Prob42

let k = key len in bits

D = numeric val of {00 asn.1 hash}

t = len of D in bits

x = offset in bits from right

$N = 2^t - D$ should be a multiple of 3, tweak hash if necessary

Desired output

$\underbrace{00\ 01}_{15\text{ bits}}$ ff ff .. ff 00 asn.1 hash garbage

Achievable with

$2^{k-15} - 2^{k-x+t} + D2^{k-x}$ + garbage

where $2^{k-15} - 2^{k-x+t}$ gives 01 ff ff .. ff $\underbrace{00\ 00\ ..\ 00}_{k-x+t\text{ bits}}$

$D2^{k-x}$ gives $\underbrace{00\ \text{asn.1 hash}}_{D\text{ having }t\text{ bits}}$ $\underbrace{00\ 00\ ..\ 00}_{k-x\text{ bits}}$

and garbage being less than 2^{k-x+1} and so not impacting D

$$(A-B)^3 = A^3 - 3A^2B + 3AB^2 - B^3$$

let $A = 2^{\frac{k-15}{3}}$

$B = \frac{N}{3} 2^{k-x-2\left(\frac{k-15}{3}\right)}$ } induced from Finney's writeup

$$= 2^{k-15} - \cancel{2^{2\left(\frac{k-15}{3}\right)}} N 2^{k-x-2\left(\frac{k-15}{3}\right)} \cancel{+} \Big\} \alpha$$

$$+ \cancel{2^{\frac{k-15}{3}}} \frac{N^2}{3} 2^{2k-2x-\frac{4}{3}\left(\frac{k-15}{3}\right)} \Big\} \beta = \text{garbage}$$

$$- \frac{N^3}{27} 2^{3k-3x-6\left(\frac{k-15}{3}\right)}$$

$$\alpha = 2^{k-15} - N 2^{k-x} = 2^{k-15} - (2^t - D) 2^{k-x}$$

$$= 2^{k-15} - 2^{k-x+t} + D 2^{k-x} \quad \checkmark$$

$$\beta = \frac{N^2}{3} 2^{2k-2x-3\left(\frac{k-15}{3}\right)} - \frac{N^3}{27} 2^{3k-3x-6\left(\frac{k-15}{3}\right)} < 2^{k-x+1}$$

$2k-2x-k+15$

$k-2x+15$

~~Therefore so long as~~ [illegible] ~~$4 \le 5$~~