{32}$$

$$C_1 = 1010101_{16}$$

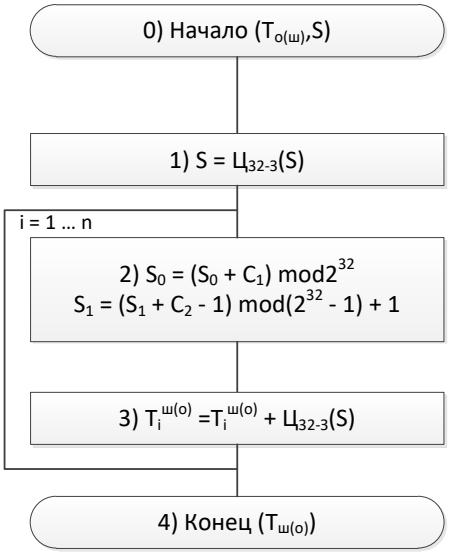
$$\Omega_{i+1}^1 = \left(\Omega_i^1 + C_2 - 1\right) \bmod \left(2^{32} - 1\right) + 1$$

$$C_2 = 1010104_{16}$$

Константы, используемые на данном шаге, записаны в 16-разрядной системе счисления.

3) Период повторения последовательности для младшей части составляет 2^{32}, для старшей - $2^{32} - 1$. Для всей последовательности - $2^{32}\left(2^{32} - 1\right).$

Алгоритм зашифрования в режиме гаммирования:



Шаг 0. Определяет исходные данные для основного шага криптопреобразования. $T_{O(Ш)}$ - массив открытых (зашифрованных) данных произвольного размера, подвергаемый процедуре зашифрования/расшифрования. По ходу преобразований массив подвергается преобразованиям порциями по 64 бита. 64-битовые элементы необходимы для генерации гаммы.

Шаг 1. Начальное преобразование синхропосылки. Выполняется для рандомизации, т.е. удаления статистических закономерностей. Результат – начальное заполнение РГПЧ.

Шаг 2. Один из шагов работы РГПЧ, реализующий его рекуррентный алгоритм. В ходе данного шага старшая часть S_1 и младшая S_0 вырабатываются независимо друг от друга.

Шаг 3. Гаммирование. Очередной 64-битовый элемент, выработанный РГПЧ, подвергается процедуре зашифрования по циклу 32-З. Результат используется как элемент гаммы для зашифрования/расшифрования очередного блока открытых зашифрованных данных того же размера.

Шаг 4. Результат работы алгоритма: зашифрованные/расшифрованные данные.

Особенности режима гаммирования:

1) Одинаковые блоки в исходном массиве дадут различные блоки шифротекста, что позволит скрыть факт их идентичности.

2) Т.к. наложение гаммы выполняется побитно, шифрование неполного блока данных легко выполнимо как шифрование битов этого неполного блока, для чего используются соответствующие биты блока гаммы.

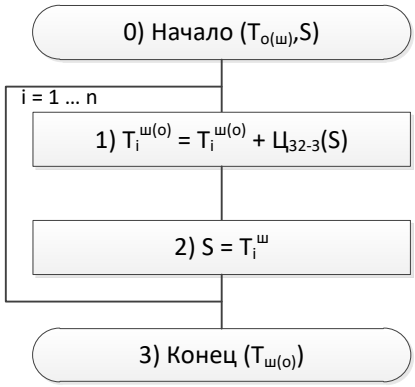
3) Синхропосылка, используемая при шифровании каким-то образом должна быть передана для расшифрования. Существует два варианта: хранить и передавать синхропосылку с зашифрованными данными, что приводит к увеличению на 8 байт. Или использовать предопределенное значение. Наиболее распространен первый способ.

4) Биты массива данных шифруются независимо друг от друга, таким образом, каждый бит шифротекста зависит от соответствующих битов открытого текста и их порядкового номера в массиве. Т.е., изменение бита шифротекста приведет к аналогичному изменению открытого текста, что позволяет рассматривать данное свойство как недостаток.

Гаммирование с обратной связью

Режим похож на режим гаммирования, отличается способом выработки гаммы: очередной элемент гаммы вырабатывается как результат преобразования по Ц32-З предыдущего блока зашифрованных данных, а для зашифрования первого блока массива данных элемент гаммы вырабатывается как результат преобразования по тому же циклу синхропосылки. Этим достигается зацепление блоков – каждый блок шифротекста зависит от соответствующего и предыдущего блока открытого текста, поэтому данный режим также называется гаммированием с зацеплением блоков.

Шифрование в режиме гаммирования с обратной связью обладает такими же особенностями, что и шифрование в режиме обычного гаммирования, за исключением наложения шифротекста на соответствующий открытый текст.



3. Асимметричные криптосистемы.

ассиметричные (двухключевые) криптосистемы (с открытым ключом).

Плюсы:

решена проблема распоряжения ключей между пользователями;

исчезает квадратичная зависимость числа ключей от числа пользователей;

позволяют реализовать протоколы взаимосвязи сторон, которые не доверяют друг другу.

Минусы:

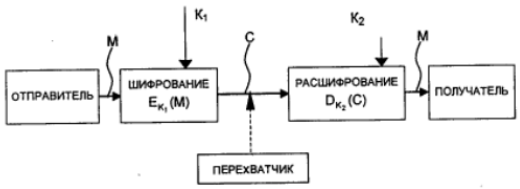
на настоящий момент нет математического док-ва необратимости используемых в алгоритмах функций;

существенно медленнее симметричных;

ресурсоемкое;

необходимость защиты открытых ключей от подмены.

Обобщенная схема асимметричных криптосистем с открытым ключом:



Открытый ключ – используется для шифрования инфы, вычисляется из секретного ключа (передается).

Секретный ключ – используется для расшифрования информации, зашифрованной с помощью парного ему открытого ключа (он не передается по каналу, находится у автора).

Алгоритм асимметричного шифрования:

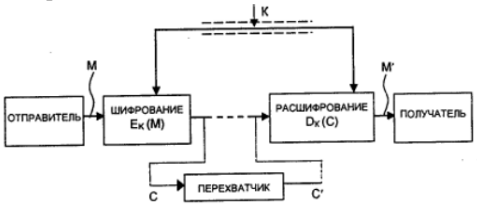
каждый пользователь генерирует пару ключей (открытый и секретный);

открытый ключ публикуется, секретный остается в личном пользовании;

пользователь А шифрует сообщение, используя открытый ключ и отправляет его пользователю В;

пользователь В дешифрует сообщение с помощью своего секретного ключа.

Поток информации в криптосистеме при активном перехвате сообщений:



Любая попытка со стороны перехватчика расшифровать шифротекст С для получения открытого текста М или зашифровать свой

собственный текст M' для получения правдоподобного шифротекста C', не имея подлинного ключа называется криптоаналитической атакой.

Если предпринятые криптоаналитические атаки не достигают поставленной цели и криптоаналитик не может, не имея подлинного ключа, вывести исходный текст M из шифротекста C или наоборот (C' из M'), полагают, что такая криптосистема является криптостойкой.

Фундаментальные принципы криптоанализа (Кирхгоф):

Весь алгоритм шифрования, кроме значения секретного ключа, известен криптоаналитику противника.

Криптоаналитик имеет в своем распоряжении шифротексты сообщений.

Типы криптоаналитических атак:

основные

при наличии только известного шифротекста;
при наличии известного открытого шифротекста;
при возможности выбора открытого текста;
с адаптивным выбором открытого текста.

дополнительные

с использованием выбранного шифротекста;
методом полного перебора всех возможных ключей.

Основные направления использования криптографических методов:
передача конфиденциальной информации по каналам связи (электронная почта);
установление подлинности передаваемых сообщений;
хранение информации (документов, БД) на носителях в зашифрованном виде.

. Схема шифрования RSA.

Р. Райвест, А. Шамир и А. Адлеман. Алгоритм RSA стал первым полноценным алгоритмом с открытым ключом, который может работать как в режиме шифрования данных, так и в режиме электронной цифровой подписи.

Надежность алгоритма основывается на трудности факторизации больших чисел и трудности вычисления дискретных логарифмов.

В криптосистеме RSA открытый ключ K_B, секретный ключ k_B, сообщение M и криптограмма C принадлежат множеству целых чисел

$$Z_N = \{0,1,2,\ldots,N-1\}, \quad (5)$$

где N – модуль: $N = P \cdot Q.$ (6)

Здесь P и Q – случайные большие простые числа. Для обеспечения максимальной безопасности выбирают P и Q равной длины и хранят их в секрете.

Множество Z_N с операцией сложения и умножения по модулю N образуют арифметику по модулю N.

Открытый ключ K_B выбирают случайным образом так, чтобы выполнялись условия:

$$1 < K_B \le \varphi(N), \quad НОД(K_B, \varphi(N)) = 1, \tag{7}$$

$$\varphi(N) = (P-1)(Q-1), \tag{8}$$

где $\varphi(N)$ - функция Эйлера.

Функция Эйлера $\varphi(N)$ указывает количество положительных целых чисел в интервале от 1 до N, которые взаимно просты с N.

Второе из указанных выше условий означает, что открытый ключ K_B и функция Эйлера $\varphi(N)$ должны быть взаимно простыми.

Далее, используя расширенный алгоритм Евклида, вычисляют секретный ключ k_B, такой, что

$$k_B \cdot K_B \equiv 1 \bmod \varphi(N) \tag{9}$$

или

$$k_B = K_B^{-1} \bmod((P-1)(Q-1)).$$

Это можно осуществить, т.к. получатель B знает пару простых чисел (P,Q) и может легко найти $\varphi(N)$. Заметим, что k_B и N должны быть взаимно простыми.

Открытый ключ K_B используют для шифрования данных, а секретный ключ k_B - для расшифрования.

Преобразование шифрования определяет криптограмму C через пару (открытый ключ K_B, сообщение M) в соответствии со следующей формулой:

$$C = E_{K_B}(M) = E_B(M) = M^{K_B} \bmod N. \tag{10}$$

В качестве алгоритма быстрого вычисления значения C используют ряд последовательных возведений в квадрат целого M и умножений на M с приведением по модулю N.

Обращение функции $C = M^{K_B} \bmod N$, т.е. определение значения M по известным значениям C, K_B и N, практически неосуществимо при $N \approx 2^{512}$.

Однако обратную задачу, т.е. задачу расшифрования криптограммы C, можно решить, используя пару (секретный ключ k_B, криптограмма C) по следующей формуле:

$$M = D_{k_B}(C) = D_B(C) = C^{k_B} \bmod N. \tag{11}$$

Процесс расшифрования можно записать так:

$$D_B\left(E_B\left(M\right)\right)=M. \qquad (12)$$

Подставляя в (12) значения (10) и (11), получаем:

$$D_B\left(M^{K_B} \bmod N\right)=M$$

$$\left(M^{K_B} \bmod N\right)^{k_B} \bmod N = M$$

$$\left(M^{K_B}\right)^{k_B} = M \bmod N \qquad \text{или}$$

$$M^{K_B k_B} = M \bmod N. \qquad (13)$$

Величина $\varphi\left(N\right)$ играет важную роль в теореме Эйлера, которая утверждает, что если $НОД\left(x,N\right)=1$, то

$$x^{\varphi(N)} \equiv 1 \bmod N,$$

или в несколько более общей форме

$$x^{n\cdot\varphi(N)+1} \equiv x \bmod N. \qquad (14)$$

Сопоставляя выражения (13) и (14), получаем

$$K_B \cdot k_B = n\cdot\varphi\left(N\right)+1$$

или, что то же самое,

$$K_B \cdot k_B \equiv 1 \bmod \varphi\left(N\right).$$

Именно поэтому для вычисления секретного ключа k_B используют соотношение (9).

Таким образом, если криптограмму

$$C = M^{K_B} \bmod N$$

возвести в степень k_B , то в результате восстанавливается исходный открытый текст M, т.к.

$$\left(M^{K_B}\right)^{k_B} = M^{K_B k_B} = M^{n\cdot\varphi(N)+1} \equiv M \bmod N.$$

Таким образом, получатель B, который создает криптосистему, защищает два параметра:

1) Секретный ключ k_B .

2) Пару чисел $\left(P,Q\right)$, произведение которых дает значение модуля N.

С другой стороны, получатель B открывает значение модуля N и открытый ключ K_B .

Противнику известны лишь значения K_B и N. Если бы он смог разложить N на множители P и Q, то он узнал бы "потайной ход" – тройку чисел $\left\{P,Q,K_B\right\}$, вычислил значение функции Эйлера

$$\varphi\left(N\right)=\left(P-1\right)\left(Q-1\right)$$

и определил значение секретного ключа k_B .

Однако, как уже отмечалось, разложение очень большого N на множители вычислительно не осуществимо (при условии, что длины выбранных P и Q составляют не менее 100 десятичных знаков).

Процедуры шифрования и расшифрования в криптосистеме RSA

Предположим, что пользователь A хочет передать пользователю B сообщение в зашифрованном виде, используя криптосистему RSA. В таком случае пользователь A выступает в роли отправителя сообщения, а пользователь B – в роли получателя. Как отмечалось выше, криптосистему RSA должен сформировать получатель сообщения, т.е. пользователь B. Рассмотрим последовательность действий пользователя B и пользователя A.

Шаг 1. Пользователь B выбирает два произвольных больших простых числа P и Q.

Шаг 2. Пользователь B вычисляет значения модуля $N = P \cdot Q$.

Шаг 3. Пользователь B вычисляет функцию Эйлера

$$\varphi(N) = (P-1)(Q-1)$$

и выбирает случайным образом значения открытого ключа K_B с учетом выполнения условий:

$$1 < K_B \le \varphi(N), \quad НОД(K_B, \varphi(N)) = 1.$$

Шаг 4. Пользователь B вычисляет значение секретного ключа k_B, используя расширенный алгоритм Евклида при решении сравнения

$$k_B = K_B^{-1} \bmod \varphi(N).$$

Шаг 5. Пользователь B пересылает пользователю A пару чисел (N, K_B) по незащищенному каналу.

Если пользователь A хочет передать пользователю B сообщение M, он выполняет шаг 6.

Шаг 6. Пользователь A разбивает исходный открытый текст M на блоки, каждый из которых может быть представлен в виде числа

$$M_i = 0,1,2,\ldots,N-1.$$

Шаг 7. Пользователь A шифрует текст, представленный в виде последовательности чисел M_i по формуле

$$C_i = M_i^{K_B} \bmod N$$

и отправляет криптограмму

$$C_1, C_2, C_3, \ldots, C_i, \ldots$$

пользователю B.

Шаг 8. Пользователь B расшифровывает принятую криптограмму

$$C_1, C_2, C_3, \ldots, C_i, \ldots,$$

используя секретный ключ k_B по формуле

$$M_i = C_i^{k_B} \bmod N.$$

В результате будет получена последовательность чисел M_i, которые представляют собой исходное сообщение M. Чтобы алгоритм RSA имел практическую ценность, необходимо иметь возможность без существенных затрат генерировать большие простые числа, уметь оперативно вычислять значения K_B и k_B.

Пример. Шифрование сообщения CAB. Для простоты вычислений будут использоваться небольшие числа. На практике применяются очень большие числа.

Действия пользователя B.

1. Выбирает $P = 3$ и $Q = 11$.

2. Вычисляет модуль $N = P \cdot Q = 3 \cdot 11 = 33$.

3. Вычисляет значение функции Эйлера для $N = 33$:

$$\varphi(N) = (P-1)(Q-1),$$
$$\varphi(33) = 2 \cdot 10 = 20.$$

Выбирает в качестве открытого ключа K_B произвольное число с учетом выполнения условий:

$$1 < K_B \le \varphi(N), \quad НОД(K_B, \varphi(N)) = 1,$$

$$1 < K_B \le \varphi(33), \quad НОД(K_B, \varphi(33)) = 1,$$

$$1 < K_B \le 20, \quad НОД(K_B, 20) = 1.$$

Пусть $K_B = 7$.

4. Вычисляет значение секретного ключа k_B, используя расширенный алгоритм Евклида при решении сравнения

$$k_B = K_B^{-1} \bmod \varphi(N),$$
$$k_B = 7^{-1} \bmod 20.$$

q	u_1	u_2	u_3	v_1	v_2	v_3
-	0	1	n=20	1	0	a=7
2	1	0	7	-2	1	6
1	-2	1	6	3	-1	1
6	3	-1	1	-20	7	0

Итерация 1:

1) $(u_1, u_2, u_3) := (0,1,20), (v_1, v_2, v_3) := (1,0,7)$

2) $u_3 \neq 1$

3) $q = [u_3 / v_3] = [20/7] = 2$

$(t_1,t_2,t_3)=(u_1,u_2,u_3)-(v_1,v_2,v_3)\cdot q=(0,1,20)-(1,0,7)\cdot 2=(0,1,20)-(2,0,14)=(-2,1,6),$
$(u_1,u_2,u_3)=(v_1,v_2,v_3)=(1,0,7),$
$(v_1,v_2,v_3)=(t_1,t_2,t_3)=(-2,1,6).$

Итерация 2:

2) $u_3\neq 1$

3) $q=[u_3/v_3]=[7/6]=1$

$(t_1,t_2,t_3)=(u_1,u_2,u_3)-(v_1,v_2,v_3)\cdot q=(1,0,7)-(-2,1,6)\cdot 1=(1,0,7)-(-2,1,6)=(3,-1,1),$
$(u_1,u_2,u_3)=(v_1,v_2,v_3)=(-2,1,6),$
$(v_1,v_2,v_3)=(t_1,t_2,t_3)=(3,-1,1).$

Итерация 3:

2) $u_3\neq 1$

3) $q=[u_3/v_3]=[6/1]=6$

$(t_1,t_2,t_3)=(u_1,u_2,u_3)-(v_1,v_2,v_3)\cdot q=(-2,1,6)-(3,-1,1)\cdot 6=(-2,1,6)-(18,-6,6)=(-20,7,0),$
$(u_1,u_2,u_3)=(v_1,v_2,v_3)=(3,-1,1),$
$(v_1,v_2,v_3)=(t_1,t_2,t_3)=(-20,7,0).$

Итерация 4:

2) $u_3=1$

При $u_1=3, u_2=-1, u_3=1$

$(a\cdot u_1+n\cdot u_2)\bmod n=(7\cdot 3+20\cdot(-1))\bmod 20=(21-20)\bmod 20=1\equiv$
$\equiv(a\cdot u_1)\bmod n=(7\cdot 3)\bmod 20=21\bmod 20=1\equiv 1,$
$a^{-1}\bmod n=7^{-1}\bmod 20\equiv u_1\bmod n=3\bmod 20=3.$

Решение дает $k_B=3$.

5. Пересылает пользователю А пару чисел $(N,K_B)=(33,7)$.

Действия пользователя А.

6. Представляет шифруемое сообщение как последовательность целых чисел в диапазоне 0…32. Пусть буква А представляется как число 1, буква В – как число 2, буква С – как число 3. Тогда сообщение САВ можно представить как последовательность чисел 312, т.е. $M_1=3, M_2=1, M_3=2$.

7. Шифрует текст, представленный в виде последовательности чисел M_1, M_2 и M_3, используя ключ $K_B=7$ и $N=33$, по формуле

$$C_i=M_i^{K_B}\bmod N.$$

Получает

$C_1=M_1^7\bmod 33=3^7\bmod 33=2187\bmod 33=9,$

$C_2=M_2^7\bmod 33=1^7\bmod 33=1\bmod 33=1,$

$C_3=M_3^7\bmod 33=2^7\bmod 33=128\bmod 33=29.$

Отправляет пользователю В криптограмму

$$C_1,C_2,C_3=9,1,29.$$

Действия пользователя И.

8. Расшифровывает принятую криптограмму C_1, C_2, C_3, используя секретный ключ $k_B = 3$, по формуле

$$M_i = C_i^{k_B} \bmod N.$$

Получает

$$M_1 = C_1^3 \bmod 33 = 9^3 \bmod 33 = 729 \bmod 33 = 3,$$

$$M_2 = C_2^3 \bmod 33 = 1^3 \bmod 33 = 1 \bmod 33 = 1,$$

$$M_3 = C_3^3 \bmod 33 = 29^3 \bmod 33 = 24389 \bmod 33 = 2.$$

Таким образом, восстановлено исходное сообщение: CAB.

. Схема шифрования Эль-Гамаля.

Схема Эль Гамаля, предложенная в 1985 г., может быть использована как для шифрования, так и для цифровых подписей. Безопасность схемы Эль Гамаля обусловлена сложностью вычисления дискретных логарифмов в конечном поле.

Для того, чтобы генерировать пару ключей (открытый ключ – секретный ключ), сначала выбирают некоторое большое простое число P и большое целое число G, причем $G < P$. Числа P и G могут быть распространены среди группы пользователей.

Затем выбирают случайное целое число X, причем $X < P$. Число X является секретным ключом и должно храниться в секрете.

Далее вычисляют $Y = G^X \bmod P$. Число Y является открытым ключом.

Для того чтобы зашифровать сообщение M, выбирают случайное целое число K, $1 < K < P - 1$, такое, что числа K и $(P-1)$ являются взаимно простыми.

Затем вычисляют числа

$$a = G^K \bmod P,$$

$$b = Y^K M \bmod P.$$

Пара чисел (a, b) является шифротекстом. Заметим, что длина шифротекста вдвое больше длины исходного открытого текста M.

Для того чтобы расшифровать шифротекст (a, b), вычисляют

$$M = \frac{b}{a^X} \bmod P.$$

(*)

Поскольку

$$a^X \equiv G^{KX} \bmod P,$$

$$\frac{b}{a^X} \equiv \frac{Y^K M}{a^X} \equiv \frac{G^{KX} M}{G^{KX}} \equiv M \bmod P,$$

то соотношение (*) справедливо.

Пример. Выберем $P = 11$, $G = 2$, секретный ключ $X = 8$.

Вычисляем

$$Y = G^X \bmod P = 2^8 \bmod 11 = 256 \bmod 11 = 3.$$

Итак, открытый ключ $Y = 3.$

Пусть сообщение $M = 5$. Выберем некоторое случайное число $K = 9$. Убедимся, что $НОД(K, P-1) = 1$. Действительно, $НОД(9,10) = 1$. Вычисляем пару чисел a и b:

$$a = G^K \bmod P = 2^9 \bmod 11 = 512 \bmod 11 = 6,$$

$$b = Y^K M \bmod P = 3^9 \cdot 5 \bmod 11 = 98415 \bmod 11 = 9.$$

Получим шифротекст $(a,b) = (6.9)$.

Выполним расшифрование этого шифротекста. Вычисляем сообщение M, используя секретный ключ X:

$$M = \frac{b}{a^X} \bmod P = \frac{9}{6^8} \bmod 11.$$

Выражение $M = \frac{9}{6^8} \bmod 11$ можно представить в виде

$$6^8 \cdot M \equiv 9 \bmod 11$$

или

$$1679616 \cdot M \equiv 9 \bmod 11.$$

Решая данное сравнение, находим $M = 5$.

В реальных схемах шифрования необходимо использовать в качестве модуля P большое целое простое число, имеющее в двоичном представлении длину 512…1024 бит.