МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра «Информационная безопасность»

УТВЕРЖДАЮ
Проректор по учебной работе
_____О.Г. Локтионова
«__» _____2016 г.

АЛГОРИТМЫ ЦИФРОВОЙ ПОДПИСИ

Методические указания по выполнению курсовой работы для студентов специальностей 10.05.03, 10.05.02, 10.03.01

Курск 2016

УДК 004.056.55

Составитель М.А. Ефремов

Рецензент
Кандидат технических наук, доцент *М.О. Таныгин*

Алгоритмы цифровой подписи: методические указания по выполнению курсовой работы / Юго-Зап. гос. ун-т; сост.: М.А. Ефремов. Курск, 2016. 31 с., Библиогр.: с. 31.

Содержат основные сведения об алгоритмах формирования цифровой подписи, приведены примеры генерации числовых параметров алгоритма. Указывается порядок выполнения работы, правила оформления и содержание отчета.

Методические указания соответствуют требованиям программы, утвержденной учебно-методическим объединением по образованию в области информационной безопасности (УМО ИБ).

Предназначены для студентов специальностей 10.05.03, 10.05.02, 10.03.01 дневной формы обучения.

Текст печатается в авторской редакции

Подписано в печать . Формат 60x84 1/16.
Усл.печ. л. . Уч.-изд.л. . Тираж 30 экз. Заказ. Бесплатно.
Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94.

СОДЕРЖАНИЕ

1. ЦЕЛЬ РАБОТЫ

Цель курсовой работы - разработка, анализ и программная реализация схемы электронной цифровой подписи на основе сложности задачи дискретного логарифмирования или основанных на сложности задачи факторизации больших чисел.

2. ЗАДАНИЕ

Ознакомьтесь с теоретическим материалом. Выберите вариант задания. Проработайте схему и программно реализуйте заданный алгоритм цифровой подписи. Сгенерируйте числовой пример работы программы. Проведите анализ алгоритма и сделайте необходимые выводы.

3. ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

1. Получить задание в соответствии с номером варианта.
2. Изучить теоретическую часть с примерами.
3. Написать программу реализующую заданный алгоритм цифровой подписи.
4. Сгенерировать числовой пример работы схемы.
5. Провести анализ схемы согласно заданию на курсовое проектирование.
6. Сделать выводы о проделанной работе.
7. Составить отчет.

4. СОДЕРЖАНИЕ ОТЧЕТА

1. Титульный лист, лист задания.
2. Содержание.
3. Введение.
4. Краткая теория по теме исследования.
5. Описание программы со скриншотами.
6. Генерация числовых примеров.
7. Анализ выбранной схемы.
8. Заключение с выводами.
9. Текст программы.

5. ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

Выполнение работ по курсовому проектированию является важным этапом инженерной подготовки. Представляется целесообразным выдавать задания по таким темам, которые развивают умение пользоваться математическим аппаратом и одновременно углубляют понимание идей, на основе которых функционируют криптосистемы. Темы заданий для курсового проектирования могут быть выбраны из основных разделов криптографии, включенных в программу подготовки специалистов и бакалавров. Темы могут быть сформулированы следующим образом:

1. Разработка и программная реализация (n,k)-пороговых схем разделения секрета на основе многочленов над конечными полями.

2. Разработка и программная реализация (n,k)-пороговых схем разделения секрета на основе китайской теоремы об остатках.

3. Разработка, анализ и программная реализация схем электронной цифровой подписи на основе сложности задачи дискретного логарифмирования.

4. Разработка, анализ и программная реализация схем электронной цифровой подписи, основанных на сложности задачи факторизации больших чисел специального вида.

5. Разработка, анализ и программная реализация хэш-

функций.

6. Разработка алгоритмов факторизации, дискретного логарифмирования, извлечения корней по модулю, относящихся к заданным частным случаям параметров задачи.

7. Оптимизация вычислительных алгоритмов для реализации операций над большими числами.

Из данного списка мы уделим детальное внимание вариантам курсовых заданий, относящихся к тематике электронной цифровой подписи. Ниже предлагаются конкретные задания по этому разделу криптографии. Задачей курсового проектирования является проработка схемы ЭЦП и ее программная реализация.

Задание для курсового проектирования включает:

- общую характеристику и обоснование схемы ЭЦП, построенной на основе заданного проверочного уравнения;
- описание процедуры генерации подписи и формулирование требований к ней;
- оценку стойкости и безопасных размеров параметров криптосхемы;
- вывод формул для вычисления параметров $к$ и $g;$
- анализ схемы на наличие слабостей и поиск вариантов усиления с минимальным модифицированием;
- рассмотрение возможности экзистенциальной подделки подписи;

- рассмотрение возможности сокращения размера подписи;
- рассмотрение необходимости дополнительных требований к выбору параметров схемы ЭЦП;
- рассмотрение необходимости дополнительных требований к генерации ключей;
- рассмотрение возможности преобразования в схему ЭЦП с восстановлением сообщения;
- критический анализ на: 1) наличие избыточных операций в процедурах генерации и проверки подписи, 2) несоответствие длины открытого ключа и подписи достигаемому уровню стойкости;
- программную реализацию схемы и генерацию примера работы схемы с искусственно уменьшенным размером значений ее параметров.

5.1 Схемы ЭЦП на основе сложности дискретного логарифмирования

В заданных ниже вариантах схем цифровой подписи используются следующие параметры: $y = a^x \bmod p$ — открытый ключ; x— секретный ключ; a– число, относящееся к некоторому простому показателю γ по модулю p; (k,S) — подпись. Общая схема генерации ключа: выбирается случайное число U, по которому вычисляется значение Z (обычно $Z = a^U mod p$, однако в

некоторых вариантах используется другая; формула, которая указана в примечании), по значениям U и Z вычисляются значения k *и* g, последнее из которых определяет элемент подписи S (обычно $S = a^g \bmod p$, хотя может быть реализована процедура формирования подписи, в которой $S = y^s \bmod p$).

Варианты заданий:

1) Проверочное сравнение $a^k y^{H(Sa^k \bmod p)} \equiv S \bmod p$

Значения параметров k и g $k = \frac{U - xHZ}{2} \bmod \gamma$;

$g = \frac{U + xHZ}{2} \bmod \gamma$

2) Проверочное сравнение $a^k y^{H(Sa^k \bmod p)} \equiv S \bmod p$

Значения параметров k и g $k = \frac{U - xHZ}{2} \bmod \gamma$;

$g = \frac{U + xHZ}{2} \bmod \gamma$

Примечание $a^\gamma \equiv 1 \bmod q$; $S \equiv a^g \bmod (pq)$

3) Проверочное сравнение $y^{Hk+(Sa^k \bmod q)} \equiv S \mod p$

Значения параметров k и g $k = \frac{U - xZ}{xH + 1} \bmod \gamma$;

$g = \frac{xHU + xZ}{xH + 1} \bmod \gamma$

Примечание $a^\gamma \equiv 1 \bmod q$; $S \equiv a^g \bmod (pq)$

4) Проверочное сравнение $y^{Hk+(Sa^k \bmod q)} \equiv S \mod p$

Значения параметров k и g

$$k = \frac{-xZ \pm \sqrt{x^2 Z^2 + 4xHU}}{2xH} \bmod \gamma;$$

$$g = xHk + xZ \bmod \gamma$$

Примечания

$$X = a^{U+1} \bmod p$$

5) Проверочное сравнение

$$S^{Hk} \equiv y^{(Sa^k \bmod p)} \bmod p$$

Значения параметров k и g

$$k = \frac{HU \pm \sqrt{H^2U^2 + 4xHZ}}{2H} \bmod \gamma;$$

$$g = U - k \bmod \gamma$$

6) Проверочное сравнение

$$S^{Hk} \equiv a^{(Sy^k \bmod p)} \bmod p$$

Значения параметров k и g

$$k = \frac{HU \pm \sqrt{H^2U^2 + 4xHZ}}{2xH} \bmod \gamma;$$

$$g = U - k \bmod \gamma$$

7) Проверочное сравнение

$$S^{Hk} \equiv a^{(Sy^k \bmod p)} \bmod p$$

Значения параметров k и g

$$k = \frac{HU \pm \sqrt{H^2U^2 + 4xHZ}}{2xH} \bmod \gamma;$$

$$g = U - xk \bmod \gamma$$

Примечание

$$a^y = 1 \bmod q;\ S = a^g \bmod (pq)$$

8) Проверочное сравнение

$$S^{Hk} \equiv y^{(Sa^k \bmod p)} \bmod p$$

Значения параметров k и g

$$k = \frac{HU \pm \sqrt{H^2U^2 + 4xHZ}}{2H} \bmod \gamma;$$

$$g = U - k \bmod \gamma$$

Примечание

$$a^y = 1 \bmod q;\ S = a^g \bmod (pq)$$

9) Проверочное сравнение $Sa^k \equiv \alpha^{H\left(y^k / S \bmod p\right)} \bmod p$

Значения параметров k и g $k = \dfrac{U - Z}{x + H} \bmod \gamma$;

$$g = \frac{xZ - UH}{x + H} \bmod \gamma$$

Примечание $a^y = 1 \bmod q$; $S = a^g \bmod (pq)$

10) Проверочное сравнение $Sa^k \equiv \alpha^{H\left(y^k / S \bmod p\right)} \bmod p$

Значения параметров k и g $k = \dfrac{U - Z}{x + 1} \bmod \gamma$;

$$g = \frac{xZ - UH}{x + 1} \bmod \gamma$$

11) Проверочное уравнение $S = \alpha^{\left(y^k S \bmod p\right) + kH} \bmod p$

Значения параметров k и g $k = \dfrac{U - Z}{x + H} \bmod \gamma$;

$$g = \frac{xZ - UH}{x + H} \bmod \gamma$$

12) Проверочное уравнение $y = S^{\left(\alpha^k S \bmod q\right) + kH} \bmod p$

Значения параметров k и g

$$k = \frac{HU - Z \pm \sqrt{\left(HU - Z\right)^2 - 4H\left(x - ZU\right)}}{2H} \bmod \gamma;$$

$$g = U - k \bmod \gamma$$

13) Проверочное сравнение $y = S^{\left(\alpha^k S \bmod q\right) + kH} \bmod p$

Значения параметров k и g

$$k = \frac{HU - Z \pm \sqrt{(HU - Z)^2 - 4H(x - ZU)}}{2H} \bmod \gamma;$$

$$g = U - k \bmod \gamma$$

Примечание $a^y = 1 \bmod q;\ S = a^g \bmod (pq)$

14) Проверочное сравнение $y = S^{\left(\alpha^k S \bmod q\right)k + H} \bmod p$

Значения параметров k и g

$$k = \frac{UZ - H \pm \sqrt{(UZ - H)^2 - 4Z(HU - x)}}{2Z} \bmod \gamma;$$

$$g = U - k \bmod \gamma$$

Примечание $a^y = 1 \bmod q;\ S = a^g \bmod (pq)$

15) Проверочное сравнение $y = (S^{a^k S \bmod p)k + H} \bmod p) \bmod q$

Значения параметров k и g

$$k = \frac{UZ - H \pm \sqrt{(UZ - H)^2 - 4Z(HU - x)}}{2Z} \bmod \gamma;$$

$$g = U - k \bmod \gamma$$

Примечание $y = (a^x \bmod p) \bmod q$

16) Проверочное сравнение $Sa^k \equiv \alpha^{\left(S^k \bmod q\right)} \bmod p$

Значения параметров k и g $\quad k = \dfrac{Z \pm \sqrt{Z^2 - 4xU}}{2x} \bmod \gamma;$

$g = Z - xk \bmod \gamma$

Примечание $a^y = 1 \bmod q;\ S = a^g \bmod (pq);$

$Z = a^U \bmod q$

17) Проверочное сравнение $(Sa)^k \equiv \alpha^{\left(Sa^k \bmod q\right)} \bmod p$

Значения параметров k и g

$$k = \frac{U + x}{2} \pm \sqrt{\frac{(U + x)^2}{4} - Z} \bmod \gamma;$$
$$g = U - k \bmod \gamma$$

Примечание Возможна подделка подписи с использованием представления параметра S в виде

$$S = y^{-1} a^8 \bmod p$$

18) Проверочное сравнение $(Sa)^k \equiv \alpha^{\left(Sa^k \bmod q\right)} \bmod p$

Значения параметров k и g $k = \frac{Z - U}{x} \bmod \gamma;$

$$g = \frac{Ux}{Z - U} \bmod \gamma$$

19) Проверочное уравнение $y \equiv (S^{(a^k / S \bmod p) + k + H} \bmod p) \bmod q$

Значения параметров k и g

$$k = \frac{U - Z - H}{2} \pm \sqrt{\frac{(U - Z - H)^2}{4} + (UZ + UH + x)} \bmod \gamma;$$
$$g = k - U \bmod \gamma$$

Примечание Схема с открытым ключом малого размера

$$y = (a^x \bmod p) \bmod q;$$

20) Проверочное уравнение $y \equiv (S^{(a^{-k} S \bmod p) kH} \bmod p) \bmod q$

Значения параметров k и g $k = \frac{-UZH \pm \sqrt{(UZH)^2 + 4xZH}}{2ZH} \bmod \gamma$

$$g = U + k \bmod \gamma$$

Примечание Схема с открытым ключом малого размера:

$$y = (a^x \bmod p) \bmod q;$$

21) Проверочное уравнение $y \equiv (S^{(a^k S \bmod p)H} \bmod p) \bmod q$

Значения параметров k и g $k = U - \frac{x}{Z} \bmod \gamma;\ g = \frac{x}{Z} \bmod \gamma$

Примечание $y = (a^x \bmod p) \bmod q;$

22) Проверочное уравнение $Sa^k \equiv \alpha^{H\left(y^k / S \bmod p\right)} \bmod p$

Значения параметров k и g $k = U - \frac{x}{Z} \bmod \gamma;\ k = \frac{x}{Z} \bmod \gamma$

Примечание $Z = Ha^U \bmod p;$
$y = (a^x \bmod p) \bmod q$

23) Проверочное уравнение $y = (S^{Hk} a^{(a^k S \bmod p)} \bmod p) \bmod q$

Значения параметров k и g $k = \frac{UH \pm \sqrt{U^2 H^2 + 4H(Z - x)}}{2H} \bmod \gamma;$
$g = k - U \bmod \gamma$

Примечание Схема с открытым ключом малого размера $y = (a^x \bmod p) \bmod q;$

24) Проверочное уравнение $y = (aS^{(S^k H \bmod p)} \bmod p) \bmod q$

Значения параметров k и g $k = \frac{UZ}{x-1} \bmod \gamma;\ g = \frac{x-1}{Z} \bmod \gamma$

Примечание $Z = Ha^U \bmod p;$
$y = (a^x \bmod p) \bmod q$

25) Проверочное уравнение $y = (aS^{(S^{H/k} \bmod p)} \bmod p) \bmod q$

Значения параметров k и g $k = \pm\sqrt{\frac{(x-1)H}{UZ}} \bmod \gamma$;

$g = \frac{x-1}{kZ} \bmod \gamma$

Примечание $y = (a^x \bmod p) \bmod q$

26) Проверочное уравнение $y = (a^{H(Sa^k \bmod p)} S^k \bmod p) \bmod \delta$

Значения параметров k и g $k = \frac{U}{2} \pm \sqrt{\frac{U^2}{4} + (HZ - x)} \bmod \gamma$;

$g = U - k \bmod \gamma$

Примечание $y = (a^x \bmod p) \bmod \delta$;

$S = a^2 \bmod(pq)$

27) Проверочное уравнение $y = ((aS^{(HS^k \bmod p)} \bmod p) \bmod q$

Значения параметров k и g $k = \frac{UZ}{x - Z} \bmod \gamma$;

$g = \frac{x - Z}{Z} \bmod \gamma$

Примечание $y = (a^x \bmod p) \bmod q$;

$Z = Ha^U \bmod p$

28) Проверочное сравнение $y^H = (aS)^{(S^k \bmod p)} \bmod p$

Значения параметров k и g $k = \frac{UZ}{Hx - Z} \bmod \gamma$;

$g = \frac{x-1}{kZ} \bmod \gamma$

29) Проверочное сравнение $a^H = Sy^{(S^k \bmod p)} \bmod q$

Значения параметров k и g $k = \dfrac{U}{H - xZ} \bmod \gamma$;

$g = H - xZ \bmod \gamma$

30) Проверочное сравнение $y^H = (aS)^{(HS^k \bmod p)} \bmod p$

Значения параметров k и g $k = \dfrac{UZ}{x - Z} \bmod \gamma$;

$g = \dfrac{x - Z}{Z} \bmod \gamma$

Примечание $Z = Ha^U \bmod p$

31) Проверочное сравнение $y^H = (aS)^{(a^k S \bmod p)} \bmod p$

Значения параметров k и g $k = \dfrac{UZ - xH + Z}{Z} \bmod \gamma$;

$g = \dfrac{Hx - Z}{Z} \bmod \gamma$

32) Проверочное сравнение $y^H = Sa^{(Ha^k S \bmod p)} \bmod p$

Значения параметров k и g $k = \dfrac{U + Z}{x + 1} \bmod \gamma$;

$g = \dfrac{Ux - Z}{x + 1} \bmod \gamma$

Примечание $Z = Ha^U \bmod p$

33) Проверочное сравнение $S^H = y^{(a^k S \bmod p)} \bmod p$

Значения параметров k и g $k = \dfrac{UH - xZ}{H} \bmod \gamma$;

$$g = \frac{xZ}{H} \bmod \gamma$$

34) Проверочное сравнение

$$Sy = a^{(Hy^k S \bmod p)} \bmod p, где\ y == a^x \bmod(pq)$$

Значения параметров k и g $\quad k = U + 1 = \frac{Z}{x} \bmod \gamma;$

$$g = \frac{Z - x}{x} \bmod \gamma$$

Примечание

$$a^{\gamma} = 1 \bmod q; S = y^g \bmod(pq); Z = Hy^U \bmod q$$

35) Проверочное сравнение $\quad S^{(Ha^k S \bmod p)} = y^{(a^k S \bmod p)} \bmod p$

Значения параметров k и g $\quad k = U - xZ / Z^{'} \bmod \gamma;$

$$g = xZ / Z^{'} \bmod \gamma$$

Примечание $\quad Z^{'} = Ha^U \bmod p$

36) Проверочное сравнение $\quad S^{(a^{-k} S \bmod p)} = y^{(Ha^k S^{-1} \bmod p)} \bmod p$

Значения параметров k и g $\quad k = U + xZ^{'} / Z \bmod \gamma;$

$$g = xZ^{'} / Z \bmod \gamma$$

Примечание $\quad Z^{'} = HZ^{-1} \bmod p$

37) Проверочное сравнение $\quad S^{(y^k S^H \bmod p)} = a^{(y^{-k} S^{-H} \bmod p)} \bmod p$

Значения параметров k и g $\quad k = \frac{UZ - HZ^{'}}{Zx} \bmod \gamma;$

$$g = Z^{'} / Z \bmod \gamma$$

Примечание $\quad Z^{'} = Z^{-1} \bmod p$

38) Проверочное сравнение $S^{(Ha^k S \bmod p)} = y^{(a^k S \bmod p)} \bmod p$

Значения параметров k и g $k = U - xZ / Z^{'} \bmod \gamma$;

$g = xZ^{'} / Z \bmod \gamma$

Примечание $a^{\gamma} = 1 \bmod q; S = a^g \bmod (pq)$;

$Z^{'} = Z^{-1} \bmod p$

39) Проверочное сравнение $S^{(y^k S^H \bmod p)} = a^{(y^{-k} S^{-H} \bmod p)} \bmod p$

Значения параметров k и g $k = \dfrac{UxHZ}{xHZ + Z^{'}} \bmod \gamma$;

$g = \dfrac{UZ^{'}}{xHZ + Z^{'}} \bmod \gamma$

Примечание $Z = y^U \bmod p$; $Z^{'} = Z^H \bmod p$

40) Проверочное сравнение $S^{[(y^k S^H \bmod p)]} = a^{k + (y^k S \bmod p)} \bmod p$

Значения параметров k и g $k = \dfrac{UxZ^{'} - Z}{1 + xZ^{'}} \bmod \gamma$;

$g = \dfrac{U + Z}{1 + xZ^{'}} \bmod \gamma$

Примечание $Z^{'} = Z^{-1} \bmod p$; $Z^{'} = Z^H \bmod p$

5.2 Схема ЭЦП на основе сложности факторизации RSA-модуля

В схемах на основе сложности факторизации составного модуля n, представляющего собой произведение двух больших

сильных простых чисел $(n=pq)$, используются следующие типовые параметры: $(n,\ a)$ — открытый ключ, где $n = rq$ и a — число, относящееся по модулю n к показателю $\gamma = \gamma'\gamma''$, где γ' и γ'' есть простые делители: $\gamma' | r-1 |$ и $\gamma'' | q-1 |$ (причем y' не делит q - 1 и y'' не делит r - 1); y - секретный ключ; (g, R), (k,S) или (R,S) — подпись; H — хэш-функция от подписываемого документа.

Общая схема генерации ключа: выбирается случайное число U, по которому вычисляется значение Z (обычно $Z=a^U \bmod n$, однако в некоторых вариантах используется другая формула, которая указана в примечании), по значениям U и Z определяются значения κ и g, из которых вычисляются элементы подписи R и S (обычно $R = a^\kappa \bmod n$ и $S = a^g \bmod n$ и, хотя эти параметры могут представляться и в другом виде при выполнении процедуры генерации подписи). Параметры $p,\ q$ и r представляют собой достаточно большие простые числа, $|x|$ — обозначение длины числа x.

Варианты заданий:

1) Проверочное уравнение

$$H = R^Q S^{Q^t} \bmod n, \text{где } Q = RS \bmod n \text{ и } |R| \approx |S| > 100 \text{ бит}$$

Значения параметров k и g $\qquad k = \dfrac{UZ^t}{Z^t - Z} \bmod \gamma;$

$$g = \frac{UZ}{Z - Z^t} \bmod \gamma$$

Примечание $\qquad S = Ha^g \bmod n;\ Z = Ha^U \bmod n$

2) Проверочное сравнение $a^{k+H(Sa^k \bmod n)} = S \bmod n$

Значения параметров k и g $k = \frac{U - HZ}{2} \bmod \gamma;$

$g = \frac{U + HZ}{2} \bmod \gamma$

Примечание $S = a^g \bmod n$

3) Проверочное сравнение $S^{H+(Sa^k \bmod n)} = a^k \bmod n$

Значения параметров k и g $k = \frac{U(H + Z)}{H + Z + 1} \bmod \gamma;$

$g = \frac{U}{H + Z + 1} \bmod \gamma$

Примечание $S = a^g \bmod n$

4) Проверочное сравнение $a^{Hk(S^k \bmod n)} = S \bmod n$

Значения параметров k и g $k = \frac{-Z \pm \sqrt{Z^2 + 4HU}}{2H} \bmod \gamma$

$g = \frac{Z \pm \sqrt{Z^2 + 4HU}}{2} \bmod \gamma$

5) Проверочное сравнение $S^{Hk} = a^{(Sa^k \bmod n)} \bmod n$

Значения параметров k и g $k = \frac{HU \pm \sqrt{H^2U^2 - 4HU}}{2H} \bmod \gamma;$

$g = U - k \bmod \gamma$

6) Проверочное уравнение $a = (RS)^{(S/R \bmod n)} \bmod n$

Значения параметров k и g $k = \frac{1 - UZ}{2Z} \bmod \gamma;$

$$g = \frac{1+ZU}{2Z} \bmod \gamma$$

7) Проверочное сравнение $S^{Hk} = a^{(Sa^k \bmod n)} \bmod n$, где (a, n', n) - открытый ключ

Значения параметров k и g $k = \frac{HU \pm \sqrt{H^2U^2 - 4HZ}}{2H} \bmod \gamma$;
$g = U - k \bmod \gamma$

Примечание $a^y = 1 \bmod n'$; $S = a^g \bmod (n'n)$;
$n' = p'q'$

8) Проверочное сравнение $R^g = a^{H(Ra^g \bmod p)} \bmod p) \bmod n$ и
$R^g = a^{H(Ra^g \bmod p)} \bmod n) \bmod n$

Значения параметров k и g $k = \frac{U}{2} \pm \sqrt{U^2 / 4 - HZ} \bmod \gamma$;
$g = \frac{U}{2} \mp \sqrt{U^2 / 4 - HZ} \bmod \gamma$

Примечание $a^y = 1 \bmod n'$; $R = a^k \bmod (pn)$

9) Проверочное сравнение $S^{(S^k \bmod n)} = a^H \bmod n$

Значения параметров k и g $k = \frac{UZ}{H} \bmod \gamma$; $g = \frac{H}{Z} \bmod \gamma$

10) Проверочное сравнение $aS^{H(S^k \bmod n)} = 1 \bmod n$

Значения параметров k и g $k = -HUZ \bmod \gamma$;
$g = \frac{-1}{Z - H} \bmod \gamma$

11) Проверочное сравнение $S^{(Sa^k \bmod n)} a^{Hk} = 1 \bmod n$

Значения параметров k и g $k = \frac{UZ}{Z - H} \bmod \gamma;$

$g = \frac{-HU}{Z - H} \bmod \gamma$

12) Проверочное уравнение $a = {}^{(Sa^k \bmod n)} \bmod n$

Значения параметров k и g $k = \frac{UZ}{Z - H} \bmod \gamma;\ g = \frac{1}{Z} \bmod \gamma$

Примечание $S = H^{-1} a^g \bmod n;$

$Z = H^{-1} a^U \bmod n$

13) Проверочное сравнение $a^{Hk} = S^{(S^k \bmod n)} \bmod n$

Значения параметров k и g $k = \pm\sqrt{UZ / H} \bmod \gamma;$

$g = \pm\sqrt{UH / Z} \bmod \gamma$

14) Проверочное сравнение $(aS)^{Hk} = a^{(S^k \bmod n)} \bmod n$

Значения параметров k и g $k = \frac{Z - UH}{H} \bmod \gamma;$

$g = \frac{UH}{Z - UH} \bmod \gamma$

15) Проверочное сравнение $(HS)^k = a^{H(Sa^k \bmod n)} \bmod n$

Значения параметров k и g $k = \frac{U}{2} \pm \sqrt{U^2 / 4 - HZ} \bmod \gamma;$

$g = \frac{U}{2} \mp \sqrt{U^2 / 4 - HZ} \bmod \gamma$

Примечание $S = H^{-1} a^g \bmod n;$

$Z = H^{-1} a^U \bmod n$

16) Проверочное сравнение $S^{H+k} = a^{(S^k \bmod n)} \bmod n$

Значения параметров k и g $k = \frac{UH}{Z - H} \bmod \gamma$;

$g = \frac{Z - U}{H} \bmod \gamma$

17) Проверочное сравнение $a^{H+k} = a^{(S^k \bmod n)} \bmod n$

Значения параметров k и g $k = \frac{U}{2} \pm \sqrt{H^2 / 4 - UZ} \bmod \gamma$;

$g = \frac{U}{k} \bmod \gamma$

Примечание $a^y = 1 \bmod n$; $n' = r'q'$;

$S = a^g \bmod (n'n)$;

$Z = a^U \bmod (n'n)$

18) Проверочное сравнение $S^{1+k} = a^{(HS^k \bmod n)} \bmod n$

Значения параметров k и g $k = \frac{U}{Z - U} \bmod \gamma$;

$g = Z - U \bmod \gamma$

Примечание $Z = Ha^U \bmod p$

19) Проверочное уравнение $S = a^{(HS^k \bmod n)} \bmod n$

Значения параметров k и g $k = \frac{U}{2} \bmod \gamma$; $g = Z \bmod \gamma$

Примечание $Z = Ha^U \bmod p$

20) Проверочное сравнение $Sa^k = a^{(HS^k \bmod n)} = 1 \bmod n$

Значения параметров k и g $k = \frac{Z}{2} \pm \sqrt{Z^2 / 4 - U} \bmod \gamma$;

$$g = \frac{Z}{2} \mp \sqrt{H^2 / 4 - U} \bmod \gamma$$

Примечание $Z = Ha^U \bmod p$

21) Проверочное сравнение $a^H = R^{(R^g \bmod p)} \bmod p \; и \; |g| < 520 бит,$ $где \; p = 2n + 1 \; и \; n = rq$

Значения параметров k и g $k = \frac{H}{Z} \bmod q;$ $g = \frac{ZU}{H} \bmod q$

Примечание $a^q = 1 \bmod p, q -$ секретный ключ

22) Проверочное сравнение $a^{Hg} = R^{(R^g \bmod p)} \bmod p \; и \; |g| < 520 бит,$ $где \; p = 2n + 1 \; и \; n = rq$

Значения параметров k и g $k = \pm\sqrt{UH / Z} \bmod q;$ $g = \pm\sqrt{UZ / H} \bmod q$

Примечание $a^q = 1 \bmod p, q -$ секретный ключ

23) Проверочное сравнение $a^H = R^{g+(Ra^g \bmod p)} \bmod p \; и \; |g| < 520 бит,$ $где \; p = 2n + 1 \; и \; n = rq$

Значения параметров k и g $k = \frac{U + Z}{2} \pm \sqrt{\frac{(U + Z)^2}{4} - H} \bmod \gamma;$

$$g = \frac{U - Z}{2} \pm \sqrt{\frac{(U + Z)^2}{4} - H} \bmod \gamma$$

Примечание $a^q = 1 \bmod p, q -$ секретный ключ

24) Проверочное сравнение $R^H = y^{(Ra^g \bmod p)} \bmod p \; и \; |g| < 520 бит,$ $где \; p = 2n+1 \; и \; n = rq$

Значения параметров k и g $k = \frac{xZ}{H} \bmod q;$ $g = \frac{UH - xZ}{H} \bmod q$

Примечание $a^q = 1 \bmod p; y = a^x \bmod p -$ элемент открытого ключа; $(x, q) -$ секрет

25) Проверочное сравнение $y^{Hg} = R^{(Ra^g \bmod p)} \bmod p \; и \; |g| < 520 бит,$ $где \; p = 2n+1 \; и \; n = rq$

Значения параметров k и g $k = \frac{xHU}{Z + xH} \bmod q;$ $g = \frac{UZ}{Z + xH} \bmod q$

Примечание $a^q = 1 \bmod p; y = a^x \bmod p -$ элемент открытого ключа; $(x, q) -$ секрет

26) Проверочное сравнение $a^g = R^{(HRy^g \bmod p)} \bmod p \; и \; |g| < 520 бит,$ $где \; p = 2n+1 \; и \; n = rq$

Значения параметров k и g $k = \frac{U}{Zx+1} \bmod q;$ $g = \frac{UZx}{Zx+1} \bmod q$

Примечание $a^q = 1 \bmod p; y = a^x \bmod p;$ $Z = Hy^U \bmod p$

27) Проверочное сравнение $R^{H+g} = R^{(R^g \bmod p)} \bmod p \; и \; |g| < 520 бит,$ $где \; p = 2n+1 \; и \; n = rq$

Значения параметров k и g

$$k = \frac{Z - U}{H} \bmod q;$$
$$g = \frac{UH}{Z - U} \bmod q$$

Примечание $a^q = 1 \bmod p$, q – секрет

28) Проверочное сравнение $Ra^{(RS \bmod n)} = S^{(HR \bmod n)} \bmod n$

Значения параметров k и g

$$k = \frac{UZ^{'} - Z}{1 + Z^{'}} \bmod \gamma;$$
$$g = \frac{U + Z}{1 + Z^{'}} \bmod \gamma$$

Примечание $Z^{'} = Ha^U \bmod n$

29) Проверочное сравнение $R^{H+g} = a^{1+(R^{Hg} \bmod n)} \bmod n$

Значения параметров k и g

$$k = \frac{Z + 1 - U / H}{H} \bmod \gamma;$$
$$g = \frac{UH}{HZ + H - U} \bmod \gamma$$

30) Проверочное сравнение $R^{gH+a} = a^{(HR^{Hg} \bmod n)} \bmod n$

Значения параметров k и g

$$k = \frac{Z - UH}{a} \bmod \gamma;$$
$$g = \frac{Ua}{Z - UH} \bmod \gamma$$

Примечание $Z = Ha^U \bmod n$

31) Проверочное сравнение $k + v = (a^{kgvH} \bmod n)^{(k - v \bmod \delta)} \bmod \delta$

(g, k, v) – подпись;

(n, a) – открытый ключ

Значения параметров k ,v и g

$$k = \frac{U_2 + Z^{U_2}}{2} \bmod \delta;$$
$$v = \frac{Z^{U_2} - U_2}{2} \bmod \delta;$$
$$k = \frac{U_1}{Hkv} \bmod \gamma$$

Примечание

$U_1 < \gamma$ и $U_2 < \delta$ – случайные числа;
$$Z = (a^{U_1} \bmod n) \bmod \delta$$

32) Проверочное сравнение

$$k = H(a^{kgvH} \bmod n) \bmod \delta$$

Значения параметров k и g

$$k = HZ \bmod \delta;$$
$$g = \frac{U}{kH} \bmod \gamma$$

Примечание

$$Z = (a^{U} \bmod n) \bmod \delta$$

33) Проверочное сравнение

$$k = H(a^{kg^2} \bmod n) \bmod \delta$$

Значения параметров k и g

$$k = Z \bmod \delta;$$
$$g = \sqrt{\frac{U}{Z}} \bmod \gamma$$

Примечание

$$Z = (Ha^{U} \bmod n) \bmod \delta$$

34) Проверочное сравнение

$$k^2 = (Ha^{kg^2} \bmod n) \bmod \delta$$

Значения параметров k и g

$$k = \pm\sqrt{Z} \bmod \delta;$$
$$g = \pm\sqrt{\frac{U}{k}} \bmod \gamma$$

Примечание

$$Z = (Ha^{U} \bmod n) \bmod \delta$$

35) Проверочное сравнение $k = (a^{k-Hg^2} \bmod n) \bmod \delta$

Значения параметров k и g $k = Z$;
$g = (Z - U)H^{-1} \bmod \gamma$

Примечание $Z = (a^U \bmod n) \bmod \delta$

36) Проверочное сравнение $k \,/\, g = (Ha^{k+g} \bmod n) \bmod \delta$

Значения параметров k и g $k = Zg$;
$g = \dfrac{U}{Z+1} \bmod \gamma$

Примечание $Z = (Ha^U \bmod n) \bmod \delta$

6. ВЫПОЛНЕНИЕ РАБОТЫ

6.1 Генерация числовых примеров

В качестве иллюстраций в пояснительную записку к курсовому проекту (курсовой работе) могут быть включены числовые примеры, генерируемые с помощью программы, реализующей заданную схему ЭЦП. Желательно, чтобы эти примеры отражали все этапы функционирования схемы ЭЦП:

1. Формирование системных параметров, являющихся общими для всех предполагаемых пользователей.
2. Генерацию открытого и секретного ключей.
3. Процедуру генерации подписи.
4. Процедуру проверки подлинности подписи.

Такое задание может быть использовано при проведении практических занятий. Для этого обучаемым задаются конкретные варианты схем ЭЦП с краткими теоретическими пояснениями. Они должны сгенерировать числовые примеры, иллюстрирующие вычислительный процесс на одном или нескольких этапах, указанных выше. Для этого могут быть использованы программы, позволяющие выполнять над большими числами типовые операции модульной арифметики. Ниже приводятся некоторые частные примеры.

Пример1. Схема ЭЦП задана проверочным сравнением

$$a^k \equiv Sy^{a^k S \bmod p} a^{\left(H\left(a^k S \bmod p\right)\right) \bmod \delta} \bmod p.$$

Сформируем системные параметры:

p= 11882429488026351022427721066379892803 57;

α= 68250220082135354422389774242962653 4895;

γ= 18726613052735935810340979053 3;

δ= 10000000000000000 3.

Выберем секретный ключ x=12345678900987654321,

тогда открытый ключ

$y = a^x \bmod p$ =515195030626449857135211347072944115270.

Пусть значение хэш-функции от сообщения, которое надо подписать, равно H = 11223344556677889900.

Процедура генерации подписи:

1. Выберем случайное значение U ($U < p-1$):

U=13894564231549754238457865456.

2. Вычислим значение

$Z = a^U \bmod p$ = 64701698466156431941656940816468800 2775.

3. Решая систему $\begin{cases} k + \mathrm{g} = U \bmod \gamma \\ k = \mathrm{g} + xZ + (HZ \bmod \delta) \bmod \gamma \end{cases}$

получаем:

$$k = \frac{U - xZ - (HZ \bmod \delta)}{2} \bmod \gamma$$

$$= 68742013608792151040356901280;$$

$$g = \frac{U + xZ + (HZ \bmod \delta)}{2} \bmod \gamma$$

$$= 13241868115011696130151075 4709.$$

4. Вычисляем $S = a^g \bmod p =$ 25127402077641808427192285642803083 15.

Подписью является пара чисел:

(k,S)=(687420136087921510403569012 80,

25127402077641808427192285642803083 15).

Проверка подписи:

$Sy^{a^k S \bmod p} a^{\left(H\left(a^k S \bmod p\right)\right) \bmod \delta} \bmod p =$

55896938576706922941565114662228101 3229,

a^k= 55896938576706922941565114662228101 3229.

Пример 2. Схема ЭЦП задана проверочным сравнением $a^{k+H(Sa^k \bmod n)} \equiv S \; mod \; n.$

Генерация секретного ключа:

r = 38336291019121266534774 83;

q = 45373466457550950652522 9;

$\gamma' = 200734627(\gamma' | \mathrm{r} - 1)$;

$\gamma'' = 96948517(\gamma'' | \mathrm{q} - 1)$;

$\gamma = \gamma' \gamma'' = 1946092439819815 9.$

Генерация открытого ключа:

$n = rq = 17394504146630105372832550258911757935327229186 07;$

$\alpha = 14428326838611439083400129803654133383576793814 12.$

Пусть H= 78645315670456453156756 0.

Процедура генерации подписи:

1. Выбираем случайное значение $U < y$.

$U = 344476610.$

2. Вычисляем значение $Z = a^H \bmod n$:

$N = 172155\,816056124122192424959631233728556701770812 1.$

3. Решая систему сравнении $\begin{cases} k + \mathrm{g} = U \bmod \gamma \\ k + HZ = \mathrm{g} \bmod \gamma \end{cases}$

получаем:

$$k = \frac{U - HZ}{2} \bmod \gamma = 3147453087865669;$$

$$g = \frac{U + HZ}{2} \bmod \gamma = 16313471654809100.$$

4. Вычисляем $S = a^s \bmod p$:

S= 125230090658607125842512070317007281419514841706 6.

Подписью является пара чисел (*k, S):*

$k = 3147453087865669;$

$S = 125230090658607125842512070317007281419514841706 6.$

Проверка подписи:

$a^{k+H(Sa^k \bmod n)} = 125230090658607125842512070317007281419514841706 6,$

$S \bmod n = 125230090658607125842512070317007281419514841706 6.$

Пример 3. Схема ЭЦП описывается проверочным сравнением

$$S^{(S^k mod n)} \equiv \alpha^H \bmod n.$$

Генерация секретного ключа:

$r = 863151485261213534633759;$

$q = 86247561966378373427412 43;$

$\gamma' = 498957821\ (\gamma' | r - 1);$

$\gamma'' = 495912449\ (\gamma'' |\ q - 1);$

$\gamma = \gamma'\gamma'' = 2474393949598136 29.$

Генерация открытого ключа:

$n = rq =$ 744447112114380436105374313903546348808110942243 7;

$\alpha =$ 168754170955043342893915075479733762663466305991 8.

Пусть H = 102304506708901203564879 4.

Процедура генерации подписи:

1. Выбираем случайное число $U < p - 1$:

$U = 94802439.$

2. Вычисляем $Z = \alpha^U \bmod p$:

$Z =$ 47284599495 00977114501570951051961049234719786624.

3. Решая систему сравнении $\begin{cases} k\mathrm{g} = U \bmod \gamma \\ \mathrm{g}Z = H \bmod \gamma \end{cases}$ получаем

$k = \frac{UZ}{H} \bmod \gamma = 1120670232541317 84;$

$\mathrm{g} = \frac{H}{Z} \bmod \gamma$ =695135039327628 68.

4. Вычисляем $S = a^k \, mod \, n$:

S= 97587919740196844623379775245485493287155203132 2.

Получена подпись (k, S), где $k = 1120670232541317 84;$

$S =$ 97587919740196844623379775245485493287155203132 2.

Проверка подписи:

$S^{(S^k \, mod \, n)} =$ 57405068519815122984307768133345626933414296013 24,

$\alpha^H \bmod n =$ 57405068519815122984307768133345626933414296013 24.

7. СПИСОК ИСПОЛЗУЕМЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ

1. Виноградов И.М. Основы теории чисел. М.: Наука,1995.

2. Молдовян Н.А. Практикум по криптосистемам с открытым ключом. – СПб.: БХВ-Петербург, 2007. – 304 с.: ил.

3. Пензин Ю.Г., Клейменов В.Ф. Сравнения. Учебно-методические разработки (тексты лекций). Изд-во ИГУ, 1998.

4. И.М. Виноградов «Элементы высшей математики» М., «Высшая школа», 1999

5. Л.Я. Куликов, А.И. Москаленко, А.А. Фомин «Сборник задач по алгебре и теории чисел» М., «Просвещение», 1993

6. Ю.С. Харин, В.И. Берник, Г.В. Матвеев, С.В. Ажевич «Математические и компьютерные основы криптологии» Минск, «Новое знание», 2003