INTRODUCTION TO CRYPTOGRAPHY – QUIZ 1

B.Tech. Computer Science and Engineering (Cybersecurity)

|  |  |
| --- | --- |
| Name: Anish Sudhan Nair | Roll No.: K041 |
| Batch: K2/A2 | Date of submission: 05/01/2021 |

Quiz 1

Consider the following cipher text that is encrypted using Substitution cipher:

Va vh j sltt-xrosr lhajutvhglb ijma agyocngoca agl fjrd-bvflrhvorjt soytbh oi agl fctavklyhl agja foha yljttd nylja bvhmoklyvlh jyl oslb ao orl uyvli foflra oi vrhwvyjavor. Aglyl’h j toa oi hwjblsoyx ivyha, oi mocyhl, uca sgja mtvrmglh agl sgotl agvrn vh agl hvnga oi, hjd, j ijttvrn jwwtl oy j uovtvrn xlaatl oy agl sjaly htvwwvrn okly agl lbnl oi agl ujag. Hoflagvrn nolh mtvmx vrhvbl agl ouhlykly’h gljb jrb aglr lklydagvrn ijtth vrao wtjml. Agl hgjwl oi BRJ, va vh wowctjytd hjvb, oslh vah bvhmoklyd ao agl mgjrml hvnga oi j hwvyjt hajvymjhl sglr agl hmvlravha’h fvrb sjh echa ja agl yvnga ylmlwavkl alfwlyjacyl. Gjb gl chlb agl ltlkjaoy, agl sgotl hmvlrml oi nlrlavmh fvnga gjkl ullr j noob bljt bviilylra.

Agvh vh agocnga oi jh hoflgos sorblyict. Va vhr’a. va vh ayjnvm. Tvaatl wjyavmtlh oi vrhwvyjavor htlla agyocng agl crvklyhl jtt agl avfl ayjklttvrn agyocng agl blrhlha fjaaly vr agl hjfl sjd agja j rlcayvro wjhhlh agyocng j mjrbditohh gjdhajmx, jrb foha oi aglf fvhh.

Lklr soyhl, foha oi agl orlh agja gva agl lpjma mlyluyjt ajynla, gva agl syorn orl.

Ioy lpjfwtl, agl slvyb byljf juoca j tljb bocngrca or j fvtl-gvng njrayd, sgvmg vr agl yvnga fvrb soctb gjkl ullr agl mjajtdha ioy agl vrklravor oi ylwylhhlb- nyjkvajavorjt ltlmayvmvad nlrlyjavor (j mgljw jrb vrlpgjchavutl jrb aoajttd ror-wottcavrn ioyf oi wosly sgvmg agl soytb vr zclhavor gjb ullr hllxvrn ioy mlracyvlh, jrb ioy agl tjmx oi sgvmg va sjh wtcrnlb vrao j alyyvutl jrb wovratlhh sjy) sjh vr ijma gjb ud j hfjtt jrb ulsvtblylb bcmx.

Ud jroagly hayoxl oi ujb tcmx, agl hvnga oi j glyb oi svtb goyhlh njttowvrn agyocng j ivltb oi svtb gdjmvragh soctb gjkl tlb j haycnntvrn mofwohly ao syval agl ijfoch Itdvrn Nob Hcval, uyvrnvrn hcmmoy jrb ujtf ao agl hocth oi fvttvorh, gjb gl roa ullr ja gofl vr ulb svag hgvrntlh. Agl vrhwvyjavor aglylud iltt ao j rljyud iyon, sgo sjh roa vr fcmg oi j wohvavor ao fjxl j hajyatvrn morayvucavor ao agl ivltb oi aorl wolayd.

Fjrd mvkvtvqjavorh gjkl ylmonrvqlb agvh hgomxvrn sjhal jrb ayvlb kjyvoch flagobh ao wylklra va, foha oi aglf vrkotkvrn lreodjutl uca vttlnjt jaalfwah ao acrl agl fvrb vrao agl yvnga sjkltlrnag ud agl chl oi lpoavm glyujnl oy dljha wyobcmah. Va rlkly soyxh wyowlytd.

1. (2 points) Find the frequency of each alphabet character in this above cipher text. You may use the following tool to count:

<https://www.mtholyoke.edu/courses/quenell/s2003/ma139/js/count.html>

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| A | B | C | D | E | F | G | H | I | J | K | L | M |
| 186 | 60 | 41 | 25 | 2 | 37 | 116 | 111 | 46 | 128 | 24 | 210 | 46 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| 54 | 139 | 4 | 2 | 112 | 38 | 85 | 28 | 139 | 33 | 13 | 96 | 1 |

Now indicate the alphabet that has the highest frequency in the given cipher text.

L - 210

1. (2 points) Write below the frequency of the alphabet that has the highest frequency in the given ciphertext. Your answer should be an integer.

L – 210 (highest frequency)

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| L | A | O | V | J | G | R | H | Y | T | B | N | I |
| 210 | 186 | 139 | 139 | 128 | 116 | 112 | 111 | 96 | 85 | 60 | 54 | 46 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| M | C | S | F | W | U | D | K | X | P | E | Q | Z |
| 46 | 41 | 38 | 37 | 33 | 28 | 25 | 24 | 13 | 4 | 2 | 2 | 1 |

1. (10 points) It is given that the alphabet J in the ciphertext is decrypted as the alphabet a in the plaintext. If the ciphertexts are given with capital letters, enter the corresponding plaintext alphabet.

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| A | B | C | D | E | F | G | H | I | J | K | L | M |
| t | d | u | y | j | m | h | s | f | a | v | e | c |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| g | o | x | z | n | w | l | b | i | p | k | r | q |

1. (6 points) Decrypt the given cipher text. Type very clearly the original plaintext. You should include all the commas, hyphens, periods, and paragraphs in your plain text.

**PLAIN TEXT:**

It is a well-known established fact throughout the many-dimensional worlds of the multiverse that

most really great discoveries are owed to one brief moment of inspiration.  There’s a lot of spadework

first, of course, but what clinches the whole thing is the sight of, say, a falling apple or a boiling

kettle or the water slipping over the edge of the bath.  Something goes click inside the observer’s

head and then everything falls into place.  The shape of DNA, it is popularly said, owes its discovery

to the chance sight of a spiral staircase when the scientist’s mind was just at the right receptive

temperature.  Had he used the elevator, the whole science of genetics might have been a good deal

different.

This is thought of as somehow wonderful.  It isn’t.  it is tragic.  Little particles of inspiration

sleet through the universe all the time travelling through the densest matter in the same way that

a neutrino passes through a candyfloss haystack, and most of them miss.

Even worse, most of the ones that hit the exact cerebral target, hit the wrong one.

For example, the weird dream about a lead doughnut on a mile-high gantry, which in the right mind

would have been the catalyst for the invention of repressed- gravitational electricity generation

(a cheap and inexhaustible and totally non-polluting form of power which the world in question had

been seeking for centuries, and for the lack of which it was plunged into a terrible and pointless

war) was in fact had by a small and bewildered duck.

By another stroke of bad luck, the sight of a herd of wild horses galloping through a field of wild

hyacinths would have led a struggling composer to write the famous flying god suite, bringing succor

and balm to the souls of millions, had he not been at home in bed with shingles.  The inspiration

thereby fell to a nearby frog, who was not in much of a position to make a startling contribution

to the field of tone poetry.

Many civilizations have recognized this shocking waste and tried various methods to prevent it, most

of them involving enjoyable but illegal attempts to tune the mind into the right wavelength by the

use of exotic herbage or yeast products.  It never works properly.