Subtleties in implementing OAEP [M '00]

```
OAEP-decrypt(ct):
        error = 0;
        ........
        if  ( RSA^-1(ct) > 2^(n-1) )
              { error =1;  goto exit; }
        ........
        if  ( pad(OAEP^-1(RSA^-1(ct))) != "01000" )
              { error = 1;  goto exit; }
```