Foundations of Cybersecurity 50.042

Lab 2 Report

Sng Wei Qi Amos 1005952

**Part I: Substitution cipher**

After running a python script to count the frequency of appearance of each character, we obtain this dictionary. We will call this the first iteration.

We omit “ “ spaces as it is given that spaces are preserved.

Each (key, value) pair corresponds to (character, frequency of character).

Resulting dictionary from iteration 1:

{'U': 0.11159, 'J': 0.09623, 'Y': 0.083790, 'Q': 0.077936, 'E': 0.075375, 'D': 0.075009, 'I': 0.072447, 'X': 0.058543, 'H': 0.047932, 'B': 0.037321, 'T': 0.035858, 'W': 0.025978, 'C': 0.025612, 'S': 0.022319, 'O': 0.021222, 'K': 0.018660, 'M': 0.018294, 'V': 0.018294, 'F': 0.015733, '.': 0.014270, ',': 0.014270, 'R': 0.012806, 'L': 0.010611, 'A': 0.007317, 'N': 0.001097, 'Z': 0.001097, 'P': 0.000365}

Comparing this to the frequency of letters in the English language (table below).

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| E | 11.1607% | 56.88 | M | 3.0129% | 15.36 |
| A | 8.4966% | 43.31 | H | 3.0034% | 15.31 |
| R | 7.5809% | 38.64 | G | 2.4705% | 12.59 |
| I | 7.5448% | 38.45 | B | 2.0720% | 10.56 |
| O | 7.1635% | 36.51 | F | 1.8121% | 9.24 |
| T | 6.9509% | 35.43 | Y | 1.7779% | 9.06 |
| N | 6.6544% | 33.92 | W | 1.2899% | 6.57 |
| S | 5.7351% | 29.23 | K | 1.1016% | 5.61 |
| L | 5.4893% | 27.98 | V | 1.0074% | 5.13 |
| C | 4.5388% | 23.13 | X | 0.2902% | 1.48 |
| U | 3.6308% | 18.51 | Z | 0.2722% | 1.39 |
| D | 3.3844% | 17.25 | J | 0.1965% | 1.00 |
| P | 3.1671% | 16.14 | Q | 0.1962% | (1) |

We realise that the dictionary obtained from iteration 1 is not able to map 1:1 to the frequency table provided as there are ‘.’ and ‘,’ characters. Hence in the next iteration, iteration 2, we choose to omit ‘.’ and ‘,’ characters.

Resulting dictionary from iteration 2:

{'U': 0.114878, 'J': 0.099058, 'Y': 0.086252, 'Q': 0.080226, 'E': 0.077589, 'D': 0.077213, 'I': 0.074576, 'X': 0.060264, 'H': 0.049341, 'B': 0.038418, 'T': 0.036911, 'W': 0.026742, 'C': 0.026365, 'S': 0.022976, 'O': 0.021846, 'K': 0.019209, 'M': 0.018832, 'V': 0.018832, 'F': 0.016196, 'R': 0.013183, 'L': 0.010923, 'A': 0.007533, 'N': 0.00113, 'Z': 0.00113, 'P': 0.000377}

We realise that there are 25 characters in this resultant dictionary from iteration 2, hence it is still possible to map each character from result of iteration 2 to the frequency table.

We do this by sorting the characters in descending order of frequency and creating a substitution table. The first iteration of the substitution table is as follows.

{'U': 'E', 'J': 'A', 'Y': 'R', 'Q': 'I', 'E': 'O', 'D': 'T', 'I': 'N','X':'S', 'H': 'L', 'B': 'C', 'T': 'U', 'W': 'D', 'C': 'P', 'S': 'M', 'O': 'H', 'K': G', 'M': 'B', 'V': 'F', 'F': 'Y', 'R': 'W', 'L': 'K', 'A': 'V', 'N': 'X', 'Z':'Z', 'P': 'J'}

By using the above replacement dictionary, to decipher the plaintext, we achieve:

BSIA RN NHPYSODEIL. FOL I COOOOOTD, COOOTD ARPE R SIKE TEKEL WOASELEU ETDIDRTD PHNECF RT ASRN FLITMSRNE. R URU TOA GTUELNAITU BSIA RA RN. TOB ASIA ASE NSOB RN SIKRTD RAN CINA NEINOT, R UEMRUEU AO FRTICCH DRKE RT, DRKE NHPYSODEIL I ALH FLOP ASE KELH NAILA. R BOTUELEU SOB SIKE R PRNNEU OGA OT ASE ITRPE OF ASE UEMIUE ICC ASENE HEILN. R SOTENACH URU TOA VTOB BSIA AO EXYEMA BIAMSRTD ASE KELH FRLNA EYRNOUE VTOBRTD IWNOCGAECH TOASRTD IWOGA ASE FLITMSRNE. ASE NSOB AOHEU BRAS PH EPOAROTN NO PGMS RT ASIA OYETRTD NEAYREME. RA ETUEU GY WERTD OTE OF ASE PONA CRFE IFFRLPRTD NSOBN

OGA ASELE. I NAGTTRTD URNYCIH OF RUROMH ITU IMAROT ASIA RN WOAS MSILPRTD ITU MIYARKIARTD. RA RN MOTFRUETA RT RAN NALETDASN ITU YILIUEN RAN BEIVTENNEN YLOGUCH, I NSOB ASIA RN WOAS ICC NAHCE ITU ICC NGWNAITME. OS WGA PONA OF ICC, RA RN I ALGE LOCCEL MOINAEL OF EPOAROTN, ITU R UO TOA GNE ASIA AELP CRDSACH. R CIGDSEU, R MLREU, R DOA FLGNALIAEU IA ASE RTEYARAGUE ITU NAGYRURAH OF WOAS

ASE MSILIMAELN ITU ASE MLEIAOLN, WGA PONA OF ICC, R COKEU. BSET ASE MGLNE OF WICIC FECC RT YCIME, NOTDN NARCC PITIDEU AO WLRUDE ASIA DIY ITU MOTTEMA GN ICC AODEASEL. ASE OTE EPOAROT ASE NSOB

TEKEL FIRCN AO UECRKEL RN SHYE. ASE NGLDE OF IULETICRTE ITU ETUOLYSRTN ITU ICC ASE MSEPRMICN RT HOGL WLIRT BSETEKEL NOPEASRTD IBENOPE RN SIYYETRTD OTNMLEET RN I LILE ALEIA RT PONA OASEL ITRPE, WGA I MOTNAITA OMMGLLETME RT ASRN NSOB. ASE SHYE UOEN OMMINROTICCH FIRC AO UECRKEL, ASE SRDSEL EXYEMAIAROTN MIT NOPEARPEN WE OS AOO PGMS, WGA NARCC, BSET HOG SEIL SRWRVR NMLEIP, HOG VTOB NSE PEITN WGNRTENN ITU ZORT SEL RT NOTD. ITU ASONE NOTDN ILE YLEMRNECH BSIA VEEYN NHPYSODEIL RT ASE PRTUN OF PITH ICC ASRN BSRCE. R IP TOA IT RUOC ITRPE YELNOT, R UENYRNE PONA RUOC ITRPE ITU HEA. ITU HEA. ASE POPETA R SEILU ASE NOTDN FOL ASE FRLNA ARPE LRDSA ASELE OT ASE RUOC MOTMELA, R BIN ETASLICCEU. R VTEB ASIA LEDILUCENN OF SOB ASE NSOB AGLTEU OGA, RA BOGCU SIKE DLEIA PGNRM. MOKELRTD PITH DETLEN, ASE NSOB SIN I URKELNE YICEAAE OF NOTDN LITDRTD FLOP MECARM LOMV AO ETVI RTNYRLEU ALIMVN, ASELE RN TO NSOLAIDE OF KILREAH. HEN ASELE ILE NOTDN ASIA UO TOA BOLV BECC, WGA ASE OTEN ASIA LENOTIAE FIL OGABERDS ASE OMMINROTIC WIU OTEN. NHPYSODEIL SIN AO WE AIVET RT IN I MOPYCEAE YIMVIDE. RA ALGCH RN POLE ASIT ASE NGP OF RAN YILAN. COOVRTD WIMV, HEN R MIT IDLEE OT

ICC ASE FCIBN, NOPE PIZOL, ASE NSOB SIN SIU. HEA RT NYRAE OF RA ICC, IMLONN NEKET HEILN ITU FRKE NEINOTN. RA RN BSH R GCARPIAECH UEMRUEU RT IBILURTD RA BRAS OTE OF PH LILE TRTEN. NOPEASRTD ASRN NYEMRIC, ASRN RTNYRLIAROTIC, ASRN COTD CINARTD RN ALGCH IT EXYELRETME AO WESOCU. FOL WEAAEL FOL BOLNE, RA RN ASE UEFRTRARKE ITRPE ASIA LEYLENETAN ASE UEMIUE. RA PIH TOA SIKE ETUEU RT ASE BIH R BITAEU, ITU RA PIH TOA SIKE ASIA OTE VRNN R BIN COOVRTD FOL, WGA RA FRCCEU ASE SOCE RT PH SEILA, ITU BRAS RA ETURTD, ASE DIYRTD BOGTU RT PH NOGC PIH TEKEL SEIC. PIHWE, FOL TOB, R BRCC NIH ASIA ASE NSOB ETUEU BECC. RA BIN TOA YELKELAEU RTAO I JOPWRE FLITMSRNE CRVE OASELN, TOL URU RA NAGPWCE SILU RT RAN FRTIC POPETA ITU NALGDDCE AO LEMCIRP RAN YINA DCOLH. RA SIU NSOLAMOPRTDN,

WGA ASRTVRTD WIMV, ASE ZOGLTEH AO ASE ETU SIN WEET I NIARNFHRTD OTE ASLOGDSOGA. NO BSIA RN NHPYSODEIL. RA RN I SHWLRU RUOC ITRPE. RA RN IT ITRPE IWOGA FRNARTD. RA RN FRKE NEINOTN ITU NEKET HEILN COTD ITU SIN MIYARKIAEU ASE SEILAN OF PITH. WGA PONA RPYOLAITACH, RA RN WECREKRTD RT ASE NOTD OF HOGL SEILA.

The result is still indecipherable, but we are able to use knowledge such as “I” and “A” being the most common single letter word and that the most common 2 letter words are: to, of, in, it, is, as, at, be, we, he, so, on, an, or, do, if, up, by, and my.

We can use the guess and check method to obtain the following swap table. Which can successfully decipher the plaintext.

{'U': 'E','J': 'T', 'Y': 'I', 'Q': 'A', 'E': 'O', 'D': 'N', 'I': 'S','X': 'H',

'H': 'R', 'B': 'L', 'T': 'D', 'W': 'G', 'C': 'M','S': 'C','O': 'Y','K': 'U', 'M': 'W', 'V': 'F', 'F': 'P', 'R': 'B', 'L': 'V', 'A': 'K', 'N': 'X','Z': 'Z',

'P': 'J'}

Deciphered plaintext:

WHAT IS SYMPHOGEAR. FOR A LOOOOONG, LOOONG TIME I HAVE NEVER BOTHERED ENGAGING MYSELF IN THIS FRANCHISE. I DID NOT UNDERSTAND WHAT IT IS. NOW THAT THE SHOW IS HAVING ITS LAST SEASON, I DECIDED TO FINALLY GIVE IN, GIVE SYMPHOGEAR A TRY FROM THE VERY START. I WONDERED HOW HAVE I MISSED OUT ON THE ANIME OF THE DECADE ALL THESE YEARS. I HONESTLY DID NOT KNOW WHAT TO EXPECT WATCHING THE VERY FIRST EPISODE KNOWING ABSOLUTELY NOTHING ABOUT THE FRANCHISE. THE SHOW TOYED WITH MY EMOTIONS SO MUCH IN THAT OPENING SETPIECE. IT ENDED UP BEING ONE OF THE MOST LIFE AFFIRMING SHOWS OUT THERE. A STUNNING DISPLAY OF IDIOCY AND ACTION THAT IS BOTH CHARMING AND CAPTIVATING. IT IS CONFIDENT IN ITS STRENGTHS AND PARADES ITS WEAKNESSES PROUDLY, A SHOW THAT IS BOTH ALL STYLE AND ALL SUBSTANCE. OH BUT MOST OF ALL, IT IS A TRUE ROLLER COASTER OF EMOTIONS, AND I DO NOT USE THAT TERM LIGHTLY. I LAUGHED, I CRIED, I GOT FRUSTRATED AT THE INEPTITUDE AND STUPIDITY OF BOTH THE CHARACTERS AND THE CREATORS, BUT MOST OF ALL, I LOVED. WHEN THE CURSE OF BALAL FELL IN PLACE, SONGS STILL MANAGED TO BRIDGE THAT GAP AND CONNECT US ALL TOGETHER. THE ONE EMOTION THE SHOW NEVER FAILS TO DELIVER IS HYPE. THE SURGE OF ADRENALINE AND ENDORPHINS AND ALL THE CHEMICALS IN YOUR BRAIN WHENEVER SOMETHING AWESOME IS HAPPENING ONSCREEN IS A RARE TREAT IN MOST OTHER ANIME, BUT A CONSTANT OCCURRENCE IN THIS SHOW. THE HYPE DOES OCCASIONALLY FAIL TO DELIVER, THE HIGHER EXPECTATIONS CAN SOMETIMES BE OH TOO MUCH, BUT STILL, WHEN YOU HEAR HIBIKI SCREAM, YOU KNOW SHE MEANS BUSINESS AND ZOIN HER IN SONG. AND THOSE SONGS ARE PRECISELY WHAT KEEPS SYMPHOGEAR IN THE MINDS OF MANY ALL THIS WHILE. I AM NOT AN IDOL ANIME PERSON, I DESPISE MOST IDOL ANIME AND YET. AND YET. THE MOMENT I HEARD THE SONGS FOR THE FIRST TIME RIGHT THERE ON THE IDOL CONCERT, I WAS ENTHRALLED. I KNEW THAT REGARDLESS OF HOW THE SHOW TURNED OUT, IT WOULD HAVE GREAT MUSIC. COVERING MANY GENRES, THE SHOW HAS A DIVERSE PALETTE OF SONGS RANGING FROM CELTIC ROCK TO ENKA INSPIRED TRACKS, THERE IS NO SHORTAGE OF VARIETY. YES THERE ARE SONGS THAT DO NOT WORK WELL, BUT THE ONES THAT RESONATE FAR OUTWEIGH THE OCCASIONAL BAD ONES. SYMPHOGEAR HAS TO BE TAKEN IN AS A COMPLETE PACKAGE. IT TRULY IS MORE THAN THE SUM OF ITS PARTS. LOOKING BACK, YES I CAN AGREE ON ALL THE FLAWS, SOME MAZOR, THE SHOW HAS HAD. YET IN SPITE OF IT ALL, ACROSS SEVEN YEARS AND FIVE SEASONS. IT IS WHY I ULTIMATELY DECIDED IN AWARDING IT WITH ONE OF MY RARE NINES. SOMETHING THIS SPECIAL, THIS INSPIRATIONAL, THIS LONG LASTING IS TRULY AN EXPERIENCE TO BEHOLD. FOR BETTER FOR WORSE, IT IS THE DEFINITIVE ANIME THAT REPRESENTS THE DECADE. IT MAY NOT HAVE ENDED IN THE WAY I WANTED, AND IT MAY NOT HAVE THAT ONE KISS I WAS LOOKING FOR, BUT IT FILLED THE HOLE IN MY HEART, AND WITH IT ENDING, THE GAPING WOUND IN MY SOUL MAY NEVER HEAL. MAYBE, FOR NOW, I WILL SAY THAT THE SHOW ENDED WELL. IT WAS NOT PERVERTED INTO A JOMBIE FRANCHISE LIKE OTHERS, NOR DID IT STUMBLE HARD IN ITS FINAL MOMENT AND STRUGGLE TO RECLAIM ITS PAST GLORY. IT HAD SHORTCOMINGS, BUT THINKING BACK, THE ZOURNEY TO THE END HAS BEEN A SATISFYING ONE THROUGHOUT. SO WHAT IS SYMPHOGEAR. IT IS A HYBRID IDOL ANIME. IT IS AN ANIME ABOUT FISTING. IT IS FIVE SEASONS AND SEVEN YEARS LONG AND HAS CAPTIVATED THE HEARTS OF MANY. BUT MOST IMPORTANTLY, IT IS BELIEVING IN THE SONG OF YOUR HEART.

**Part II: Compromising OTP integrity**

Since we know that:

y = x ⊕ k

m = x ⊕ x′

y′ = y ⊕ m

y′ ⊕ k = x′

we can XOR our initial message and final message to find the change and then XOR the change with the initial cipher text to produce a new cipher text, which will change the original message to our target message: b’Student ID 1006954 gets 4 points\n’