問5.3

256ビットの有限体上の楕円曲線暗号であるから Enc の定義域のサイズは、

k_2 = 32バイト、K は k_2=16バイトである。

$k = k_0 + k_1 + k_2$ となる必要があるから $k_0 + k_1 = 16$ である。

一方のバイト数が極端に小さいと、そこから攻撃がなされる可能性があるので、$k_0 = k_1 = 8$ とするのがよいと考える。