ERRATA do EP de MAC0336-5723 de 2012

2.2.2 Segunda parte de uma iteração

(((((((Parágrafo Inicial sem alterações – abaixo as alterações:)))))))

1. Inicialmente é calculado um valor intermediário chamado Y_1 da seguinte forma:

(a) $Y_1 = X_e \oplus X_f$

2. A seguir outros dois valores intermediários chamados Y_2 e Z são calculados:

(a) $Y_2 = [(k_e \odot Y_1) \boxplus Y_1] \odot k_f$

(b) $Z = (k_e \odot Y_1) \boxplus Y_2$

3. E os valores X'_e e X'_f são calculados da seguinte maneira:

(a) $X'_e = Z \oplus X_e$

(b) $X'_f = Z \boxplus X_f$