Students: Andrei Ursachi 3351912

Milan Veul 3411389

The way I cracked the Vigenere cypher was by trying the know keyword attack. I was thinking that the text might be containing the word "Pearl" as in the 5.6 B. So I created a python script that was looping through the text character by character and it was decomposing the key based on the word Pearl and the letters in the cypher text. For example: If the cypher text was: "abcdefg", I was checking for (abcde, pearl), (bcdef, pearl), (cdefg, pearl). After that, because I have search in my terminal, with the same script I was decrypting all the possibilities by printing the decrypted texts with all the keys saved. - I have to specify that I sanitized the text first by removing spaces, \n and punctuation. After printing the I was searching the terminal for words that would make sense and in one of the prompts I could see that it started with IFYOU which is English but the rest was Gibberish. But it was the only one that was making sense so I updated another decryption script used for 5.6 B to check for keys that start with SKSKS as that was the key found but by adding another letter from the English alphabet. Checking all of them I found the text. Which I separated into words and finally was able to read it. After a few unsuccessful tries I finally understood the text and was able to write a quick python program to compute the password.

A = 964737507281948222657249562527181027 13<38> = 90054748583372746 57<19> · 107127888585330244 09<20>

B = 553940868665557431428417314331158855 63<38> = 626796744941809639 7<19> · 88376475011366566 79<19>

C = 556078009590083339975004041608915626 47<38> = 678939348229425046 1<19> · 819039301581582822 7<19>

D = 103183222240832246367639689876909232721<39> = 7792242517156656529<19> · 132417878439547332 49<20>

E = 81595675594617074625241781712689179295<38> = 5 · 167 · 23633 · 413486954553384195727742830 4869<31>

N = 1327692810082714690238645759171965598 89<39> = 8190393015815828227<19> · 16210367530824354907<20>

W = 1327839328799265016037514089840506 4704<38> = 2^13 · 242802727 · 66757801207198356663439 31<25>

"Used crack_key_vigenere.py to find keys" Key: SKSKS Decrypted Message:
IFYOUUIFZWADTHIKGGCEANAGEVBGJJEAKTHWDAOWNERECAXZMJTHISIKIFQEPORTAFBXQJSTSTEHQFBZISBONMASAKIGNMEFBLPW
ACTUADJGVMSASSIYVEMFTCANBWNGCFDINTHWXVNXILEPRGDALWDINTHWLWLACATEDKMUBAONCALDMVJGNUSASKQYVEENTONLPWX
WARLCRQXLWYRAPHYHIYMGNCANVSASXSSSWORVQKVWEDEDTGWHMFTHEPDXNATWWEPRONQVMLHISPAKAOWJDINENUZQXLEDFOREIL
BZEENDOXBZQKMESSAYMVMFOTEDAKELPWPASSWGZVPSSBEENWVUZQPTEDUKQFOLHERSAUZQXLOSYSTWUOQLHTHESLILMVRSAPUTT
AKEODULUKVSVVPUBLIUMPXGNENTEQWMZLASKISLWOZATEYOUJWOVHYTHONHZGOJAMTHALJJMSKSTHEWVUZQPTIONGNLPWPASSWG
ZVQFORDERLWJMSDTHEPVNXQDEALTHGCYPLHERSAEWVCDUSNISDIJOWITMIGZBEICESENSWBGBJYTOFAUBGZAZEITTGMSAWTHISPJ
WUMKSWEWOMTVTAKETOPJWNQVEYOUWABZBZEBELOOALILEDADDABAWFALRSAEWVCDIABCAFLVEZICHHANMTMWNUSEDAVSKGMPLE
TWTQLAFFEREFBUWFTEXTBMBLPSTHAVETMWVYENERALMVEATHTHEKIEMTADRANVWEXJIMEGEFMJILORASWSAMAWDTOGEFMJILENM
AYTMLPWYHELPQWMBGFACTOJQRMF

"Used vigenere_dec.py to try multiple variations of the key to find the correct text"

"The final key is SKSKSK"

Final Message: IF YOU CAN READ THIS YOU MANAGED TO BREAK THE VIGENERE CIPHER THIS IS AN IMPORTANT FIRST STEP IN THIS BONUS ASSIGNMENT THE ACTUAL BONUS ASSIGNMENT CAN BE FOUND IN THE PDF FILE PROVIDED IN THE DEDICATED SECTION CALLED BONUS ASSIGNMENT ON THE PEARL CRYPTOGRAPHY PAGE ON CANVAS A PASSWORD IS NEEDED TO OPEN THE PDF FILE WE PROVIDE THIS PASSWORD IN ENCRYPTED FORMAT THE END OF THIS MESSAGE DENOTED AS W THE PASSWORD HAS BEEN ENCRYPTED USING THE RSA CRYPTOSYSTEM WITH THE STATED RSA PUBLIC MODULUS N AND PUBLIC EXPONENT E YOUR TASK IS TO WRITE YOUR OWN PYTHON PROGRAM THAT BREAKS THE ENCRYPTION OF THE PASSWORD IN ORDER TO READ THE PDF FILE ALTHOUGH THER S A MODULUS N IS LARGE IT MIGHT MAKE SENSE TO TRY TO FACTORIZE IT TO EASE THIS PROCESS WE WOULD LIKE TO PROVIDE YOU WITH THE BELOW STATED ADDITIONAL RSA MODULI A B C AND D WHICH HAVE BEEN USED IN A COMPLETELY DIFFERENT CONTEXT BUT THAT HAVE BEEN GENERATED WITH THE SAME BAD RANDOM PRIME GENERATOR AS WAS USED TO GENERATE N MAYBE THEY HELP YOU TO FACTORIZE N

"Cracked the pdf password with the script crack_t.py:"

Factors of N: p = 8190393015815828227, q = 16210367530824354907

Decrypted password: 384625665664413817427952414206387688 69