

## FIPS Publication Change Notice

### **FIPS PUB 186, *Digital Signature Standard (DSS)***

#### **Change No.: 1**

**Date of Change: 1996 December 30**

#### **Change Items:**

I. The following change is made to **Appendix 3.2 Algorithm for Precomputing one or more k and r Values:**

- Change from

"This algorithm can be used to precompute k, k-1, and r for m messages at a time.

Algorithm:"

- To

"This algorithm can be used to precompute k, k-1, and r for m messages at a time. Note that implementation of the DSA with precomputation may be covered by U.S. and foreign patents.

Algorithm:"

II. The following change replaces **Appendix 5, Example of the DSA**. This example has been changed for use with FIPS 180-1, *Secure Hash Standard (SHS)*:

---

## **APPENDIX 5. EXAMPLE OF THE DSA**

### **(Revised for use with FIPS 180-1)**

This appendix is for informational purposes only and is not required to meet the standard.

Let  $L = 512$  (size of  $p$ ). The values in this example are expressed in hexadecimal notation. The  $p$  and  $q$  given here were generated by the prime generation standard described in appendix 2 using the 160-bit SEED:

d5014e4b 60ef2ba8 b6211b40 62ba3224 e0427dd3

With this SEED, the algorithm found  $p$  and  $q$  when the counter was at 105.  $x$  was generated by the algorithm described in appendix 3, section 3.1, using the SHA-1 to construct  $G$  (as in appendix 3, section 3.3) and a 160-bit XKEY:

XKEY =

bd029bbe 7f51960b cf9edb2b 61f06f0f eb5a38b6

t =

67452301 EFCDAB89 98BADCFE 10325476 C3D2E1F0

$x = G(t, XKEY) \bmod q$

$k$  was generated by the algorithm described in appendix 3, section 3.2, using the SHA-1 to construct  $G$  (as in appendix 3, section 3.3) and a 160-bit KKEY:

KKEY =

687a66d9 0648f993 867e121f 4ddf9ddb 01205584

t =

EFCDAB89 98BADCFE 10325476 C3D2E1F0 67452301

$$k = G(t, \text{KKEY}) \bmod q$$

**Finally:**

$$h = 2$$

$$p =$$

8df2a494 492276aa 3d25759b b06869cb eac0d83a fb8d0cf7  
cbb8324f 0d7882e5 d0762fc5 b7210eaf c2e9adac 32ab7aac  
49693dfb f83724c2 ec0736ee 31c80291

$$q =$$

c773218c 737ec8ee 993b4f2d ed30f48e dace915f

$$g =$$

626d0278 39ea0a13 413163a5 5b4cb500 299d5522 956cefcb  
3bff10f3 99ce2c2e 71cb9de5 fa24babf 58e5b795 21925c9c  
c42e9f6f 464b088c c572af53 e6d78802

$$x =$$

2070b322 3dba372f delc0ffc 7b2e3b49 8b260614

$$k =$$

358dad57 1462710f 50e254cf 1a376b2b deaadfbf

$$k^{-1} =$$

0d516729 8202e49b 4116ac10 4fc3f415 ae52f917

M = ASCII form of "abc" (See FIPS PUB 180-1, Appendix A)

$$(\text{SHA-1})(M) =$$

a9993e36 4706816a ba3e2571 7850c26c 9cd0d89d

$$y =$$

19131871 d75b1612 a819f29d 78d1b0d7 346f7aa7 7bb62a85  
9bfd6c56 75da9d21 2d3a36ef 1672ef66 0b8c7c25 5cc0ec74  
858fba33 f44c0669 9630a76b 030ee333

$$r =$$

8bac1ab6 6410435c b7181f95 b16ab97c 92b341c0

$$s =$$

41e2345f 1f56df24 58f426d1 55b4ba2d b6dcd8c8

$$w =$$

9df4ece5 826be95f ed406d41 b43edc0b 1c18841b

$$u_1 =$$

bf655bd0 46f0b35e c791b004 804afcb8 8ef7d69d

$$u_2 =$$

821a9263 12e97ade abcc8d08 2b527897 8a2df4b0

$$g^{u_1} \bmod p =$$

51b1bf86 7888e5f3 af6fb476 9dd016bc fe667a65 aafc2753  
9063bd3d 2b138b4c e02cc0c0 2ec62bb6 7306c63e 4db95bbf  
6f96662a 1987a21b e4ec1071 010b6069

$y^{u^2} \bmod p =$

8b510071 2957e950 50d6b8fd 376a668e 4b0d633c 1e46e665  
5c611a72 e2b28483 be52c74d 4b30de61 a668966e dc307a67  
c19441f4 22bf3c34 08aebaf 0a4dbec7

$v =$

8bac1ab6 6410435c b7181f95 b16ab97c 92b341c0