**Лабораторная работ № 10**

**Электронная цифровая подпись.**

**Цель работы**

Ознакомиться со схемами цифровой подписи и получить навыки создания и проверки подлинности ЦП.

**Указание к работе**

На протяжении многих веков при ведении деловой переписки, заключении контрактов и оформлении любых других важных бумаг подпись ответственного лица или исполнителя была непременным условием признания его статуса или неоспоримым свидетельством его важности. Подобный акт преследовал две цели:

* гарантирование истинности письма путем сличения подписи с имеющимся образцом;
* гарантирование авторства документа (с юридической точки зрения).

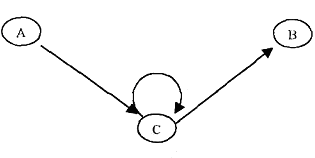
Выполнение данных требований основывается на следующих свойствах подписи:

* подпись аутентична, то есть с ее помощью получателю документа можно доказать, что она принадлежит подписывающему;
* подпись служит доказательством, что только тот человек, чей автограф стоит на документе, мог подписать данный документ, и никто другой не смог бы этого сделать;
* подпись непереносима, то есть является частью документа и поэтому перенести ее на другой документ невозможно:
* документ с подписью является неизменяемым, то есть после подписания его невозможно изменить, оставив данный факт незамеченным;
* подпись неоспорима, то есть человек, подписавший документ, в случае признания экспертизой, что именно он засвидетельствовал данный документ, не может оспорить факт подписания;
* любое лицо, имеющее образец подписи, может удостовериться в том, что данный документ подписан владельцем подписи.

С переходом к безбумажным способам передачи и хранения данных, а также с развитием систем электронного перевода денежных средств, в основе которых – электронный аналог бумажного платежного поручения, проблема виртуального подтверждения аутентичности документа приобрела особую остроту. Развитие любых подобных систем теперь немыслимо без существования электронных подписей под электронными документами. Однако применение и широкое распространение *электронно-цифровых подписей* (ЭЦП) повлекло целый ряд правовых проблем. Так, ЭЦП может применяться на основе договоренностей внутри какой-либо группы пользователей системы передачи данных, и в соответствии с договоренностью внутри данной группы ЭЦП должно иметь юридическую силу. Но будет ли электронная подпись иметь доказательную силу в суде, например, при оспаривании факта передачи платежного поручения?

**Схема 1**

Данная схема предполагает шифрование электронного документа (ЭД) на основе симметричных алгоритмов и предусматривает наличие в системе третьего лица (арбитра), пользующегося доверием участников обмена подписанными подобным образом электронными документами. Взаимодействие пользователей данной системой производится по следующей схеме:



***Рис. 1. Основные методы построения схем ЭЦП. Схема 1.***

Участник A зашифровывает сообщение своим секретном ключе KA, знание которого разделено с арбитром (С на рис. 1), затем шифрованное сообщение передается арбитру с указанием адресата данного сообщения (информация, идентифицирующая адресата, передается также в зашифрованном виде).

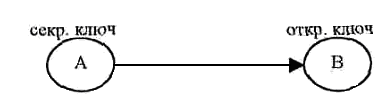
Арбитр расшифровывает полученное сообщение ключом КА, производит необходимые проверки и затем зашифровывает его секретным ключом участника B (KB). Далее зашифрованное сообщение посылается участнику B вместе с информацией, что оно пришло от участника A.

Участник B расшифровывает данное сообщение и убеждается в том, что отправителем является участник A.

Авторизацией документа в данной схеме считается сам факт шифрования электронного документа (ЭД) секретным ключом и передача зашифрованного ЭД арбитру. Основным преимуществом этой схемы является наличие третьей стороны, исключающей какие-либо спорные вопросы между участниками информационного обмена, то есть в данном случае не требуется дополнительной системы арбитража ЭЦП. Недостатком схемы является так же наличие третьей стороны и использование симметричных алгоритмов шифрования. На практике эта схема не получила широкого распространения.

**Схема 2**

Фактом подписания документа в данной схеме является шифрование документа секретным ключом его отправителя. Здесь используются асимметричные алгоритмы шифрования.

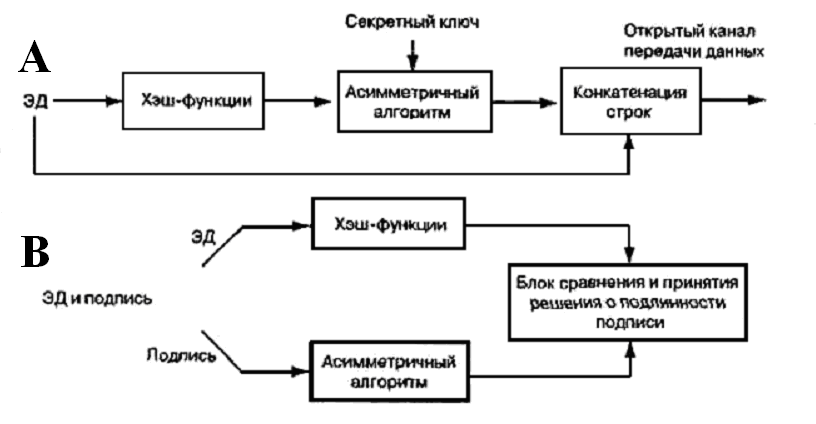


***Рис. 2. Основные методы построения схем ЭЦП. Схема 2***

Вторая схема используется довольно редко вследствие того, что длина ЭД может оказаться очень большой (шифрование асимметричным алгоритмом может оказаться неэффективным по времени), но в этом случае в принципе не требуется наличие третьей стороны, хотя она и может выступать в роли сертификационного органа открытых ключей пользователя.

**Схема 3**

Наиболее распространенная схема ЭЦП использует шифрование окончательного результата обработки ЭД хэш-функцией при помощи асимметричного алгоритма. Структурная схема такого варианта построения ЭЦП представлена на рисунке 3.



***Рис.3. Основные методы построения схем ЭЦП. Схема 3***

**Процесс генерации ЭЦП происходит следующим образом.**

Участник A вычисляет хэш-код от ЭД. Полученный хэш-код проходит процедуру преобразования с использованием своего секретного ключа. После чего полученное значение (которое и является ЭЦП) вместе с ЭД отправляется участнику B.

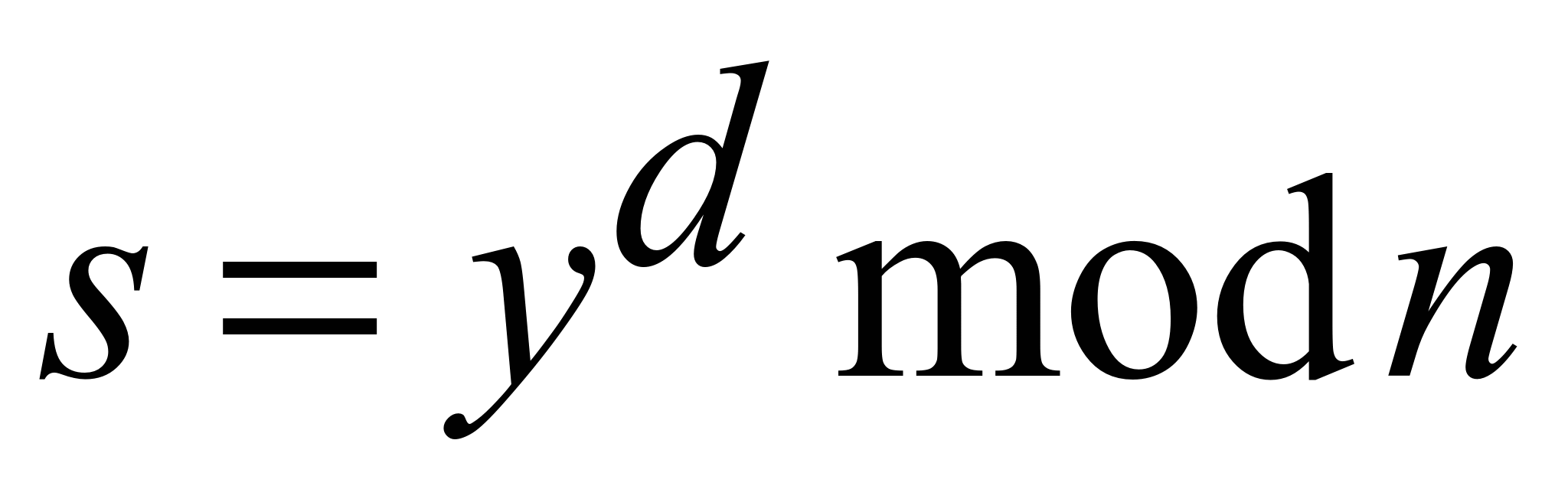
Участник B должен получить ЭД с ЭЦП и сертифицированный открытый ключ участника A, а затем произвести расшифрование на нем ЭЦП, сам ЭД подвергается операции хэширования, после чего результаты сравниваются, и если они совпадают, то ЭЦП признается истинной, в противном случае ложной.

В настоящее время применяются несколько алгоритмов цифровой подписи:

* RSA (наиболее популярен);
* Digital Signature Algorithm, DSA (алгоритм цифровой подписи американского правительства, который применяют в стандарте цифровой подписи (Digital Signature Standard, DSS), также используется часто);
* алгоритм Эль-Гамаля (иногда можно встретить).
* алгоритм, который применяют в стандарте ГОСТ РЗ4.10-94 (в основе лежит DSA и является вариацией подписи Эль-Гамаля);
* Так же существуют алгоритмы подписей, в основе которых лежит криптография эллиптических кривых; они похожи на все прочие, но в некоторых ситуациях работают эффективнее.

**Электронная подпись RSA**

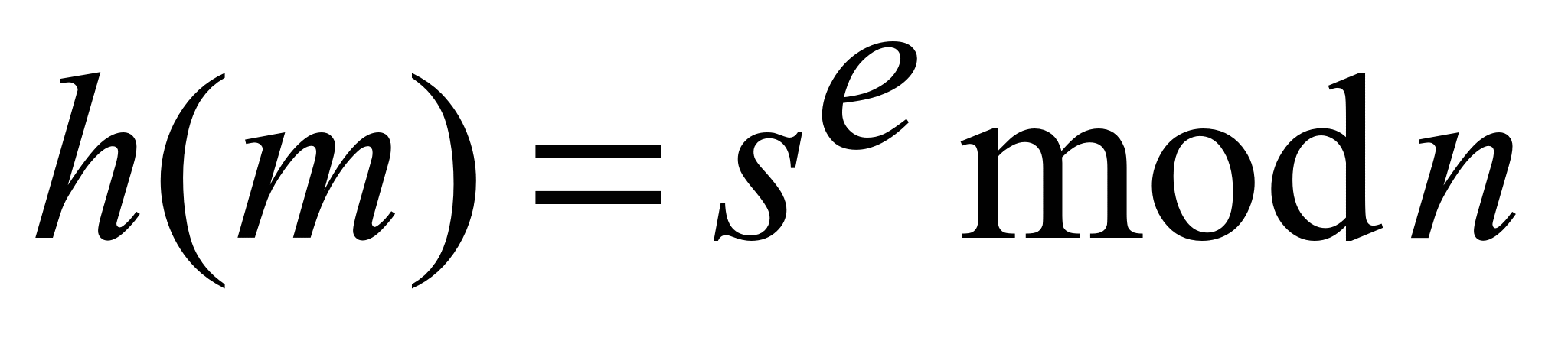
Для осуществления подписи сообщения m=m1m2m3..mn необходимо вычислить хеш-функцию y=h(m1m2m3..mn), которая ставит в соответствие сообщению m число y. На следующем шаге достаточно снабдить подписью только число y, и эта подпись будет относиться ко всему сообщению m.

Далее по алгоритму RSA вычисляются ключи (e,n) и (d,n) (см. лабораторную работу №6.1).

Затем вычисляется (d на этот раз секретная степень).

Число s это и есть цифровая подпись. Она просто добавляется к сообщению и получается подписанное сообщение.

Теперь каждый, кто знает параметры подписавшего сообщение (т.е. числа e и n), может проверить подлинность подписи.

Для этого необходимо проверить выполнение равенства.

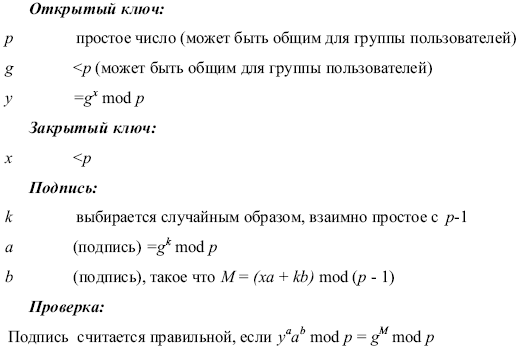
**Алгоритм Эль-Гамаля**

Для генерации пары ключей сначала выбирается простое число p и два случайных числа g и x. Оба эти числа должны быть меньше p.

http://umotnas.ru/umot/laboratornaya-rabot-14-7-elektronnaya-cifrovaya-podpise/6.pngЧтобы подписать сообщение М, сначала выбирается случайное число k, взаимно простое с p-1. Затем вычисляется

http://umotnas.ru/umot/laboratornaya-rabot-14-7-elektronnaya-cifrovaya-podpise/7.pngи с помощью расширенного алгоритма Евклида находится b в следующем уравнении:

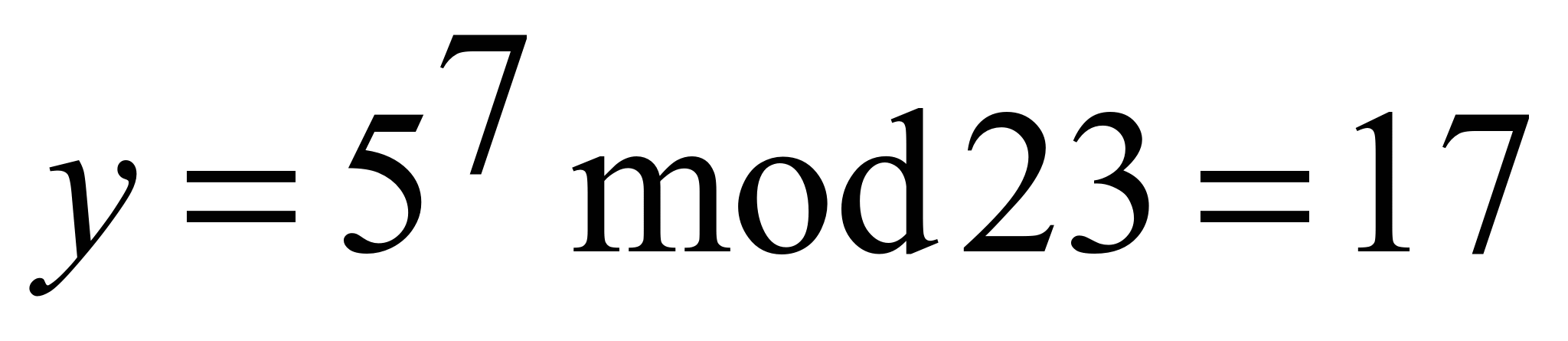
http://umotnas.ru/umot/laboratornaya-rabot-14-7-elektronnaya-cifrovaya-podpise/8.pngПодписью является пара чисел: a и b. Случайное значение k должно храниться в секрете. Для проверки подписи нужно убедиться, что



**ПРИМЕР (алгоритм Эль-Гамаля)**

1)Пусть общие параметры для некоторого сообщества пользователей p=23 и g=5.

Пусть секретный ключ x=7. Вычислим открытый ключ y:

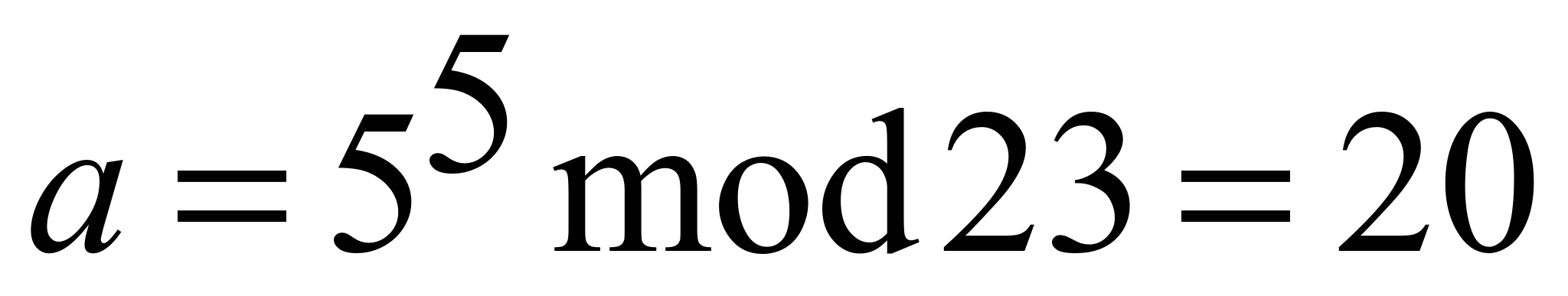
2)

Пусть нужно поставить подпись на сообщение m=baaqab

*Перейдем к вычислению подписи по алгоритму.*

3)Прежде всего, вычисляется хеш-функция. Пусть её значение h(m)=h(baaqab)=M=3.

4)Затем генерируется случайное число k, например k=5. Вычисляем по формулам

5)

И по расширенному алгоритму Евклида находим b

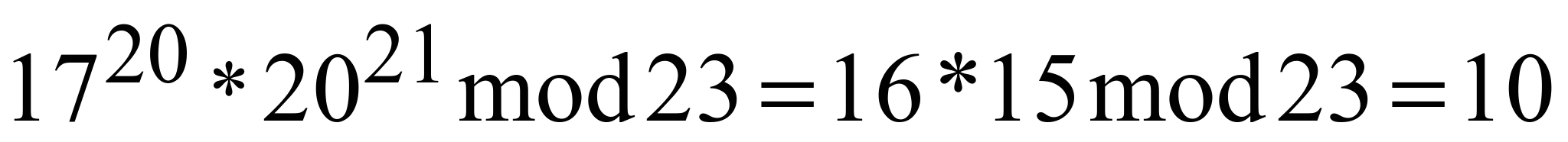
6)3=(7\*20+5\*b) mod 22

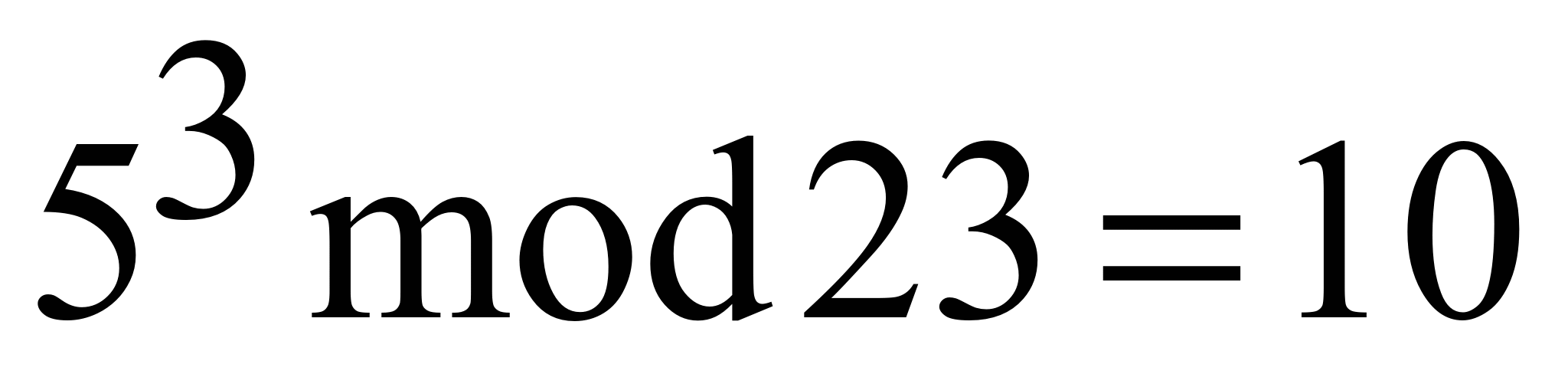
Такое b существует, т.к. НОД(k,p-1)=1. Получили b=21.

7)Получили подписанное сообщение в виде

Подписанное сообщение передается.

**Полученное сообщение проверим на подлинность.**

http://umotnas.ru/umot/laboratornaya-rabot-14-7-elektronnaya-cifrovaya-podpise/8.png1)Прежде всего, вычисляется хеш-функция h(baaqab)=M=3.

2)Затем вычисляем левую часть

3)и после этого правую

Так как левая часть совпала с правой, то можно сделать вывод, что подпись верна.

**Задание**

Реализовать приложение, позволяющие решить задачи в соответствии с вариантом.

**Задачи**

1.Для указанных открытых ключей пользователя RSA проверить подлинность подписанных сообщений:

1. n=55, e=3: <7,28>, <22,15>,<16,36> <h,s>
2. n=65, e=5: <6,42>, <10,30>,<6,41>
3. n=77, e=7: <13,41>, <11,28>,<5,26>
4. n=91, e=5: <15,71>, <11,46>,<16,74>
5. n=33, e=3: <10,14>, <24,18>,<17,8>

2. Абоненты некоторой сети применяют подпись Эль-Гамаля с общими параметрами p=23, g=5. Для указанных секретных параметров абонентов найти открытый ключ (y) и построить подпись для сообщения m:

1. x=11, k=3, m=15
2. x=10, k=15, m=5
3. x=3, k=13, m=8
4. x=18, k=7, m=5
5. x=9, k=19, m=15

Во всех вариантах будем предполагать, что h(m)=m для всех значений m.

|  |  |
| --- | --- |
| № варианта | № задач |
| 1 | 1.1 , 2.1 |
| 2 | 1.2 , 2.2 |
| 3 | 1.3 , 2.3 |
| 4 | 1.4 , 2.4 |
| 5 | 1.5 , 2.5 |
| 6 | 1.4 , 2.2 |
| 7 | 1.3 , 2.1 |

**Контрольные вопросы**

1. Для чего нужна цифровая подпись?
2. Назовите основные свойства цифровой подписи.
3. Какие схемы цифровой подписи существуют?
4. Какая схема самая распространенная? Почему?
5. Как осуществляется подпись RSA? Какое отличие подписи RSA от шифра RSA?
6. Как осуществляется подпись Эль-Гамаля?
7. Как осуществляется проверка на подлинность подписи Эль-Гамаля?