**Алгоритм цифровой подписи DSA**

Алгоритм оперирует следующими параметрами:

– простое число длиной бит. и должно быть кратно 64;

– простое число, длиной 160 бит. делит ;

, где , такое что ;

число*,* меньшее ;

*;*

Также алгоритм использует криптографическую хэш-функцию.

Параметры являются публичными и могут использоваться всеми пользователями. Приватным ключом является параметр . Публичный ключ – параметр .

Алгоритм подписи сообщения .

1) Алиса: генерирует случайное число ;

2) Алиса: генерирует и . (Параметры являются подписью);

Алгоритм проверки подписи.

1) Боб:

Если , то подпись верна.