1.

Given the description, we know that :

$$[(M_1^{IK} \bmod n) \oplus M_2]^{IK} \bmod n = h$$

by RSA, the private key prv of $IK = IK^{-1} \bmod n$

$$\Rightarrow (M_1^{IK} \bmod n) \oplus M_2 = h^{prv} \bmod n$$

then we choose any random block N_2, for every N_2 we can find N_1 such that :

$$[(h^{prv} \bmod n) \oplus N_2]^{prv} \bmod n = N_1$$

i.e. we can find $H(N_1 N_2) = h$

$\Rightarrow$ it is not preimage resistant #

2. $f_0 = \sum_{x=0}^{7}\left[a_x \cdot \sin\frac{0\pi x}{4}\right] = 0$ #

$f_1 = \sum_{x=0}^{7}\left[a_x \cdot \sin\frac{\pi x}{4}\right] = \sin\frac{\pi}{4} + 3\sin\frac{3\pi}{4} + \sin\frac{5\pi}{4} + 3\sin\frac{7\pi}{4}$

$= \frac{\sqrt{2}}{2} + \frac{3\sqrt{2}}{2} - \frac{\sqrt{2}}{2} - \frac{3\sqrt{2}}{2} = 0$ #

$f_2 = \sum_{x=0}^{7}\left[a_x \cdot \sin\frac{\pi x}{2}\right] = \sin\frac{\pi}{2} + 3\sin\frac{3\pi}{2} + \sin\frac{5\pi}{2} + 3\sin\frac{7\pi}{2}$

$= 1 - 3 + 1 - 3 = -4$ #

$f_3 = \sum_{x=0}^{7}\left[a_x \cdot \sin\frac{3\pi x}{4}\right] = \sin\frac{3\pi}{4} + 3\sin\frac{9\pi}{4} + \sin\frac{15\pi}{4} + 3\sin\frac{21\pi}{4}$

$= \frac{\sqrt{2}}{2} + \frac{3\sqrt{2}}{2} - \frac{\sqrt{2}}{2} - \frac{3\sqrt{2}}{2} = 0$ #

3. $e \approx 2.71828$

$$\approx 2 + \cfrac{1}{\cfrac{1}{0.71828}}$$

$$\approx 2 + \cfrac{1}{1 + \cfrac{1}{\cfrac{1}{0.3922}}}$$

$$\approx 2 + \cfrac{1}{1 + \cfrac{1}{2 + 0.5497}}$$

$$\approx 2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + 0.8191}}}$$

$$\approx 2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{1 + 0.2208}}}}$$

$$\approx 2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{4 + 0.5289}}}}}$$

$$\approx 2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{4}}}}}$$

$$= \frac{87}{32} \quad \#$$

4. (a) calculate $\sum_{k=0}^{1023} [7^k \bmod 39]\, \omega^{-ky}$ for $y \in [0, 1023]$ by online tool

we find that $d_1 = 84$, $d_2 = 168$ .....

$\Rightarrow 7^{84} \bmod 39 = 1 \Rightarrow 7^{84} - 1 \equiv 0$

and $7^{42} \bmod 39 = 25$

$\Rightarrow (7^{42}+1)(7^{42}-1) \equiv 26 \cdot 24 \equiv 0$

$\Rightarrow p = \gcd(26, 39) = 13$

$q = \gcd(24, 39) = 3$

$\Rightarrow 39 = 13 \times 3$ #

(b) for $x \in \vec{f}$, which $x > 0.001$, there are 50 of them out of 122 whose denominator can be represented as $s = 12$,

and the probability is $\frac{50}{122} \fallingdotseq 0.4098$

#