B.2.1. MGF1

MGF1 is a mask generation function based on a hash function.

MGF1 (mgfSeed, maskLen)

Options:

Hash hash function (hLen denotes the length in octets of the hash function output)

Input:

mgfSeed seed from which mask is generated, an octet string
maskLen intended length in octets of the mask, at most 2^32 hLen

Output:

mask mask, an octet string of length maskLen

Error: "mask too long"

Steps:

1. If maskLen > 2^32 hLen, output "mask too long" and stop.

2. Let T be the empty octet string.

3. For counter from 0 to \ceil (maskLen / hLen) - 1, do the following:

   A. Convert counter to an octet string C of length 4 octets (see Section 4.1):

      C = I2OSP (counter, 4) .

   B. Concatenate the hash of the seed mgfSeed and C to the octet string T:

      T = T || Hash(mgfSeed || C) .

4. Output the leading maskLen octets of T as the octet string mask.

The object identifier id-mgf1 identifies the MGF1 mask generation function:

```
id-mgf1    OBJECT IDENTIFIER ::= { pkcs-1 8 }
```