Note 1 1/30/2012

$$Q_1 = a^{p_b - 1} \bmod n$$

- Repeatedly compute

$$Q_i = ((Q_{i-1})^2 \bmod n)\, a^{p_b - i} \bmod n$$

↳ $i = 2$, $Q_2 = Q_1^2 \cdot a^{p_{b-2}} \bmod n$

$= a^{2p_{b-1} + p_{b-2}} \bmod n$

$k \approx 1.17\, m^{1/2}$ if $m = 1024 = 2^{10}$

$k = 1.17\sqrt{m} = 1.17 \times 2^5 = \underline{38}$

$\left(\frac{m-(i-1)}{m}\right) = 1 - \frac{i-1}{m}$