Министерство образования республики Беларусь

Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ»

**Институт информационных технологий**

Специальность «Инженерно-психологическое обеспечение информационных технологий»

**КОНТРОЛЬНАЯ РАБОТА**

По курсу «Криптографические технологии»

Вариант 2

«Роль криптографических протоколов в системах защиты информации»

Студентки 3 курса 680971 группы

заочного отделения

Барковской Ольги Вячеславовны

Зачетная книжка № 68097002

тел. +375(29) 141-14-74

:

Минск 2019

Криптографический протокол (КП), называемый также просто протоколом это распределённый алгоритм, определяющий порядок обмена сообщениями между несколькими агентами, в качестве которых могут выступать, например, люди, компьютерные программы, вычислительные комплексы, базы данных, сети связи, банковские карточки, и т.д. Агенты, принимающие участие в работе протокола, называются участниками этого протокола.

* Действия, выполняемые каждым из участников протокола, могут иметьследующий вид:
* посылка сообщения другому участнику этого протокола (или группе участников),
* приём сообщения от другого участника,
* внутренние действия, к числу которых относятся:
  + выполнение участником некоторых вычислений,
  + проверка логических условий, и
  + обновление значений переменных.

Криптографические протоколы предназначены для обеспечения безопасности передачи, обработки и хранения информации в небезопасной среде. Свойства безопасности, которые должен обеспечивать протокол, могут иметь, например, следующий вид:

* целостность передаваемых сообщений, которая заключается в том,  
  что всякое изменение сообщений в процессе их передачи будет обнаружено в ходе выполнения протокола,
* секретность передаваемых сообщений, которая заключается в отсутствии неавторизованной утечки информации в процессе работы  
  протокола.

Нарушения свойств безопасности в процессе работы КП могут происходить по причине противодействия со стороны агентов, называемых противниками.

Противники подразделяются на следующие два класса:

* пассивные противники, они могут перехватывать сообщения, пересылаемые участниками КП, и анализировать их,
* активные противники, они могут делать то же, что и пассивные противники, а также
  + модифицировать или удалять перехваченные сообщения,
  + генерировать новые сообщения и посылать их участникам КП,
  + выдавать себя за участников КП.

Кроме того, нарушения свойств безопасности КП возможны из-за действий участников КП, которые могут нарушать (умышленно или неумышленно) предписанные протоколом правила взаимодействия с другими участниками этого КП.

Возможность нарушения свойств безопасности в процессе работы КП называют уязвимостями этого КП.

При решении задач анализа уязвимостей КП используются следующие предположения о противнике:

* противник полностью знает КП,
* противнику доступны все сообщения, пересылаемые между участниками КП, он может их модифицировать, удалять, и заменять своими сообщениями,
* противник не может извлечь из перехваченных ШТ соответствующие ОТ, если он не знает необходимых ключей.

Разновидности атак на протоколы:

* Атаки, направленные против криптографических алгоритмов
* Атаки против криптографических методов, применяемых для реализации протоколов
* Атаки против самих протоколов (активные или пассивные)

Известные атаки на криптографические протоколы:

1. Подмена (impersonation) — попытка подменить одного пользователя другим. Нарушитель, выступая от имени одной из сторон и полностью имитируя ее действия, получает в ответ сообщения определенного формата, необходимые для подделки отдельных шагов протокола. Методы противодействия состоят в: — сохранении в тайне от противника информации, определяющей алгоритм идентификации; — использование различных форматов сообщений, передаваемых на разных шагах протокола; — вставка в них специальных идентификационных меток и номеров сообщений. В протоколах с использованием третьей стороны возможны атаки, основанные на подмене доверенного сервера. Например, одна из сторон, имеющая доверительные отношения с сервером, выступает от его имени, подменяет его трафик обмена с другими сторонами и в результате получает возможность раскрывать значения генерируемых центром ключей. Эта атака может быть успешной для протоколов, в которых аутентификация при доступе к серверу основана только на идентификаторах сторон и случайных числах, генерируемых при каждом взаимодействии. Для защиты от таких атак применяют средства привязки ключей не к одной, а к обеим взаимодействующим сторонам путем передачи обоих идентификаторов в зашифрованном виде.
2. Повторное навязывание сообщения (replay attack) — повторное использование ранее переданного в текущем или предыдущем сеансе сообщения или какой-либо его части в текущем сеансе протокола. Например, повторная передача информации ранее проведенного протокола идентификации может привести к повторной успешной идентификации того же самого или другого пользователя. В протоколах передачи ключей данная атака часто применяется для повторного навязывания уже использованного ранее сеансового ключа — атака на основе новизны (freshness attack). Методы противодействия состоят в обеспечении целостности сеанса и невозможности вставки в него лишних сообщений. Для этого используется: — техника типа «запрос — ответ»; — вставка в передаваемые сообщения временных меток, случайных чисел или возрастающих последовательностей чисел.
3. Еще один тип подобных атак связан с обратной передачей адресату ранее переданных им сообщений и получил название атака отражением (reflection attack). Часто атаки данного типа относят к классу атак с повторным навязыванием сообщения. Для защиты от таких атак протоколы специально делают несимметричными, включая в зашифрованные сообщения идентификаторы сторон либо изменяя процедуры так, чтобы стороны должны были выполнять разные действия, вводят в протокол идентификационную информацию, используют различные ключи для приема и передачи сообщений.
4. Задержка передачи сообщения (forced delay) — перехват противником сообщения и навязывание его в более поздний момент времени. Это также разновидность атаки с повторным навязыванием сообщения. Методы противодействия включают использование случайных чисел совместно с ограничением временного промежутка для ответа, использование временных меток.
5. Комбинированная атака (interleaving attack) — подмена или другой метод обмана, использующий комбинацию данных из ранее выполненных протоколов, в том числе протоколов, ранее навязанных противником. Метод противодействия состоит в обеспечении целостности сеансов протоколов и отдельных сообщений.
6. Специальный частный случай предыдущей атаки, в котором противник специально открывает одновременно несколько параллельных сеансов с целью использования сообщений из одного сеанса

Симметричные системы шифрования (СШ) в основном относятся к следующим двум классам: блочные и поточные.

Блочные системы шифрования

В блочных СШ открытый текст перед шифрованием разбивается на блоки, и каждый блок шифруется при помощи одного и того же алгоритма.

Шифрующие преобразования блоков заключаются в суперпозиции нескольких простых отображений, называемых базовыми преобразованиями.

Среди базовых преобразований блоков наибольшее распространение получили преобразования Фейстеля.

Алгоритм шифрования реализуется несколькими итерациями преобразования Фейстеля, при этом очередная итерация использует в качестве входного блока результат предыдущей итерации.

Для дешифрования применяется обратное преобразование, которое вычисляется по той же схеме, как и исходное:

Поточные системы шифрования.

В поточных СШ шифрование заключается в сложении по модулю 2 каждого бита открытого текста с соответствующим битом псевдослучайной последовательности, называемой гаммой. Дешифрование осуществляется по той же схеме, как и шифрование.

Для порождения гаммы используются регистры сдвига с линейной обратной связью (называемые ниже просто регистрами).

Гамма, порождаемая регистром, представляет собой последовательность его выходных сигналов (которые он выдает в моменты 0, 1, и т.д.).

Для шифрования или дешифрования при помощи регистра его начальное состояние полагается равным ключу.

Существуют и другие способы порождения гаммы:

1. один из них заключается в использовании двух регистров: если гаммы, порожденные ими, имеют вид a0, a1, . . . и b0, b1, . . . соответственно, то результирующая гамма получается из гаммы a0, a1,... удалением еј компонентов с такими номерами i, что bi = 0,

2. другой способ заключается в том, что вместо регистров используются автономные автоматы с состояниями из Rn (где R конечное кольцо, элементы Rn рассматриваются как вектор-столбцы длины n над R), отображение переходов которых переводит состояние q � Rn в состояние Aq + b, где A матрица порядка n над R, b � Rn

Асимметричные системы шифрования

Каждая асимметричная СШ предполагает использование пары ключей, связанной с каким-либо агентом, причем

* ключ для шифрования известен всем агентам, и
* ключ для дешифрования должен быть известен только тому агенту,с которым он связан.

Система шифрования RSA

Название системы шифрования RSA является аббревиатурой, связанной с фамилиями её создателей (Rivest, Shamir и Adleman). Криптографическая стойкость данной СШ (т.е. сложность нахождения по ШТ соответствующих им ОТ без знания ключа дешифрования) основывается на вычислительной сложности задачи разложения на множители больших целых чисел.

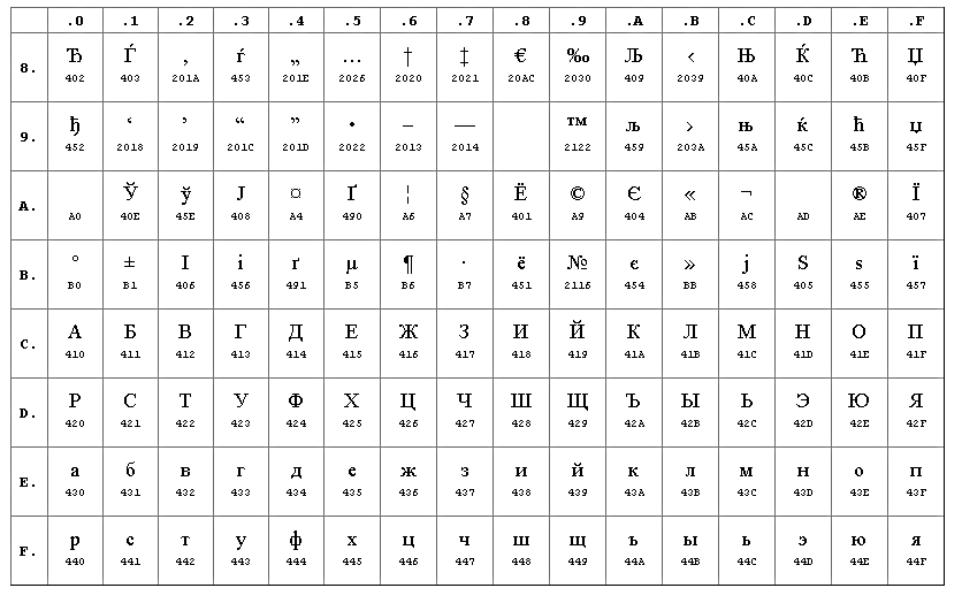
Для шифрования ОТ разбивается на блоки, каждый из которых можно рассматривать как двоичную запись числа из Zn. Каждый из этих блоков шифруется отдельно.

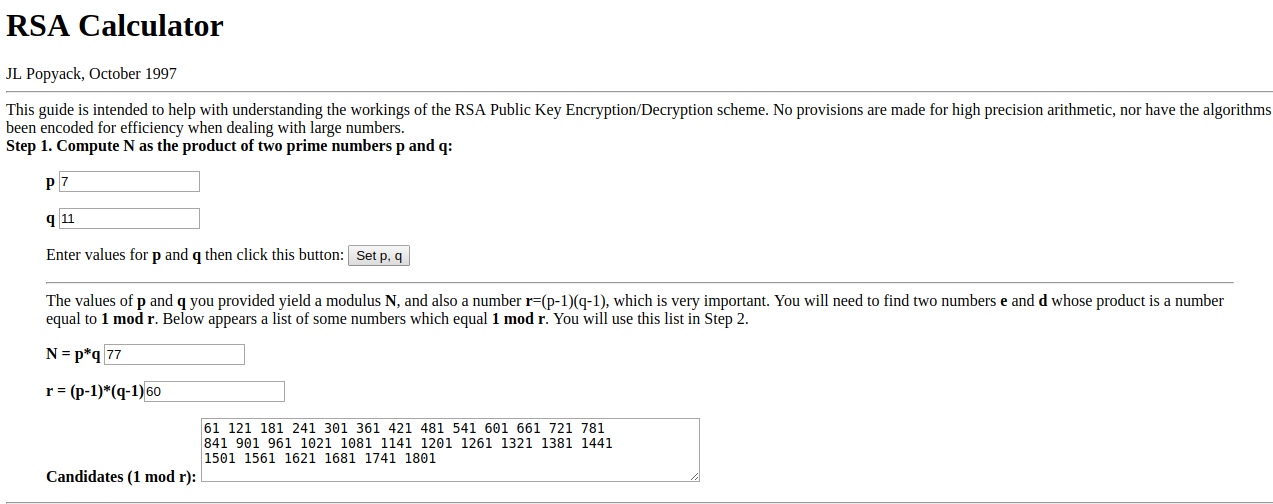
Система шифрования Эль-Гамаля

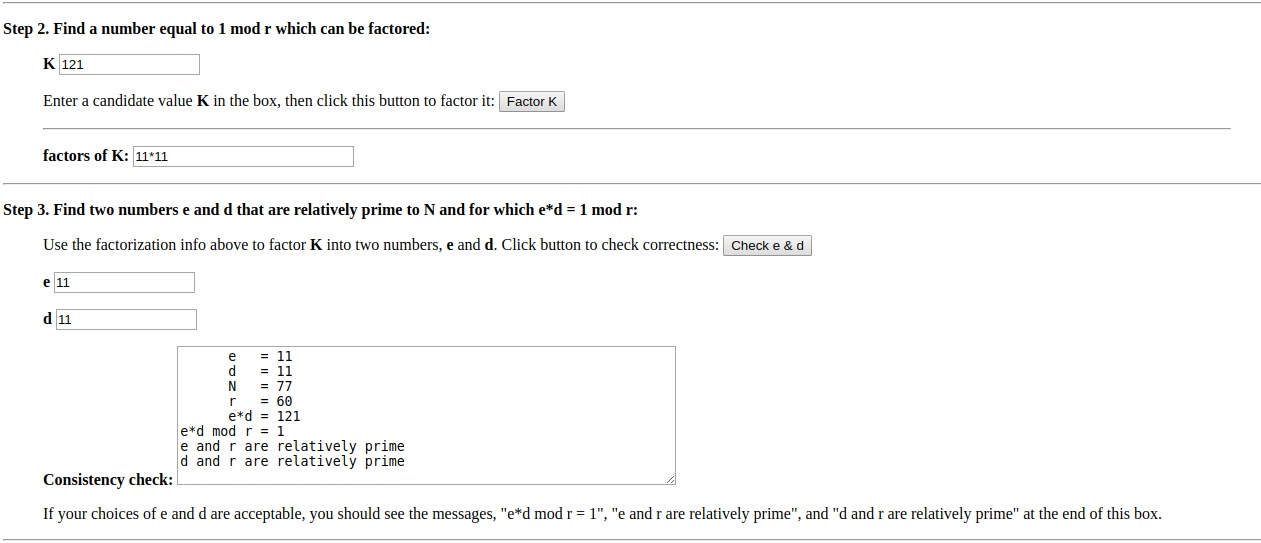
Другим примером АСШ является СШ Эль-Гамаля, еј криптографическая стойкость основывается на вычислительной сложности задачи дискретного логарифмирования.

Для шифрования ОТ разбивается на блоки, каждый из которых можно рассматривать как двоичную запись числа из Zp. Каждый из этих блоков шифруется отдельно.

**Задание 1**







Ответ: 33204743441574201121

**Задание 2**

барковск - жесмзацм

# СПИСОК ЛИТЕРАТУРЫ

1. Словарь по кибернетике / Под редакцией академика В. С. Михалевича. — 2-е. — Киев: Главная редакция Украинской Советской Энциклопедии имени М. П. Бажана, 1989. — 751 с. — (С48). — 50 000 экз. — ISBN 5-88500-008-5.
2. RS/6000 SP: Practical MPI Programming. — IBM RedBook, 1999. — 238 с. Архивировано 19 января 2008 года. (англ.)
3. Воеводин В. В., Воеводин Вл. В. Параллельные вычисления. — СПб: БХВ-Петербург, 2002. — 608 с. — ISBN 5-94157-160-7.
4. Оленев Н. Н. Основы параллельного программирования в системе MPI. — М.: ВЦ РАН, 2005. — 80 с. — ISBN 5201098320