26. Сутність алгоритму ЕЦП, що ґрунтується на перетвореннях в скінченному полі Галуа (DSA) та його застосування?

DSA (Digital Signature Algorithm) — алгоритм с использованием открытого ключа для создания электронной подписи, но не для шифрования. Секретное создание хеш-значения и возможность её публичной проверки означает, что только один субъект может создать хеш-значение сообщения, но любой может проверить её корректность. Основан на вычислительной сложности взятия логарифмов в конечных полях.

Алгоритм был предложен Национальным Институтом Стандартов и Технологий (США) в августе 1991 и является запатентованным U.S. Patent 5231668 (англ.), но НИСТ сделал этот патент доступным для использования без лицензионных отчислений.

Для подписывания сообщений необходима пара ключей — открытый и закрытый. При этом закрытый ключ должен быть известен только тому, кто подписывает сообщения, а открытый — любому желающему проверить подлинность сообщения. Также общедоступными являются параметры самого алгоритма.

1. Выбор хеш-функции H(x). Для использования алгоритма необходимо, чтобы подписываемое сообщение являлось числом. Хеш-функция должна преобразовать любое сообщение в число
2. Выбор большого простого числа q, размерность которого в битах совпадает с размерностью в битах значений хэш-функции H(x)
3. Выбор простого числа p, такого, что (p-1) делится на q. Размерность p задаёт криптостойкость системы. Ранее рекомендовалась длина в 1024 бита. В данный момент для систем, которые должны быть стойкими до 2010 (2030) года, рекомендуется длина в 2048 (3072) бита.
4. Выбор числа g такого, что его мультипликативный порядок по модулю p равен q. Для его вычисления можно воспользоваться формулой $g = h^{(p-1)/q} \mod p$, где h — некоторое произвольное число, $h \in (1; p-1)$ такое, что $g \neq 1$. В большинстве случаев значение h = 2 удовлетворяет этому требованию

Подпись сообщения

Подпись сообщения выполняется по следующему алгоритму:

1. Выбор случайного числа $k \in (0; q)$
2. Вычисление $r = (g^k \mod p) \mod q$
3. Вычисление $s = (k^{-1}(H(m) + x \cdot r)) \mod q$
4. Выбор другого k, если оказалось, что r=0 или s=0

Подписью является пара чисел (r, s)

Проверка подписи

Проверка подписи выполняется по алгоритму:

1. Вычисление $w = s^{-1} \mod q$
2. Вычисление $u_1 = (H(m) \cdot w) \mod q$

3. Вычисление $u_2 = (r \cdot w) \mod q$
4. Вычисление $v = ((g^{u_1} \cdot y^{u_2}) \mod p) \mod q$

Подпись верна, если v = r