**Play Nice**

nc mercury.picoctf.net 6057

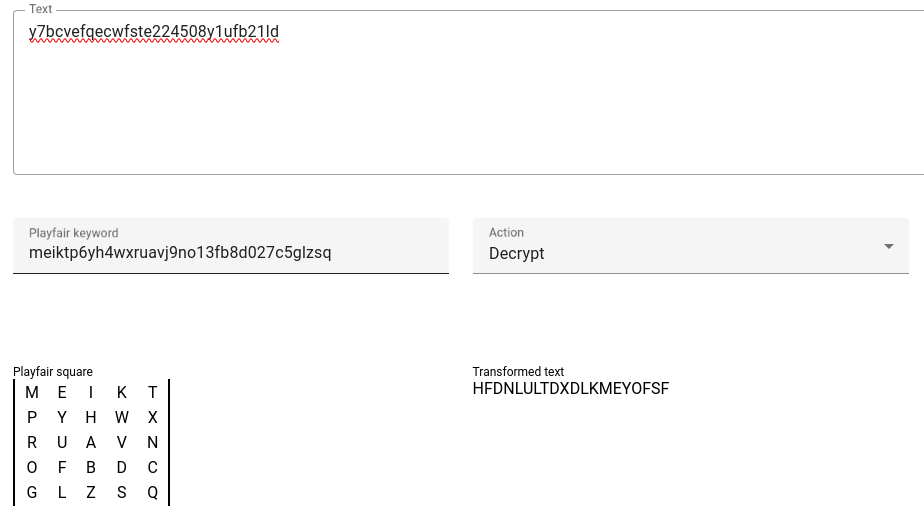
-->

Here is the alphabet: meiktp6yh4wxruavj9no13fb8d027c5glzsq

Here is the encrypted message: y7bcvefqecwfste224508y1ufb21ld

What is the plaintext message?

Using Playfair decoder with these alphabet and encrypted message to find the plaintext:



--> Plaintext: “hfdnlultdxdlkmeyofsf”

--> Flag: “2e71b99fd3d07af3808f8dff2652ae0e”

**Compress and Attack**

Solution: <https://github.com/apoirrier/CTFswriteups/blob/master/PicoCTF/Crypto/CompressAndAttack.md>

--> Using: /Compress and Attack/solve.py

--> Flag: “picoCTF{sheriff\_you\_solved\_the\_crime}”

**It’s not my fault 1**

Solution:

<https://github.com/HHousen/PicoCTF-2021/blob/master/Cryptography/It's%20Not%20My%20Fault%201/README.md>

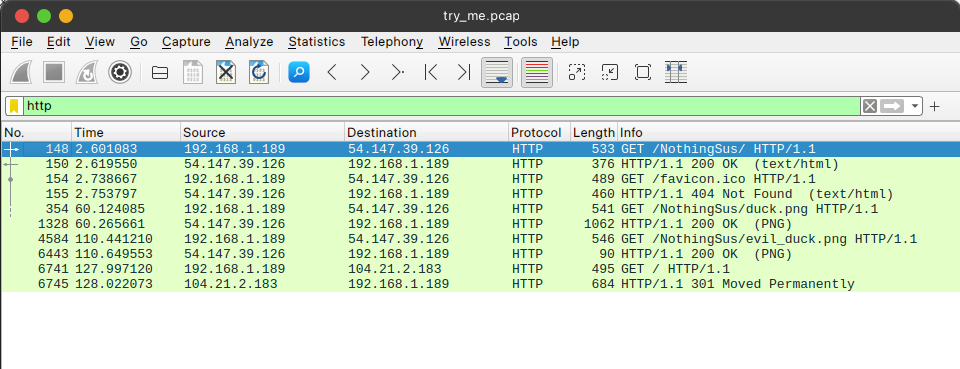
--> Using: /It’s not my fault/solve.py

--> Flag: “picoCTF{1\_c4n'7\_b3l13v3\_17'5\_n07\_f4ul7\_4774ck!!!}”

**Very very very hidden**

try\_me.pcap

Open try\_me.pcap in Wireshark and filter for http



Notice that there are .png GET from the server

--> We can extract these images from the PCAP file by going to File > Export Objects > HTTP and choosing "Save All".

--> open the evil\_duck.png image in the PowershellStegoDecode.exe program to get the following output:

$out = "flag.txt"

$enc = [system.Text.Encoding]::UTF8

$string1 = "HEYWherE(IS\_tNE)50uP?^DId\_YOu(]E@t\*mY\_3RD()B2g3l?"

$string2 = "8,:8+14>Fx0l+$\*KjVD>[o\*.;+1|\*[n&2G^201l&,Mv+\_'T\_B"

$data1 = $enc.GetBytes($string1)

$bytes = $enc.GetBytes($string2)

for($i=0; $i -lt $bytes.count ; $i++)

{

$bytes[$i] = $bytes[$i] -bxor $data1[$i]

}

[System.IO.File]::WriteAllBytes("$out", $bytes)

Notice that there are 2 strings $string1 and $string2

--> XOR them together to get the flag

--> Using: /very very very hidden/solve.py

--> Flag: “picoCTF{n1c3\_job\_f1nd1ng\_th3\_s3cr3t\_in\_the\_im@g3}”

**rsa-pop-quiz**

ManchurioX@pico-2019-shell1:~$ nc 2019shell1.picoctf.com 61751

Good morning class! It's me Ms. Adleman-Shamir-Rivest

Today we will be taking a pop quiz, so I hope you studied. Cramming just will not do!

You will need to tell me if each example is possible, given your extensive crypto knowledge.

Inputs and outputs are in decimal. No hex here!

#### NEW PROBLEM ####

q : 60413

p : 76753

##### PRODUCE THE FOLLOWING ####

n

IS THIS POSSIBLE and FEASIBLE? (Y/N):Y

#### TIME TO SHOW ME WHAT YOU GOT! ###

n: 4636878989

Outstanding move!!!

#### NEW PROBLEM ####

p : 54269

n : 5051846941

##### PRODUCE THE FOLLOWING ####

q

IS THIS POSSIBLE and FEASIBLE? (Y/N):Y

#### TIME TO SHOW ME WHAT YOU GOT! ###

q: 93089

Outstanding move!!!

#### NEW PROBLEM ####

e : 3

n : 12738162802910546503821920886905393316386362759567480839428456525224226445173031635306683726182522494910808518920409019414034814409330094245825749680913204566832337704700165993198897029795786969124232138869784626202501366135975223827287812326250577148625360887698930625504334325804587329905617936581116392784684334664204309771430814449606147221349888320403451637882447709796221706470239625292297988766493746209684880843111138170600039888112404411310974758532603998608057008811836384597579147244737606088756299939654265086899096359070667266167754944587948695842171915048619846282873769413489072243477764350071787327913

##### PRODUCE THE FOLLOWING ####

q

p

IS THIS POSSIBLE and FEASIBLE? (Y/N):N

Outstanding move!!!

#### NEW PROBLEM ####

q : 66347

p : 12611

##### PRODUCE THE FOLLOWING ####

totient(n)

IS THIS POSSIBLE and FEASIBLE? (Y/N):Y

#### TIME TO SHOW ME WHAT YOU GOT! ###

totient(n): 836623060

Outstanding move!!!

#### NEW PROBLEM ####

plaintext : 6357294171489311547190987615544575133581967886499484091352661406414044440475205342882841236357665973431462491355089413710392273380203038793241564304774271529108729717

e : 3

n : 29129463609326322559521123136222078780585451208149138547799121083622333250646678767769126248182207478527881025116332742616201890576280859777513414460842754045651093593251726785499360828237897586278068419875517543013545369871704159718105354690802726645710699029936754265654381929650494383622583174075805797766685192325859982797796060391271817578087472948205626257717479858369754502615173773514087437504532994142632207906501079835037052797306690891600559321673928943158514646572885986881016569647357891598545880304236145548059520898133142087545369179876065657214225826997676844000054327141666320553082128424707948750331

##### PRODUCE THE FOLLOWING ####

ciphertext

IS THIS POSSIBLE and FEASIBLE? (Y/N):Y

#### TIME TO SHOW ME WHAT YOU GOT! ###

ciphertext: 256931246631782714357241556582441991993437399854161372646318659020994329843524306570818293602492485385337029697819837182169818816821461486018802894936801257629375428544752970630870631166355711254848465862207765051226282541748174535990314552471546936536330397892907207943448897073772015986097770443616540466471245438117157152783246654401668267323136450122287983612851171545784168132230208726238881861407976917850248110805724300421712827401063963117423718797887144760360749619552577176382615108244813

Outstanding move!!!

#### NEW PROBLEM ####

ciphertext : 107524013451079348539944510756143604203925717262185033799328445011792760545528944993719783392542163428637172323512252624567111110666168664743115203791510985709942366609626436995887781674651272233566303814979677507101168587739375699009734588985482369702634499544891509228440194615376339573685285125730286623323

e : 3

n : 27566996291508213932419371385141522859343226560050921196294761870500846140132385080994630946107675330189606021165260590147068785820203600882092467797813519434652632126061353583124063944373336654246386074125394368479677295167494332556053947231141336142392086767742035970752738056297057898704112912616565299451359791548536846025854378347423520104947907334451056339439706623069503088916316369813499705073573777577169392401411708920615574908593784282546154486446779246790294398198854547069593987224578333683144886242572837465834139561122101527973799583927411936200068176539747586449939559180772690007261562703222558103359

##### PRODUCE THE FOLLOWING ####

plaintext

IS THIS POSSIBLE and FEASIBLE? (Y/N):N

Outstanding move!!!

#### NEW PROBLEM ####

q : 92092076805892533739724722602668675840671093008520241548191914215399824020372076186460768206814914423802230398410980218741906960527104568970225804374404612617736579286959865287226538692911376507934256844456333236362669879347073756238894784951597211105734179388300051579994253565459304743059533646753003894559

p : 97846775312392801037224396977012615848433199640105786119757047098757998273009741128821931277074555731813289423891389911801250326299324018557072727051765547115514791337578758859803890173153277252326496062476389498019821358465433398338364421624871010292162533041884897182597065662521825095949253625730631876637

e : 65537

##### PRODUCE THE FOLLOWING ####

d

IS THIS POSSIBLE and FEASIBLE? (Y/N):Y

#### TIME TO SHOW ME WHAT YOU GOT! ###



d: 1405046269503207469140791548403639533127416416214210694972085079171787580463776820425965898174272870486015739516125786182821637006600742140682552321645503743280670839819078749092730110549881891271317396450158021688253989767145578723458252769465545504142139663476747479225923933192421405464414574786272963741656223941750084051228611576708609346787101088759062724389874160693008783334605903142528824559223515203978707969795087506678894006628296743079886244349469131831225757926844843554897638786146036869572653204735650843186722732736888918789379054050122205253165705085538743651258400390580971043144644984654914856729

Outstanding move!!!

#### NEW PROBLEM ####

p : 153143042272527868798412612417204434156935146874282990942386694020462861918068684561281763577034706600608387699148071015194725533394126069826857182428660427818277378724977554365910231524827258160904493774748749088477328204812171935987088715261127321911849092207070653272176072509933245978935455542420691737433

ciphertext : 9276182891752530901219927412073143671948875482138883542938401204867776171605127572134036444953137790745003888189443976475578120144429490705784649507786686788217321344885844827647654512949354661973611664872783393501992112464825441330961457628758224011658785082995945612195073191601952238361315820373373606643521463466376095236371778984942891123936191796720097900593599447528583257806196551724676380135110693228330934418147759387990754368525068685861547977993085149359162754890674487823080750579601100854795031284533864826255207300350679553486505961837349042778851010569582458629638648589442067576234798724906377157351

e : 65537

n : 23952937352643527451379227516428377705004894508566304313177880191662177061878993798938496818120987817049538365206671401938265663712351239785237507341311858383628932183083145614696585411921662992078376103990806989257289472590902167457302888198293135333083734504191910953238278860923153746261500759411620299864395158783509535039259714359526738924736952759753503357614939203434092075676169179112452620687731670534906069845965633455748606649062394293289967059348143206600765820021392608270528856238306849191113241355842396325210132358046616312901337987464473799040762271876389031455051640937681745409057246190498795697239

##### PRODUCE THE FOLLOWING ####

plaintext

IS THIS POSSIBLE and FEASIBLE? (Y/N):Y

#### TIME TO SHOW ME WHAT YOU GOT! ###



plaintext: 14311663942709674867122208214901970650496788151239520971623411712977119642137567031494784893

Outstanding move!!!

If you convert the last plaintext to a hex number, then ascii, you'll find what you need! ;)

--> Using: /rsa-pop-quiz/solve.py

--> Flag: “picoCTF{wA8\_th4t$\_ill3aGal..ode01e4bb}”

**Sum-O-Primes**

gen.py

output.txt

In the output.txt and gen.py file, we will have three variables x, n, c and e

n: modulus

c: ciphertext

x: the sum of p and q

e: public exponent

We have some math equations:

n = p \* q

x = p + q

--> p = x - q

--> n = (x - q) \* q

--> n = -q2 + x\*q

--> -q2 + x\*q - n = 0

--> Using delta to solve this equations to get q and p

--> Using: /Sum-O-Primes/calc.py

--> With p, q, e and c, we can calculate the plaintext to get the flag

--> Flag: “picoCTF{pl33z\_n0\_g1v3\_c0ngru3nc3\_0f\_5qu4r35\_3921def5}”