# Example from equation editor

Application Number:

Filing Date:

Appellants:

As per claim 3, Matyas, Jr. further explains:

wherein said seed comprises length which is less than a block size for said asymmetric private key (see column 3, lines 61-67; the random number seed Xp is such that it is greater than or equal to  and less than or equal to ; see column 4, lines 12-13; the private signature exponent, d, is greater than ).

**My equation:**

End of my equation.

## Text formula example from OA 10046224:

Claim 2 is objected to because of the following informalities: “(q is a prime factor…)”, “(10k1+k2 ….<p)”, “(|α1| = k1 , |α2| = k2)”, “(|m| = k3 where…)”. The parenthesis should be removed for the limitation to be given patentable weight. Appropriate correction is required.

Regarding claim 1, Cramer et al. teach a public-key cryptographic scheme comprising: a key generation step of generating a secret-key:

* x1, x2, y11, y12, y21, y22, z Zq (column 7, lines 10-19), and
* a public-key:
  + G, G': finite (multiplicative) group G G’,
  + q: prime number (the order of G),
  + g1,g2 G (column 6, lines 65-67, column 7, lines 1-10),
  + c= g1^x1 g2^x2, d1= g1^y11 g2^y12, d2= g1^y21 g2^y22, h= g1^z,
  + π : X1 x X2 x M → G’ : one-to-one mapping
  + π-1 : Im(π) → X1 x X2 x M (column 7, lines 20-27)