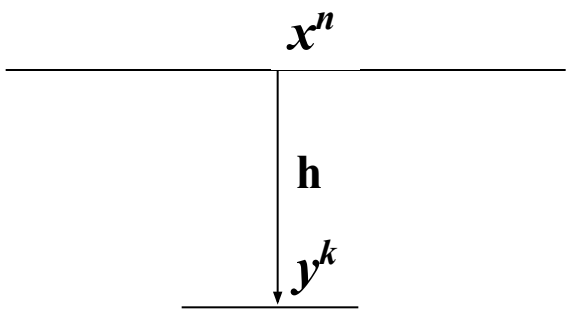
Лекция:
ПОНЯТИЕ ОБ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ

Понятие хэширующей-функции

Определение. Хэширующая функция это отображение строки (цепочки) бит произвольной длины в строку (цепочку) бит фиксированной длины.



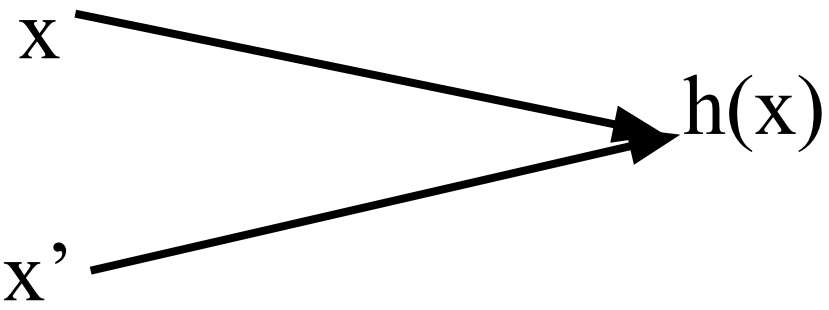
$y=h(x)$

$x \in X,\ y \in Y,\ h \in H,$ X,Y - дискретные множества, $|X|=2^n$, $|Y|=2^k$

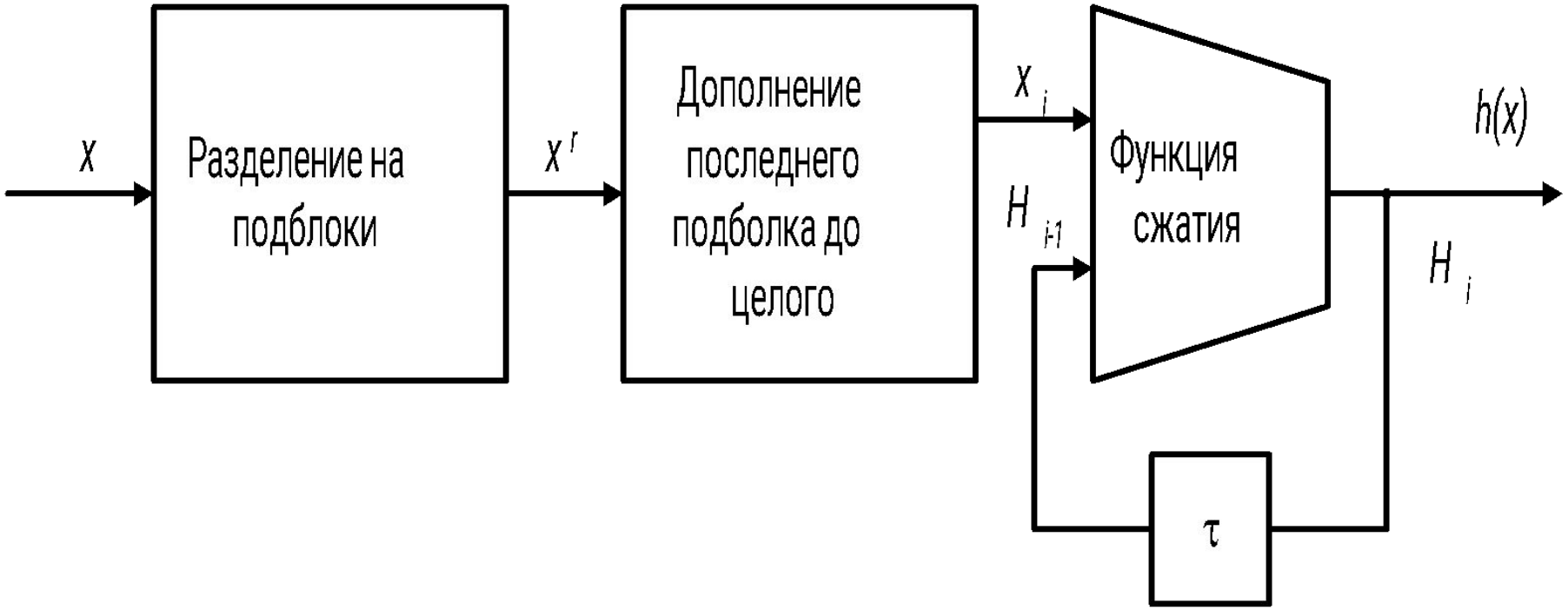
Свойства хэш-функции

- **1.Хэш-функция должна быть стойкой в смысле обращения.** Для данного значения h(x) должно быть вычислительно сложно найти аргумент x.
- 2. **Хэш-функция должна быть стойкой в смысле вычисления коллизий.** Коллизия возникает, когда несколько сообщений имеют одинаковое значение хэш-функции.

  Для данного аргумента x должно быть вычислительно сложно найти другой аргумент x’, такой что h(x)=h(x’).



Принцип построения итеративной хэшфункции



ГОСТ Р34.11-94
Информационная технология. Криптографическая защита информации. Функция хэширования.

Алгоритм хэширования на основе одношаговой сжимающей функции

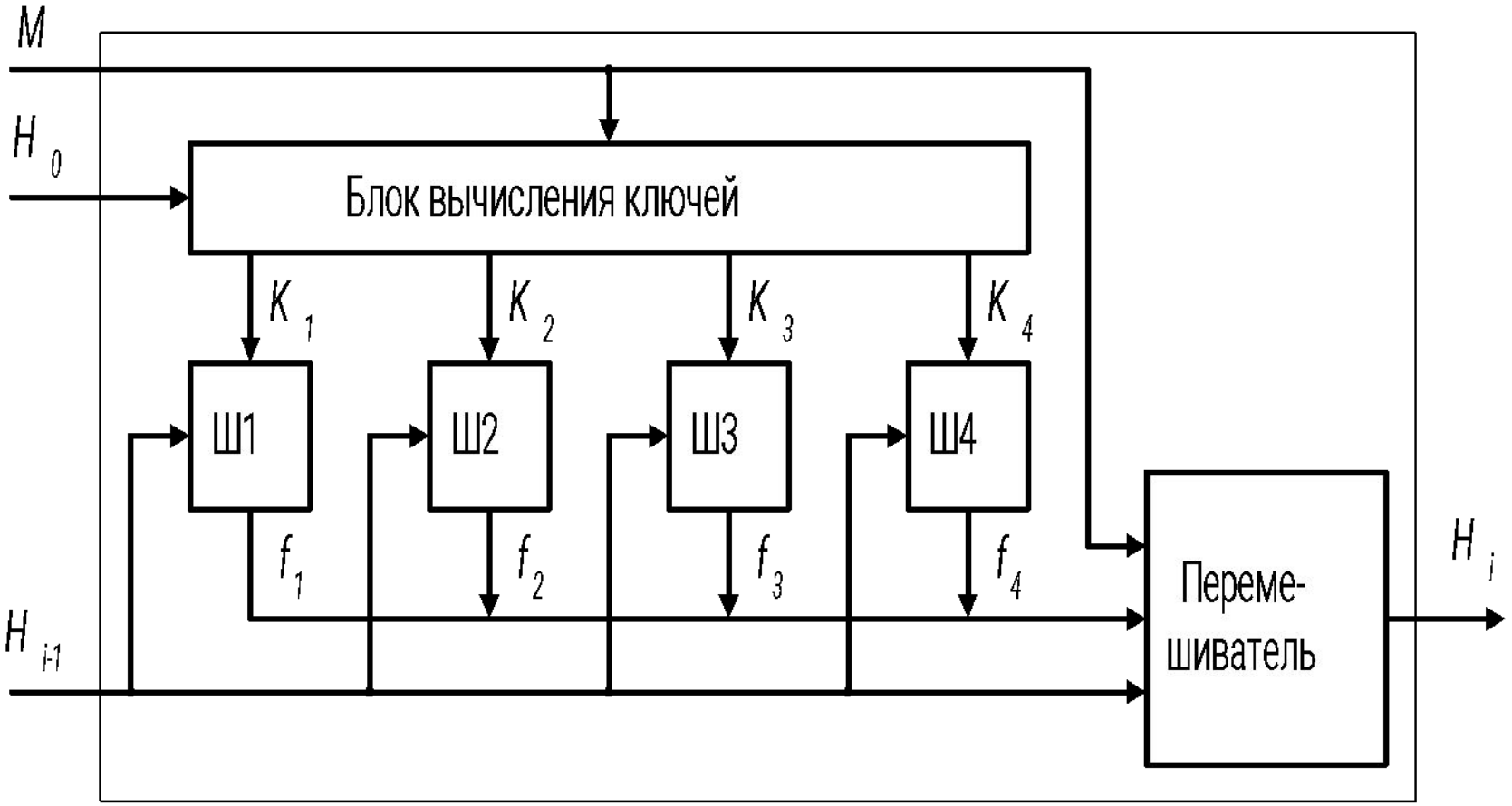
$H_0 = v$

$H_i \leftarrow h(M_i, H_{i-1}),\ i=1,2,\ldots N$

$h(M^n) = H_N$

v- начальный (стартовый) вектор

Функция сжатия



Алгоритм вычисления функции сжатия

1-й этап.

Генерация четырех 256 битных ключей K_1, K_2, K_3, K_4

$K_j=A_jM+C_j$, $j=1,2,3,4$.

A_j- блочная матрица, C_j – вектор (константа).

2-й этап.

Зашифрование четырех 64-битных слов на этих ключах:

$f_j=E(h_j,K_j)$, $j=1,2,3,4$, где h_j – 64-битный подблок 256 –битного блока хэш-функции, вычисленного на предыдущем шаге.

Формирование 256- блока криптограммы $f=f_1 | f_2 | f_3 | f_4$

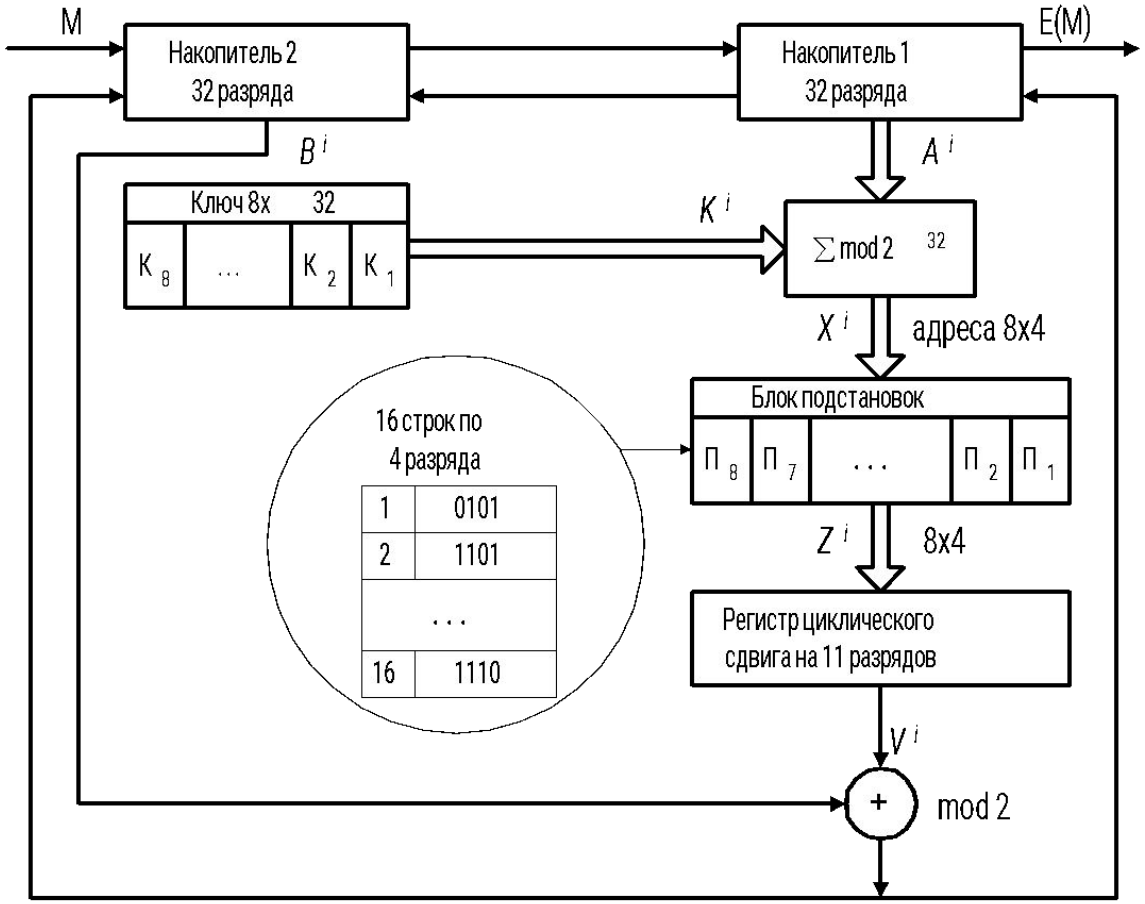
3-й этап. Перемешивание блока сообщения, результата шифрования и предыдущего значения хэш-кода.

$$H_i=\Psi^{61}(H_{i-1}\oplus\Psi(M_i\oplus\Psi^{12}(f_i))),$$

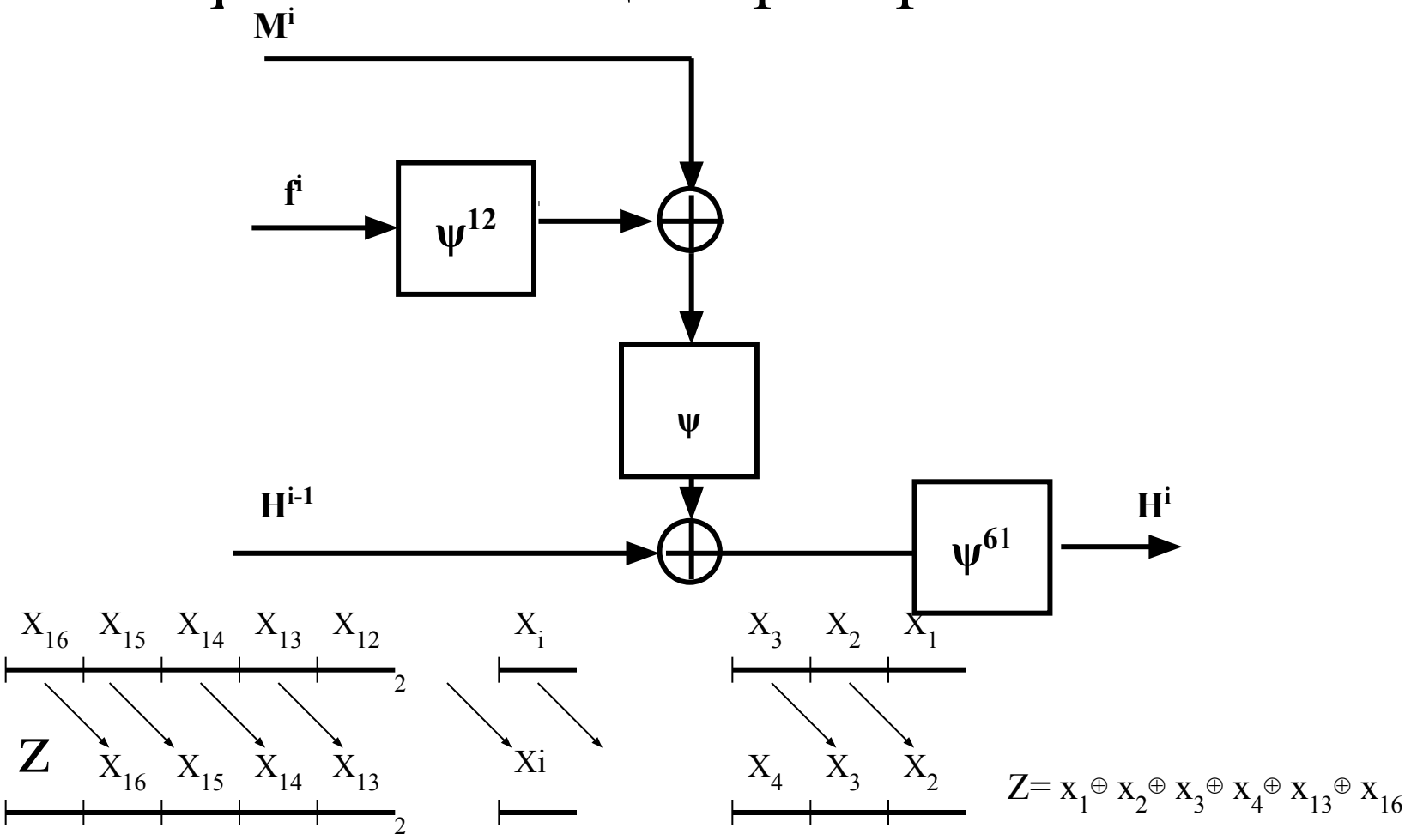
где Ψ^r – обозначает r -кратное применение перемешивающего преобразования Ψ.

$\Psi: \{0,1\}^{256} \rightarrow \{0,1\}^{256}$

Алгоритм шифрования согласно ГОСТ 28147-89



Перемешивающее преобразование



Пусть $X = x_{16} \mid x_{15} \mid x_{14} \mid \ldots \mid x_2 \mid x_1 \mid$, где x_i –16-битные блоки.

Тогда

$\Psi(X) = x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_{13} \oplus x_{16} \mid x_{16} \mid x_{15} \mid x_{14} \mid \ldots \mid x_2 \mid$

2. Определение, классификация, основные свойства ЭЦП

Подпись – собственноручно написанная фамилия.

Толковый словарь русского языка.

С.И. Ожегов, Н.Ю. Шведова

Свойства подписи на бумаге

1. Сформировать подпись может только ее автор. (подпись уникальна)
2. Проверить подпись может каждый, имеющий образец подписи.
3. Подпись трудно подделать.
4. Подпись неоспорима, автор не может отказаться от подписи.
5. Документ с подписью неизменяем.
6. Подпись неотделима от документа.

Основные понятия электронной подписи

Электронная подпись (ЭП) – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписавшего информацию.

ключ ЭП – уникальная последовательность символов предназначенная для создания электронной цифровой подписи.

ключ проверки ЭП – уникальная последовательность символов, однозначно связанная с ключем ЭП и предназначенная для проверки подлинности электронной подписи.

Свойства электронной подписи

1. Сформировать подпись может только обладатель закрытого ключа.
2. Проверить подпись может любой пользователь, имеющий открытый ключ.
3. Вероятность подделки подписи пренебрежительно мала.
4. Подпись неоспорима, пользователь не может отказаться от подписи.
5. Электронный документ неизменяем.
6. Подпись и подписанное сообщение могут передаваться и храниться отдельно.

Свойства электронной цифровой подписи (ЭЦП)

Свойства подписи на бумаге

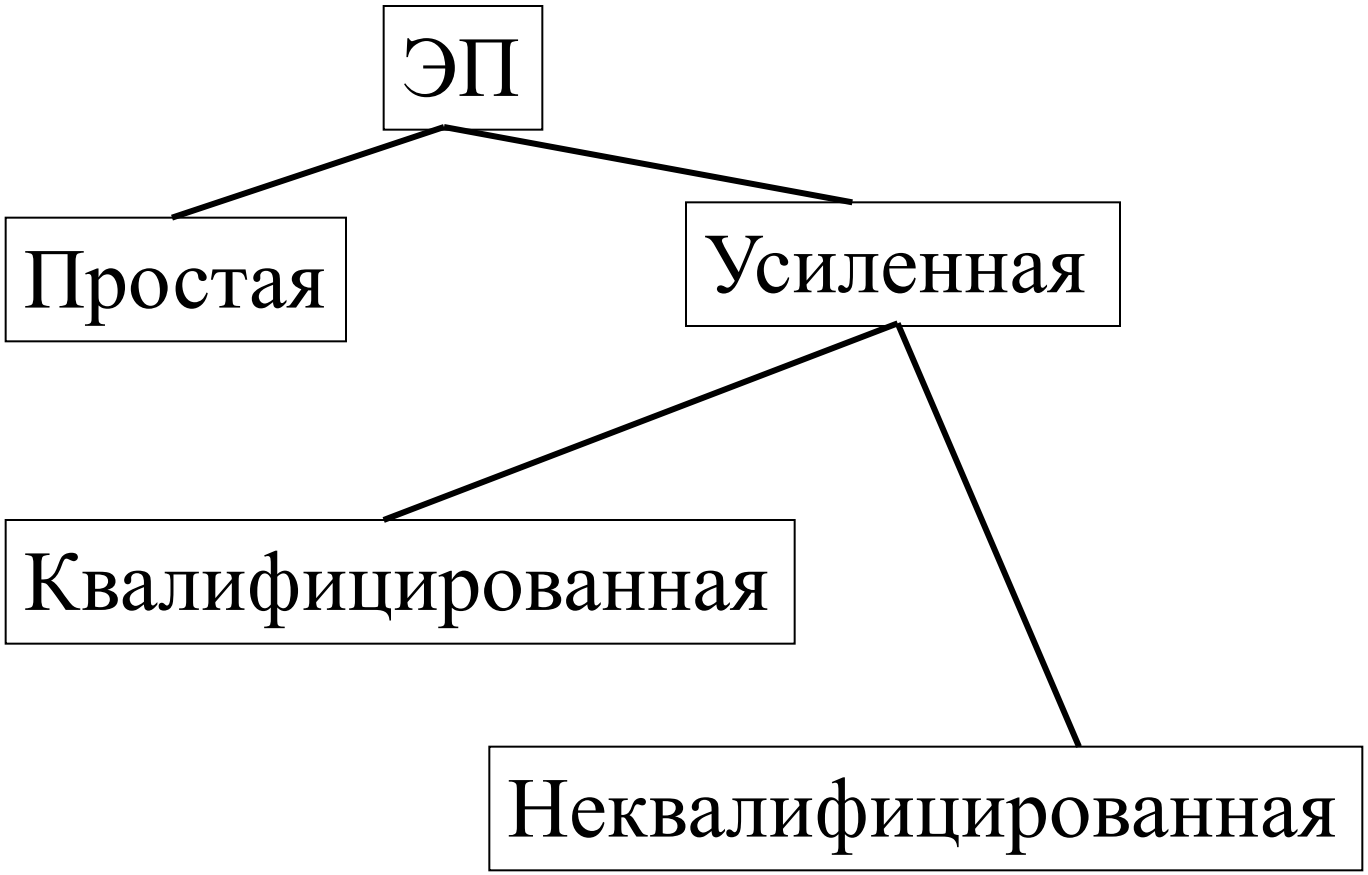
1. Сформировать подпись может только ее автор.
2. Проверить подпись может каждый , имеющий образец подписи.
3. Подпись трудно подделать.
4. Подпись неоспорима, автор не может отказаться от подписи.
5. Документ с подписью неизменяем.
6. Подпись неотделима от документа.

Свойства ЭЦП

1. Сформировать подпись может только обладатель закрытого ключа.
2. Проверить подпись может любой пользователь, имеющий открытый ключ.
3. Вероятность подделки подписи пренебрежительно мала.
4. Подпись неоспорима, пользователь не может отказаться от подписи.
5. Электронный документ неизменяем.
6. Подпись и подписанное сообщение могут передаваться

Виды электронных подписей

(Согласно Закону РФ от 6 апреля 2011г. N 63-ФЗ. Об электронной подписи)



- Простая ЭП – подпись, которая путем использования кодов, паролей или иных средств подтверждает факт формирования ЭП определенным лицом.

Неквалифицированная ЭП

- Получена в результате криптографического преобразования информации с использованием ключа ЭП;
- Позволяет определить лицо, подписавшее документ;
- Позволяет обнаружить факт внесения изменений в ЭД;
- Создается с использованием средств ЭП;

Квалифицированная ЭП

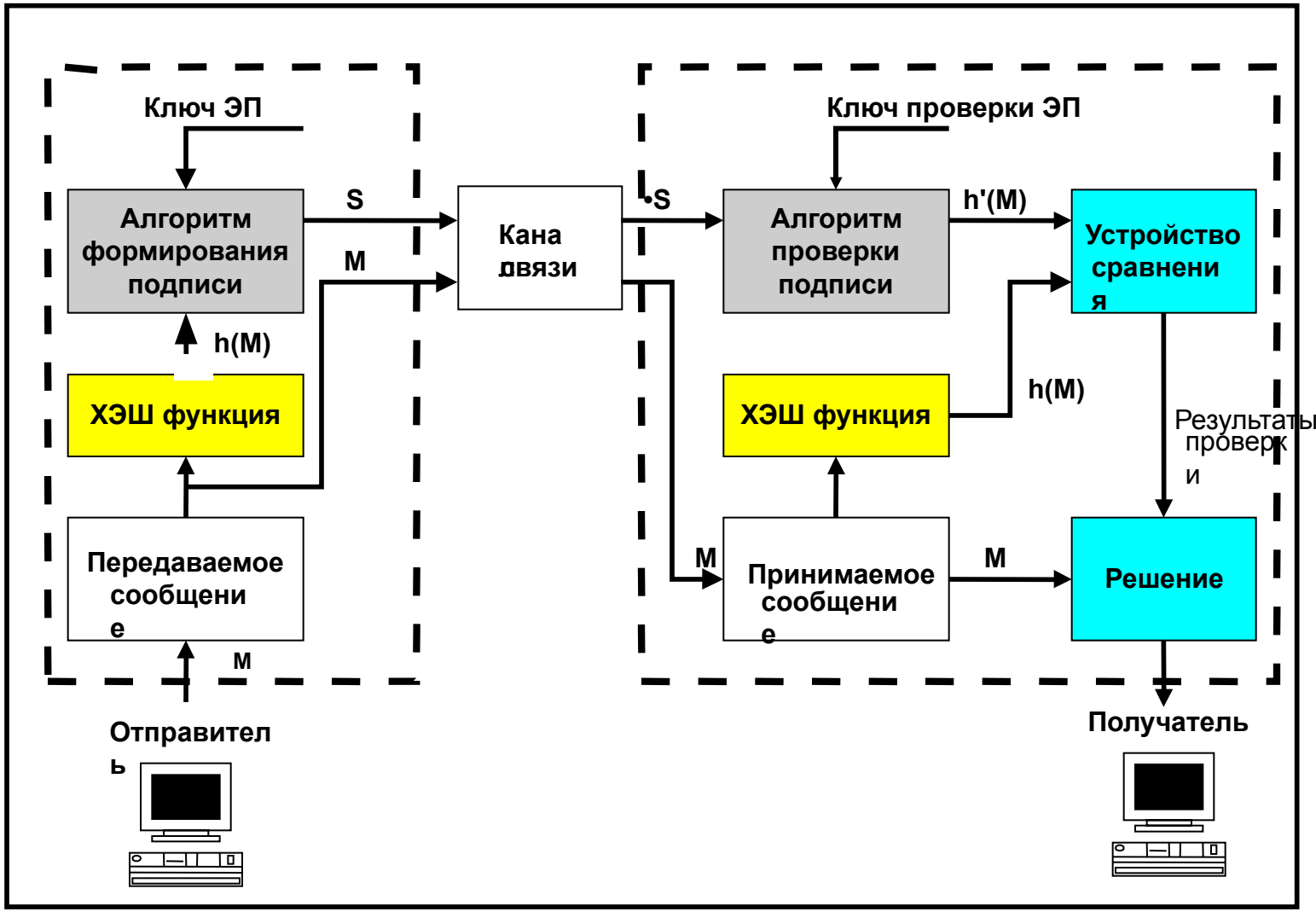
- 1. Соответствует всем признакам неквалифицированной ЭП;
- 2. Ключ проверки ЭП указан в квалифицированном сертификате.
- 3. Для создания и проверки ЭП используются средства ЭП, получившие подтверждение соответствия в соответствии с законом об ЭП.

Основные понятия ЭП

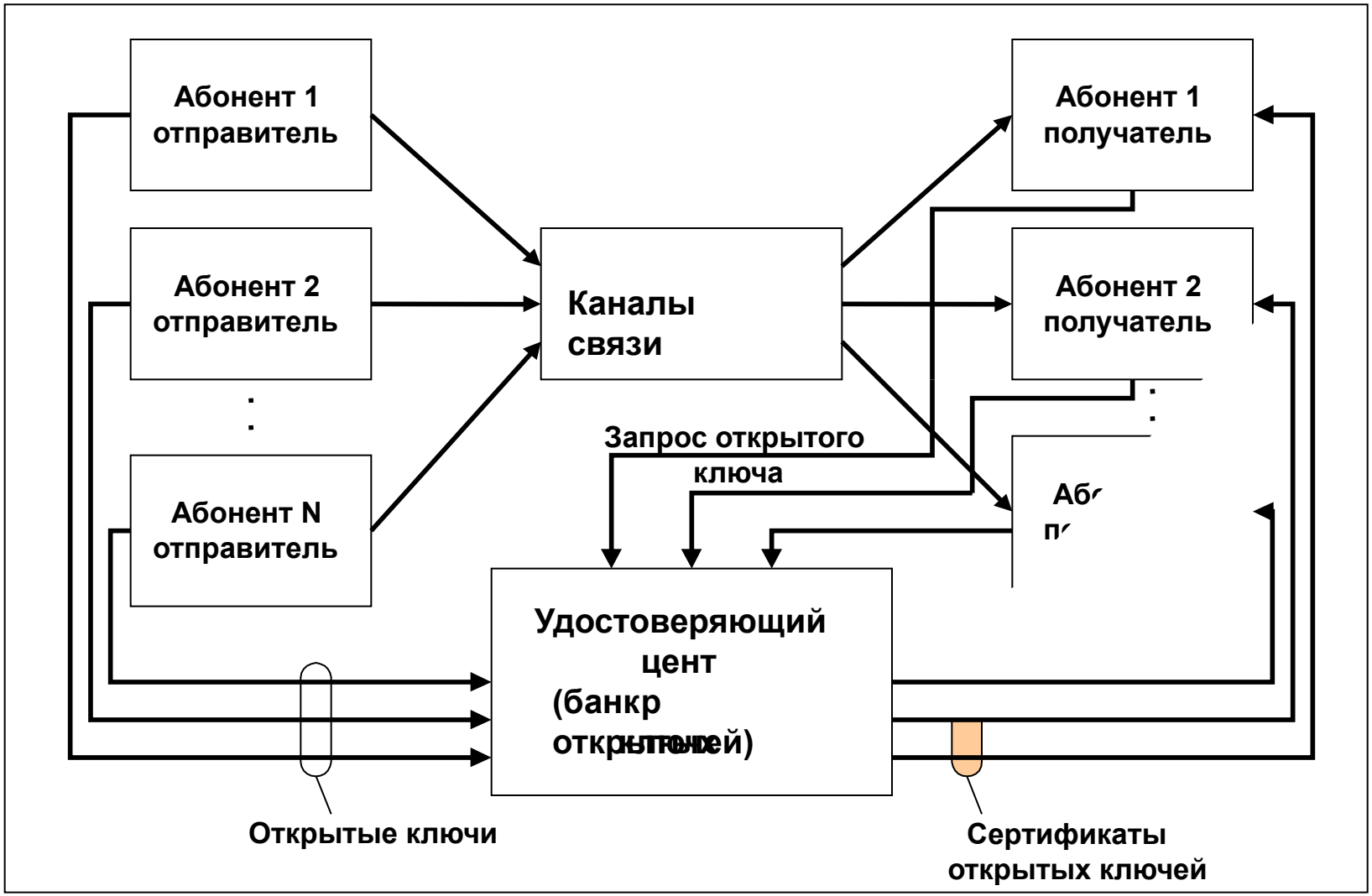
Сертификат ключа проверки электронной подписи - электронный документ или документ на бумажном носителе, выданные удостоверяющим центром и подтверждающие принадлежность ключа проверки ЭП владельцу сертификата клоча проверки ЭП

Владелец сертификата ключа проверки ЭП – лицо, которому в установленном законом порядке выдан сертификат ключа проверки ЭП

Модель ЭЦП


Ключ ЭП
Алгоритм формирования подписи
S
M
Кана
двязи
S
Ключ проверки ЭП
Алгоритм проверки подписи
h'(M)
Устройство сравнени
я
h(M)
ХЭШ функция
ХЭШ функция
h(M)
Результаты проверк
и
Передаваемое сообщени
е
M
M
Принимаемое сообщени
е
M
Решение
M
Отправител
ь
Получатель

Распределение открытых ключей



ПРАВОВЫЕ ДОКУМЕНТЫ ОБ ЭЛЕКТРОННОЙ ПОДПИСИ

1. Закон РФ от 6 апреля 2011г. N 63-ФЗ. Об электронной подписи.
2. ГОСТ Р34.11-94. Информационная технология. Криптографическая защита информации. Функция хэширования.
3. ГОСТ Р34.10-94. Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки цифровой подписи на базе асимметричного криптографического алгоритма.
4. ГОСТ Р34.10-01. Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки цифровой подписи на базе асимметричного криптографического алгоритма.

Хронология развития систем ЭЦП

- **1976 г. – открытие М. Хэлменом и У. Диффи асимметричных криптографических систем;**
- **1978 г. – Р. Райвест, А. Шамир, Л. Адельман – предложили первую систему ЭЦП, основанную на задаче факторизации большого числа;**
- **1985 г. – Эль Гамаль предложил систему ЭЦП, основанную на задаче логарифмирования в поле чисел из *p* элементов;**
- **1991 г.- Международный стандарт ЭЦП ISO/IEC 9796 (вариант РША);**
- **1994 г. – Стандарт США FIPS 186 (вариант подписи Эль Гамаля);**
- **1994 г. – ГОСТ Р 34.10-95 (вариант подписи Эль Гамаля);**
- **2000 г. – Стандарт США FIPS 186 – 2;**
- **2001 г. – ГОСТ Р 34.10-01 (ЭЦП на основе математического аппарата эллиптических кривых).**

Разновидности ЭЦП (теоретические разработки)

1. Неоспоримая ЭЦП (для проверки ЦП необходимо участие подписавшего лица).

2. Групповая ЭЦП (владелец подписи является анонимным членом группы).

3. Слепая подпись (подпись электронного документа без ознакомления с его содержанием).

4. Одновременный обмен секретами (пользователь передает другому пользователю свой секрет при одновременном получении от него его секрета)

5. Коллективная подпись. В подписании документа участвуют несколько лиц. Проверка подписи- одно лицо.

Система ЭЦП Эль-Гамаля (1985г.)

Пусть p -простое число; a - примитивный элемент GF(p).

Генерирование ключей

A - генерирует число x_A, $1< x_A <p-2$

вычисляет открытый ключ

$y_A=a^x \pmod p$.

(SK= x_A , PK= y_A). y_A передается корр. B.

Подписание сообщения

Пусть корр. A хочет послать корр.B подписанное сообщение M.

1.Корр. A осуществляет хэширование M m=h(M), m<p.

2. Генерирует случайное число 1<k<p-2.

3. Формирует первую часть подписи

$r=a^k \pmod p$,

4. Находит вторую часть подписи

$s=k^{-1} \cdot (m-xr) \pmod{p-1}$, $kk^{-1}=1 \pmod{(p-1)}$

5, Отправляет корр. B (M,(r,s)).

Система ЭЦП Эль-Гамаля (1985г.)

Проверка подписи

1.Корр. В осуществляет хэширование принятого сообщения M’ m’=h(M’)

2. Проверяет выполнение сравнения

$y^r r^s (mod p) = a^{m'} (mod p)$

3. Если сравнение выполняется, то подпись верна.

Проверка обратимости преобразований

$a^{xr}\, a^{ks} (mod p) = a^{xr+ks} (mod p) =$ $a^{xr+kk^{-1}(m-xr)} (\mathrm{mod}\ p) = a^m (\mathrm{mod}\ p)$

$$s=k^{-1} \cdot (m-xr)(modp-1),$$

Пример ЭЦП

Общесистемные параметры: p=11, a=2

Генерирование ключей: случайно генерируем x=3 – закрытый ключ;
Находим $y=a^x(\mathrm{mod}p)= 2^3(\mathrm{mod}11)= 8$, y=8 – открытый ключ

Формирование подписи:
Пусть хэшированное сообщение m=4.
Случайно генерируем число k=7.
Находим первую часть подписи $r=a^{k(}\mathrm{mod}p)=2^7(\mathrm{mod}11)=7$, $k^{-1}=3$,т.к
$k\,k^{-1}=1(\mathrm{mod}10)$
Находим вторую часть подписи $s=k^{-1}(m -xr)(\mathrm{mod}p-1)$
$=3(4-3*7)(\mathrm{mod}10)=9$
Подпись (r=7,s=9).

Проверка подписи.
Проверяем выполнение сравнения
$y^r r^s(\mathrm{mod}p)=a^{m'}(\mathrm{mod}p)$. $y^r r^s(\mathrm{mod}p)=8^7 7^9(\mathrm{mod}11)=2*8(\mathrm{mod}11)=5$
$a^{m'}(\mathrm{mod}p)=2^4=16(\mathrm{mod}11)=5$
Подпись верна.

Быстрое возведение в степень методом Д. Кнута

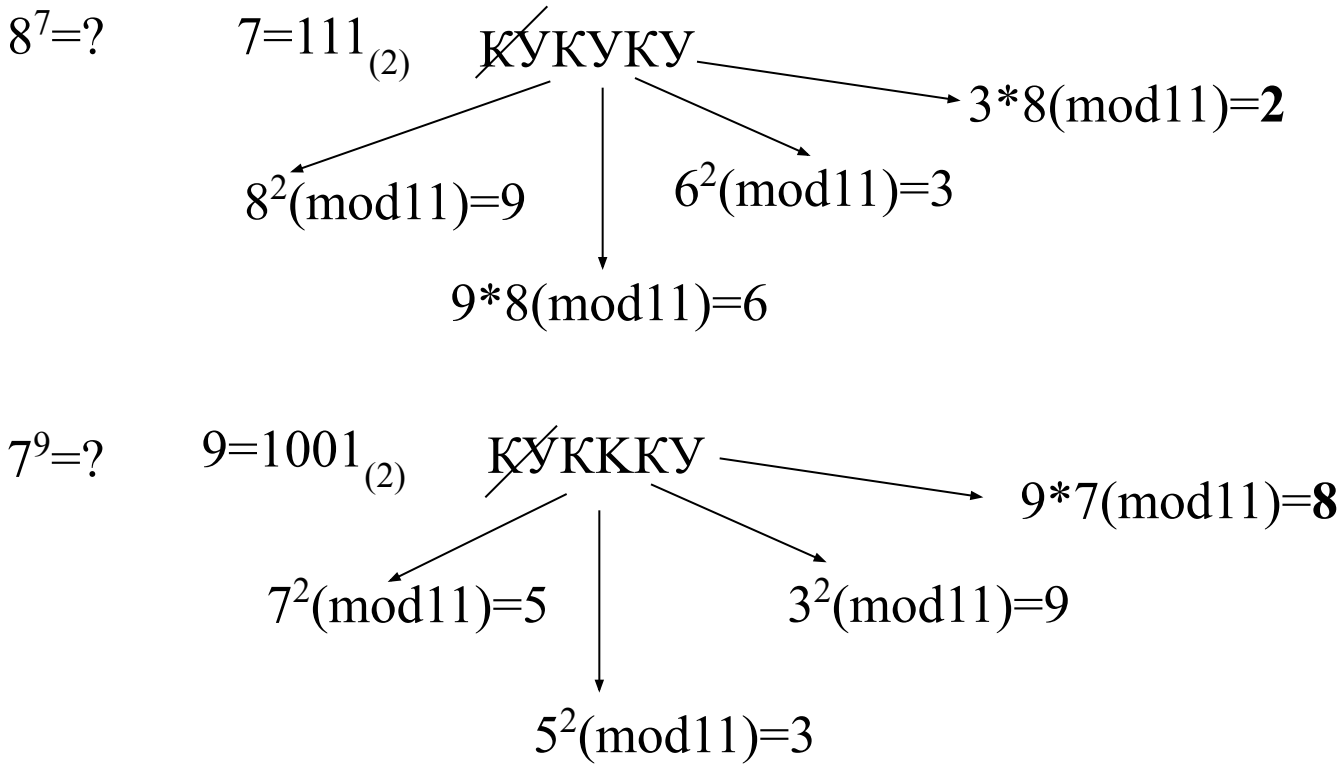


Схема ЭЦП РША

Генерирование ключей.

Случайно выбираются два простых числа p и q

Находится модуль N=pq. Находится функция Эйлера $\phi(N)= (p-1)(q-1)$

Выбираем число e такое, что НОД(e, $\phi(N)$)=1. Находим d, как обратный элемент к e $de=1(\mathrm{mod}\ \phi(N))$.

Объявляем d=SK, (e,N)=PK. PK сообщается всем корреспондентам.

Формирование подписи.

Корр. А хэширует сообщение M m=h(M).

Используя свой закрытый ключ d подписывает m $s=m^d(\mathrm{mod}N)$.

Передает корр. B (M,s)

Проверка подписи.

Корр. B хэширует сообщение M m'=h(M)

Используя открытый ключ, корр.A осуществляет проверку подписи, вычисляя $m=s^e(\mathrm{mod}N)$.

Сравнивая m и m' принимает решение о верности подписи.

2.2. Алгоритм шифрования Эль-Гамаля

Пусть p -простое число; a - примитивный элемент.

Генерирование пары открытых ключей (SK= x_A , PK= y_A).
A - генерирует число x_A,
вычисляет открытый ключ
$y_A=a^x$ (modp). y_A передается корр.
B.

Шифрование сообщения
Пусть корр. B хочем послать корр.A
сообщение m<p.
Генерирует случайное число k<p.
Формирует криптограмму E=(c_1c_2)
$c_1=a^k$(modp), $c_2=m\cdot(y_A^{-1})^k$.
Отправляет E корр. A.

Система шифрования Эль-Гамаля

Расшифрование сообщения.

Корр.А вычисляет $c_1^x \pmod p = a^{kx} \pmod p$,

Затем находит

$c_2 a^{kx} \pmod p = m \cdot (y_A^{-1})^k a^{kx} \pmod p = m \cdot a^{-xk} a^{kx} \pmod p = m$

Замечание.

Как найти y_A^{-1} ?

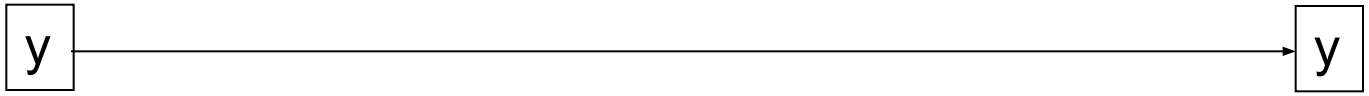
$y_A^{p-2} \pmod p = y_A^{p-1} \pmod p \cdot y_A^{-1} \pmod p = y_A^{-1} \pmod p$

Пример системы Эль-Гамаля

p=11, a=4, a- примитивный элемент $GF(2^p)$

Пусть x=3 – закрытый ключ

$y=4^3(mod11)=64(mod11)=9$ открытый ключ



Шифрование сообщения m=6

Генерирование СЧ k=4

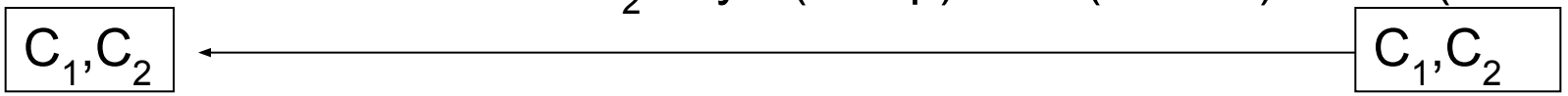
Вычисление:

$C_1=a^k(modp)=4^4(mod11)=256(mod11)=3$

$y^{-1}=y^{p-2}(modp)= 9^9(mod11)=9^29^29^29^29(mod11)=$

$4*4*4*4*9(mod11)=5*5*9(mod11)=5$

$C_2=my^{-1k}(modp)=6*5^4(mod11)=6*3*3(mod11)=10$



Расшифрование

$C_1^x (modp)=3^3(mod11)=5$

$C_2*C_1^x (modp)=10*5 (mod11)=50(mod11)=\mathbf{6}$

Система ЭЦП Эль-Гамаля (1985г.)

Пусть p -простое число; a - примитивный элемент GF(p).

Генерирование ключей

A - генерирует число x_A, $1< x_A <p-2$

вычисляет открытый ключ

$y_A=a^x \pmod p$.

(SK= x_A , PK= y_A). y_A передается корр. B.

Подписание сообщения

Пусть корр. A хочет послать корр.B подписанное сообщение M.

1.Корр. A осуществляет хэширование M m=h(M), m<p.

2. Генерирует случайное число 1<k<p-2.

3. Формирует первую часть подписи

$r=a^k \pmod p$,

4. Находит вторую часть подписи

$s=k^{-1} \cdot (m-xr) \pmod{p-1}$, $kk^{-1}=1 \pmod{(p-1)}$

5, Отправляет корр. B (M,(r,s)).