1. Consider to use RSA with a known key IK to construct a cryptographic hash function H as follow: Encrypt the first block, XOR the result with the second block and encrypt again, etc. Then, the last ciphertext block is the hash value. For example,

$$\mathrm{H}(\mathrm{M}_1\mathrm{M}_2) = \mathrm{Enc}(\mathrm{IK}, \mathrm{Enc}(\mathrm{IK}, \mathrm{M}_1) \oplus M_2) = h.$$

Show that this H does not satisfy the property of second image resistance. That is, we can find $N_1$ and $N_2$ such that $H(N_1N_2)=h$.

$H(N_1N_2) = Enc(IK, Enc(IK, N_1) \oplus N_2)$

$= Enc(IK, Enc(IK, N_1) \oplus Enc(IK, N_1) \oplus Enc(IK, M_1) \oplus M_2)$

$= Enc(IK, Enc(IK, M_1) \oplus M_2)$

$= h$

2. Do convolution on the function $\sin 2\pi\left(\frac{f}{8}\right)x$ and the 8-sample vector $\vec{a} = [0\ 1\ 0\ 3\ 0\ 1\ 0\ 3]$ for f=0, 1, 2, 3.

f = 0: convolution with $\sin 2\pi(\frac{f}{8})x$ = [0 0 0 0 0 0 0 0 ] = 0

f = 1: convolution with $\sin 2\pi(\frac{f}{8})x = [0\ \ \frac{1}{\sqrt{2}}\ \ 0\ \ \frac{3}{\sqrt{2}}\ \ 0\ \ \frac{-1}{\sqrt{2}}\ \ 0\ \ \frac{-3}{\sqrt{2}}\ ] = 0$

f = 2: convolution with $\sin 2\pi(\frac{f}{8})x$ = [0 1 0 -3 0 1 0 -3 ] = -4

f = 3: convolution with $\sin 2\pi(\frac{f}{8})x = [0\ \ \frac{1}{\sqrt{2}}\ \ 0\ \ \frac{3}{\sqrt{2}}\ \ 0\ \ \frac{-1}{\sqrt{2}}\ \ 0\ \ \frac{-3}{\sqrt{2}}] = 0$

3. Use the continued fraction method to find a rational number to approximate e with accuracy up to 3 decimal digits under the decimal point.

e = 2.71828...

$$\approx 2 + \cfrac{1}{\cfrac{1}{0.71828}} \approx 2 + \cfrac{1}{1 + 0.39221} \approx 2 + \cfrac{1}{1 + \cfrac{1}{2 + 0.54925}}$$

$$\approx 2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + 0.8206}}} \approx 2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{1 + 0.21862}}}}$$

$$\approx 2 + \frac{51}{71}$$

4. Use the DFT method to factor M=39 by choosing a=7. We sample N=1024 points for $g(x) = a^x \bmod M$. Use an online tool or Matlab to compute DFT.
   a) Show all steps of computation.
   b) What is the probability of the frequencies of form $[\frac{kN}{s}]$ in the result of DFT, where k is an integer and s is the period of g(x).

a)

Prepare a vector x = [0,1,2…..1023]

Compute $g_{a,M}(x) = [a^0 \bmod M, a^1 \bmod M, a^2 \bmod M, \ldots\ldots, a^{1023} \bmod M]$ = [1, 7, 10, 31, 22, 37, 25, 19, 16, …..]

Compute and normalize $f = DFT(g_{a,M}(x)) \approx$ [0.1619 , 0 .0001, 0.0001 , 0.0001,……]

f[0] ≈ 0.1619, f[85] ≈ 0.0312, f[171] ≈ 0.0225 , f[341] ≈ 0.0223

D = [0, 85, 171, 341, 427, 512, 597, 683, 853, 939]

Compute z1 , z2 , …, zr denominators by continued fraction method for approximating d1/N, d2/N, ⋯, dr/N and get

s = 12.

M = p*q = gcd(25+1, 39)*gcd(25-1, 39) = 13 x 3 b)

N=1024, s=12

k=0 $\rightarrow$ f[0] = 0.162

k=1 $\rightarrow$ f[85] = 0.031

k=2 $\rightarrow$ f[171] = 0.022

k=3 $\rightarrow$ f[256] = 0.0002

k=4 $\rightarrow$ f[341] = 0.022

k=5 $\rightarrow$ f[427] = 0.013

k=6 $\rightarrow$ f[512] = 0.054

k=7 $\rightarrow$ f[597] = 0.013

k=8 $\rightarrow$ f[683] = 0.022

k=9 $\rightarrow$ f[768] = 0.002

k=10 $\rightarrow$ f[853] = 0.023

k=11 $\rightarrow$ f[939] = 0.031

Total probability of the frequencies of form $[\frac{kN}{s}]$ = 0.393