Problem 1

Assume the ciphertext is c*, the target is to get m

Send S(c*) which is equivalent to S(Enc(sk,m))=Enc(sk,m+1) to oracle

Then the oracle would send back m+1

(m+1)-1=m

Problem 2

1.

Assume two identical Vigenère cipher are "ABC"

There would be such possibilities

Choice	A	B	C
1	L	U	C
2	K	L	U
3	C	K	L
4	U	C	K

There would be 4*4 possibilities and only 4 of them would have the same plaintext, that is when the two ciphertexts have the same choices (1-1,2-2,3-3,4-4)

Therefore, probability of two 3-letter strings having different plaintexts for a given Vigenere cipher would be (16-4)/16=3/4

2

Since we’ve already known

$\Delta \equiv 0$ (mod m)

Let $\Delta1=m*x1$

$\Delta2=m*x2$

…

Where x1,x2… are integer

Then $\gcd(\Delta1, \Delta2\ldots)=m*\gcd(x1,x2\ldots)$

Therefore, m divides $\gcd(\Delta1, \Delta2\ldots)$

Problem 3

	0	1	2	3	4	5
0	0≡ 0 (mod6)	1≡ 1 (mod6)	2≡ 2 (mod6)	3≡ 3 (mod6)	4≡ 4 (mod6)	5≡ 5 (mod6)
1	1≡ 1 (mod6)	2≡ 2 (mod6)	3≡ 3 (mod6)	4≡ 4 (mod6)	5≡ 5 (mod6)	6≡ 0 (mod6)
2	2≡ 2 (mod6)	3≡ 3 (mod6)	4≡ 4 (mod6)	5≡ 5 (mod6)	6≡ 0 (mod6)	7≡ 1 (mod6)
3	3≡ 3	4≡ 4	5≡ 5	6≡ 0	7≡ 1	8≡ 2 (mod6)

	(mod6)	(mod6)	(mod6)	(mod6)	(mod6)	
4	4≡ 4 (mod6)	5≡ 5 (mod6)	6≡ 0 (mod6)	7≡ 1 (mod6)	8≡ 2 (mod6)	9≡ 3 (mod6)
5	5≡ 5 (mod6)	6≡ 0 (mod6)	7≡ 1 (mod6)	8≡ 2 (mod6)	9≡ 3 (mod6)	10≡4(mod6)

Pr[D1=x] (for 0<=x<=5) =1/6

a)

Pr [D1=x, S1=y] (for 0 ≤ x ≤ 5 and 0 ≤ y ≤ 10 and y-x<=5) =1/6*1/6=1/36

Pr [D1=x, S1=y] (for 0 ≤ x ≤ 5 and 0 ≤ y ≤ 10 and y-x>5) =0 because the value for the second dice cannot be more than 5.

b)

Pr [D2=x, S2=y] (for 0 ≤ x ≤ 5 and 0 ≤ y ≤ 5) =1/6*1/6=1/36

c)

Pr[S1 = s|D1 = i] for 0 ≤ i ≤ 5 and 0 ≤ s ≤ 10

When i-s>5: Pr[S1 = s|D1 = i]=0

When i-s<=5: Pr[S1 = s|D1 = i]=(1/36)/(1/6)=1/6 d)

P r[D1 = i|S2 = s] (for $0 \le i \le 5$ and $0 \le s \le 5$) = 1/6

e)

D1 and S1 are not independent

Because

When x=1,y=10, Pr[x,y] = 0 which is not equal to Pr[x]P[y]=1/6*1/36

f)

D1 and S2 are independent

Because Pr[x,y] = Pr[x]P[y]=1/6*1/6=1/36, for all($0 \le x \le 5$ and $0 \le y \le 5$)

Problem 4

1)

91=7*13=(6+1)*(12+1)

6*12=72

ed mod 72=1

$e=5$

$72+1=73$

$72*2+1=145=5*29$

Therefore, $d=29$

2) $Enc(pk, M1)=M^e \bmod n=8*8*8*8*8 \bmod 91= 8$

3) $Sign(sk, M2)= M^d \bmod N=17^{29} \bmod 91=75$

Problem 5

By contraposition, if a implies b, then (not b) implies (not a),

therefore, if we can find an attack in the CPA game if the encryption is deterministic

then we can prove IND-CPA implies that the encryption is randomized

Assume the encryption is deterministic in the CPA game. That implies the challenger would always choose b=0 or 1. The adversary would try if it is 0 or 1 at the first time. Then, he would know if he is right or not. And no matter it is true or not, he would know it to always win the game in the future. That is how the attack works.

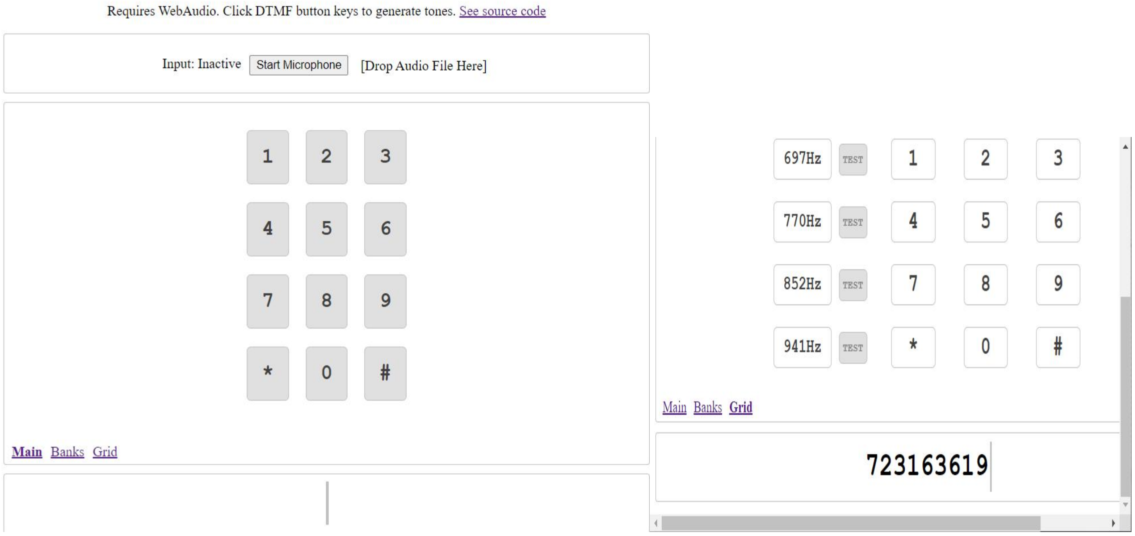
Therefore, IND-CPA implies that the encryption is randomized

Problem 6

Part A

Use the website below to generate the tone:

https://unframework.github.io/dtmf-detect/



Requires WebAudio. Click DTMF button keys to generate tones. See source code

Input: Inactive

723163619

Then I got the number:

723163619

Part B

I used the number as a password to open the secret file. The file is in hex(obviously). So, I converted it with ASCII

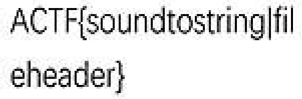
In the file, I found it a PNG file so I change the name of the file with”.png”. Then I see the picture:

Welcome to
ACTF

PART C

Compare the hex code between the png file and jpg file. I find they both have “ddf8” inside.

Delete everything in front of “ddf8”, then I got the jpg version.



ACTF{soundtostring|fil
eheader}

Therefore, the string should be:

“soundtostring[fileheader]”