COL759 Tutorial-1

Riddhidipta Pal

August 13, 2024

Question 1

plain_text:
cybersecurity is important now. it shields systems networks and data from attacks. as threats rise strong measures are needed. encryption updates and employee training help reduce risks. a culture of awareness is key for everyone. in a connected world proactive actions protect information and ensure trust.

key:
ydlqigavjnxfsmkpurzctwboeh

cipher_text:
tawyrmytqreua em enpxrugju jxv. eu mzeycbm mamuynm jyuvxrom gjb bgug lrxn guugtom. gm uzrygum remy murxjf nygmqrym gry jyybyb. yjtrapuexj qpbguym gjb ynpcxayy urgejejf zycp rybqty remom. g tqcuqry xl gvgryjymm em oya lxr yhyraxjy. ej g txjjytuyb vxrcb prxgtuehy gtuexjm prxuytu ejlxrnguexj gjb yjmqry urqmu.

Approach to Solving:
Since there are gaps between words, I thought at least some of the digrams would be ”is” or ”in” or ”it”.

After the digrams were successfully substituted, words start to become visible and more substitutions start to come up. For example, in the ciphertext ”trqst” can be seen as ”trust”, thus we can see that ”q” has to be substituted with ”u”.

As some letters were decrypted, more letters and words started becoming recognisable, and I progressively worked through the ciphertext.

Question 2

plain_text:
cryptography changes data into a coded form making it unreadable without the correct key. this process protects information from unauthorized access. encryption techniques and strong keys are crucial. regular updates and reviews help ensure cryptographic methods remain effective. cryptography is vital for digital security.

key:
pfkxzdembhalujsvwigqroncty

cipher_text:
xuzayvsukajzxjkwsgofkykrwyvkxvfgfbvuhhkcrwsrymwugkfkilgqryjvmyyjgxvuugxycgzyjroauvxgooauvygxyorwbvuhkyrvwbuvhmwkmyjvuregfkxxgoogwxuzayrvwygxjwrtmgokwfoyuvwscgzokugxumxrklugsmlkumafkygokwfugprgqojglagwomugxuzayvsukajrxhgyjvfoughkrwgbbgxyrpgxuzayvsukajzropryklbvufrsryklogxmuryz

Approach to Solving:
Since the text does not have gaps, I performed frequency analysis of digrams and trigrams. I figured, one of the trigrams has to be ”for”, so tried it for the more frequent ones, on hitting the correct one, other words became more visible, so I progressively worked through the letters to decrypt them.

In between, there are repeating letters like ”oo” and ”xx”. One of the common letter that occurs consecutively is ”s” (like in access) and ”l” (like in balloon). Tried substituting them with the letters to get more readable words in the ciphertext.

Eventually, words start to become visible and offer up clues for decryption. Like in the phrase ”secmrity”, we can easily make the substitution of m -¿ u to get the correct word ”security”.

Question 3

plain_text:
DURING THE SUMMER, WE DECIDED TO TAKE A TRIP TO THE MOUNTAINS. THE WEATHER WAS PERFECT, WITH THE SUN SHINING BRIGHTLY AND A GENTLE BREEZE BLOWING THROUGH THE TREES. WE HIKED UP STEEP TRAILS, EXPLORED HIDDEN WATERFALLS, AND ENJOYED BREATHTAKING VIEWS FROM THE PEAKS. IN THE EVENINGS, WE GATHERED AROUND AX CAMPFIRE, ROASTING MARSHMALLOWS AND SHARING STORIES. THE NIGHTS WERE COOL AND CLEAR, WITH THE SKY FULL OF STARS. IT WAS A PEACEFUL ESCAPE FROM THE HUSTLE AND BUSTLE OF EVERYDAY LIFE, A CHANCE TO RECONNECT WITH NATURE AND EACH OTHER.

key:
KUNDARILSHTBCEFGMOPQVWXYZ

keyword:
KUNDARILSHT

cipher_text:
ANILKO FRCY IDOWPBLV, YB SPBLSPNY CG FKDT NZ GTSM CG FRCY OPNDFKLULY. FRCY YBKFSFLV ZULY YPHTFECV, UBFR FRCY IDLN HRLULUOV TIRMRFSX KDNY NZ PTKCSC TICYFYCY CIMXLUOV FRLGKMLZ FRCY GTCYPE. YB RLDTNY DM RECYPY GTUHSH, CYOSGLPS RLNYSPLN ZUBFHTNHSH, KDNY CDLMDPNY TIFDFRFKURKO WRBYLY THPO FRCY YPKULY. LU FRCY TYCDLUPR, YB QKFRTSPS KHMNDA NZ FNOQBHST, LGDHBRKO QUIHIQNHCXYI KDNY HRKHLUOV REGLSBLY. FRCY ULQRER YBST OXXC KDNY OCFDLV, UBFR FRCY RDZY BACNCN QC REKHLY. RB ZULY NZ YPNFFTNI PEFNYP THPO FRCY IARESC KDNY MIRESC QC TYTSDSDZ SLTF, NZ FLKDEF CG STOXLNDCEB UBFR DKBKST KDNY FDFL GCSFLV.

Approach to Solving:
Performed frequency analysis of the words in the ciphertext, and assumed that the most frequent 4 letter words would be ”ANDX”, ”WASX”, ”THEX”, etc. Similarly, assumed that the frequent 2 letter words would be ”AX”, ”TO”, ”IN”, ”IT”, etc. After some trial and error with assigning words to the ciphertext, I started reverse-engineering the incomplete values of the key matrix.

Using this incomplete key matrix, I solved more of the bigrams in the cipher. Words started to become more visible as they became partially solved by putting bigrams in them. This led us to get more bigrams and complete the matrix further.