

СТАНДАРТ ЭЛЕКТРОННО-
ЦИФРОВОЙ ПОДПИСИ ГОСТ Р
34.10 РАЗЛИЧИЯ ВЕРСИЙ 94 И
12 ГОДОВ.

Терешкина Марина МЗО-425Бк-18

Введение

- Одним из эффективных направлений защиты информации является криптография (криптографическая защита), широко применяемая в различных сферах деятельности в государственных и коммерческих структурах.

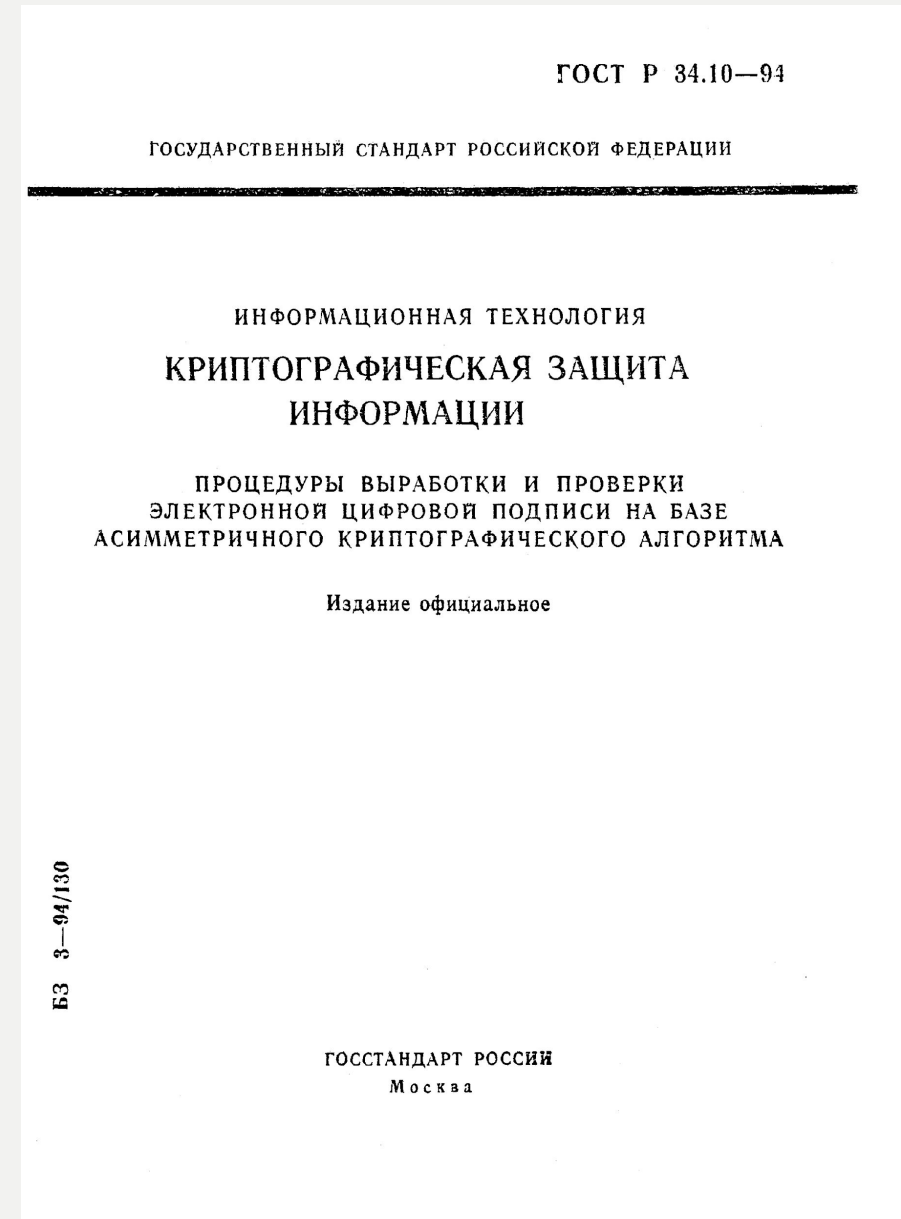
История

- США можно считать родиной ЭП: в 1976 году американскими криптографами Уитфилдом Диффи и Мартином Хеллманом было впервые предложено понятие «электронная цифровая подпись», хотя они всего лишь предполагали, что схемы ЭЦП могут существовать.



ГОСТ Р 34.10-94

- ГОСТ Р 34.10-94 — российский стандарт, описывающий алгоритмы формирования и проверки электронной цифровой подписи.



Область применения

Цифровая подпись позволяет:

- Аутентифицировать лицо, подписавшее сообщение;
- Контролировать целостность сообщения;
- Защищать сообщение от подделок;
- Доказать авторство лица, подписавшего сообщение.

Общее назначение

Использование ЭП предполагается для осуществления следующих важных направлений в электронной экономике:

- Полный контроль целостности передаваемого электронного платежного документа.
- Эффективная защита от изменений (подделки) документа.
- Фиксирование невозможности отказа от авторства данного документа.
- Формирование доказательств подтверждения авторства документа.

Основные соотношения

- p - простое число, $2^{509} < p < 2^{512}$ либо $2^{1020} < p < 2^{1024}$.
- q - простое число, $2^{254} < q < 2^{256}$ и q является делителем для $(p-1)$
- a - целое число, $1 < a < p-1$, при этом $aq \pmod p = 1$.
- k - целое число, $0 < k < q$.
- d - наименьшее целое число, не меньше, чем d .
- d - наименьшее целое число, не большее, чем d
- $e := g$ - присвоение параметру e значения g .
- x - секретный ключ пользователя для формирования подписи $0 < x < q$.
- y - открытый ключ пользователя для проверки подписи. $y = a^x \pmod p$.

Алгоритм выработки подписи

■ Процедура подписи сообщения включает в себя следующие этапы:

- Вычислить $h(M)$ - значение хеш-функции h от сообщения M . Если $h(M) \pmod{q} = 0$, присвоить $h(M)$ значение $0^{255} 1$.
- Выработать целое число k , такое, что $0 < k < q$.
- Вычислить два значения: $r = a^k \pmod{p}$ и $r' = r \pmod{q}$. Если $r' = 0$, перейти к этапу 2 и выработать другое значение числа k .
- С использованием секретного ключа x пользователя (отправителя сообщения) вычислить значение $s = (xr' + kh(M)) \pmod{q}$. Если $s = 0$, перейти к этапу 2, в противном случае закончить работу алгоритма.
- Подписью сообщения M является вектор $\langle r' \rangle_{256} \parallel \langle s \rangle_{256}$.

Процедура проверки подписи

Процедура проверки включает в себя следующие этапы:

- Проверить условие: $0 < s < q$ и $0 < r' < q$. Если хотя бы одно из этих условий не выполнено, то подпись считается недействительной.
- Вычислять $h(M1)$ - значение хеш-функции h от полученного сообщения $M1$. Если $H(M1) \pmod q = 0$, присвоить $h(M1)$ значение $0^{255} 1$.
- Вычислить значение $v = (h(M1))^{q-2} \pmod q$
- Вычислить значения: $z_1 = sv \pmod q$ и $z_2 = (q - r') v \pmod q$
- Вычислить значение $u = (a^{z_1} y^{z_2} \pmod p) \pmod q$
- Проверить условие: $r' = u$.