Introduction to Cryptography, 2021 Fall

Homework 4, due 4pm, 12/2/2021 (Thursday)

Part 1: Written Problems

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 lastciphertext 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 andN_2 such that $H(N_1N_2)=h$.

For arbitrary N_1, choose $N_2 = \mathrm{Enc}(\mathrm{IK}, \mathrm{N}_1) \oplus \mathrm{Enc}(\mathrm{IK}, \mathrm{M}_1) \oplus M_2$

$\mathrm{H}(\mathrm{N}_1\mathrm{N}_2) = \mathrm{Enc}(\mathrm{IK}, \mathrm{Enc}(\mathrm{IK}, \mathrm{N}_1) \oplus \mathrm{N}_2)$

$= \mathrm{Enc}(\mathrm{IK}, \mathrm{Enc}(\mathrm{IK}, \mathrm{N}_1) \oplus \mathrm{Enc}(\mathrm{IK}, \mathrm{N}_1) \oplus \mathrm{Enc}(\mathrm{IK}, \mathrm{M}_1) \oplus M_2)$

$= \mathrm{Enc}(\mathrm{IK}, \mathrm{Enc}(\mathrm{IK}, \mathrm{M}_1) \oplus M_2)$

$= \mathrm{h}$

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 : $\sum_{x=0}^{7} sin 2\,\pi \left(\frac{0}{8}\right) \mathrm{x} * \mathrm{a_x} = 0$

F = 1 : $\sum_{x=0}^{7} sin 2\,\pi \left(\frac{1}{8}\right) \mathrm{x} * \mathrm{a_x} = 0$

F = 2 : $\sum_{x=0}^{7} sin 2\,\pi \left(\frac{2}{8}\right) \mathrm{x} * \mathrm{a_x} = -4$

F = 3 : $\sum_{x=0}^{7} sin 2\,\pi \left(\frac{3}{8}\right) \mathrm{x} * \mathrm{a_x} = -1.77636e - 015$

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

e = 3 + 1/(-4 + 1/(2 + 1/5)) = 106/39 ≅ 2.718

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 $[\frac{kN}{s}]$ in the result of DFT, where k is an integer formand s is the period of g(x).**

(a)

Step 1:

Prepare a vector x = [0,1,2…..1023]

Step 2:

Compute $g_{a,M}(x)$

= [a^0 mod M, a^1 mod M, a^2 mod M,……, a^{1023} mod M]

= [1, 7, 10,…………]

Step 3:
Compute and normalize $f = DFT(g_{a,M}(x))$
$f \approx$ [0.1619 , 0 .0001, 0.0001 , 0.0001,……]
f[0] ≈0.1619, f[86] ≈0.0312, f[172] ≈ 0.0225 , f[342] ≈ 0.0223。
D=[0, 86, 172, 342, 428, 513, 598, 684, 854, 940]

Step 4:
Use "continued fraction" method to compute z1 , z2 , …, zr of denominators for approximating d1/N, d2/N, …, dr/N within 1/2N。
d1/N= 86/1024= 0.083984375 ≈1/12。
∴ period s = 12 。(a^s mod M = 1)

Step: 5:
S is even and $a^{s/2}$ mod M ≠ ±1 ，then gcd($a^{s/2}$±1,M) = p or q。
gcd(a^6+1,M)=gcd(117,650, 39)=13
gcd(a^6 -1,M)=gcd(117,648, 39)=3
∴ M=13 x 3

(b)
f[0] = 0.1619
f[86] = 0.0312
f[172] = 0.0225
f[342] = 0.0223
f[428] = 0.0133
f[513] = 0.0538
f[598] = 0.0133
f[684] = 0.0223
f[854] = 0.0225
f[940] = 0.0312

So, the total probability of the frequencies of $[\frac{kN}{s}]$ is 0.3718.