COMP3260 | Assignment 1

By c and c3349828

**Cipher 1:**

Ran frequency distribution: clearly polyalphabetic substitution.

IC = 0.04246 = period of about 7

Kasiski with 7-size words = intervals are 904, 1432, 88 and 368 – all divide by 8

period is 8

ran frequency distribution over 8 alphabets – noticed that frequency distribution is REVERSED English, therefore Beaufort

Derived key “mistrust”

Cipher text:

thedi gitsz eroan donea rethe natur allan guage ofcom puter

salmo stany thing canbe repre sente dinsi deaco mpute rsmem

orysi mplyb yarra nging zeros andon esint othep roper seque

nceho wever becau semos tcomp uterm emory consi stsof nothi

ngmor ethan amicr oscop icmag netic charg ethes ebina rydig

itsbi tscan alsob esusc eptib letot hecon ditio nsoft heirp

hysic alenv ironm entou rbits arest oredi nside incre asing

lycom pactd evice sthat funct ionou tside inthe harsh envir

onmen tofpl anete arthm anyof ourde vices arero utine lysub

jecte dtoex treme sinte mpera turei naddi tiont ohaza rdssu

chasc osmic raysu ndera dvers econd ition ssuch asthe seaon

eocca siona llyan dinad verte ntlyf lipss tatet obeco meaze

roorv iceve rsafo rusth ecomm onint ernet users biter rorsc

anhav eapro found effec tonou rinte rnett raffi cfore xampl

ethro ughth eflip ofasi ngleb itthe domai nname sdoty timgd

otcom canbe comet hedom ainna mesny timgd otcom there iseve

nawor dtode scrib ether egist ratio nofth esebi terro rdoma

insbi tsqua tting misdi recti ngint ernet traff ictom alici

ousbi tsqua ttedd omain shass eriou simpl icati onsfo rcomp

uters ecuri tyhow everb iterr orsca nalso havet errib leeve

nlife threa tenin gcons equen cesin austr aliai ntwot housa

ndand eight qanta sflig htqfs event ytwow ascar rying moret

hanth reehu ndred passe ngers atcru ising altit udewh enits

udden lynos edive dsixh undre dfift yfeet thepi lotsw ereab

letob ringt hepla nebac ktoit sorig inala ltitu debef oreit

sudde nlypl unged again thist imefa lling forhu ndred feets

omepa sseng erswe rethr ownou tofth eirse atsan dsome weree

jecte douto fthei rseat belts accor dingt oarep ortby theau

stral iantr anspo rtsaf etybu reaua tsbso mepas senge rswer

eflun gsovi olent lytha tthei mpact damag edthe aircr aftca

bince iling theat sbinv estig ation wasab letoe limin ateal

mosta llthe poten tialc auses offai luree xcept onean airpl

aneco mpute rbite rrorc aused bycos micra diati onacc ordin

gtoth eatsb repor tthec pumod ulesf orthe twoaf fecte dunit

sdidn othav eerro rdete ction andco rrect ioned ac

Plain English:

The digits zero and one are the natural language of computers. Almost anything can be represented inside a computer’s memory simply by arranging zeros and ones into the proper sequence. However, because most computer memory consists of nothing more than a microscopic magnetic charge, these binary digits bits can also be susceptible to the conditions of their physical environment. Our bits are stored inside increasingly compact devices that function outside in the harsh environment of Planet Earth.

Many of our devices are routinely subjected to extremes in temperature in addition to hazards such as cosmic rays. Under adverse conditions such as these, a one occasionally and inadvertently flips state to become a zero, or vice versa. For us, the common internet users, bit errors can have a profound effect on our internet traffic. For example, through the flip of a single bit the domain names dotytimgdotcom can become the domain names nytimgdotcom. There is even a word to describe the registration of these bit error domains: bit squatting.

Misdirecting internet traffic to malicious bit squatted domains has serious implications for computer security. However, bit errors can also have terrible, even life-threatening consequences. In Australia, in two thousand and eight, QANTAS flight “QF seventy two” was carrying more than three hundred passengers at cruising altitude when it suddenly nosedived six hundred fifty feet. The pilots were able to bring the plane back to its original altitude before it suddenly plunged again, this time falling for hundred feet. Some passengers were thrown out of their seats and some were ejected out of their seatbelts. According to a report by the Australian Transport Safety Bureau (ATSB), some passengers were flung so violently that the impact damaged the aircraft cabin ceiling.

The ATSB investigation was able to eliminate almost all the potential causes of failure except one: an airplane computer bit error caused by cosmic radiation. According to the ATSB report, the CPU modules for the two affected units did not have error detection and correction (EDAC).

**Cipher 2:**

Ran frequency distribution: matches English language, therefore transposition.

Easiest way of decrypting is with Search

I wanted a common but unusually spelt word in the English language – this would generate a likely result but would cut down on false positives.

My plan was to run permutations of 4-9 letters (within the bounds of the assignment, any more would require an unreasonable amount of computing power). If no proper results appeared, I would try again with a different word.

My first word choice was “which”, the 48th most popular word according to the Oxford English Corpus.

“which” with a period of 4: 0 results

“which” with a period of 5: 0 results

“which” with a period of 6: 1 result

“which” with a period of 7: 15 results

Studying each permutation carefully, I saw that the row cipher with key [2,3,7,4,5,1,6] produced a plain English text.

Cipher Text:

thens aisse tting firet othef uture ofthe inter netsn owden

decla reddu ringa livec hatat theso uthby south westi ntera

ctive festi valon march tenth speak ingdi rectl ytoth eamer

icanp eople forth efirs ttime since fleei ngthe count ryinj

uneof lasty earsn owden tookt heopp ortun ityto reite rateh

isstr ongly heldb elief thato urfed eralg overn menth asbur

nedth eparc hment onwhi chour fourt hamen dment right soffr

eedom andde mocra cywer etran scrib edbyo urfor efath ersce

nturi esago regar dless ofyou rtake onsno wdenh issag aisju

stasm allch apter inala rgers toryt henig htbef oresn owden

sappe aranc ethec bsnew sshow sixty minut esair edari vetin

gandf right ening expos eonda tabro kerso rgani zatio nstha

tcoll ectan alyse andse llour perso nalin forma tiona sacom

modit ywere notju sttal kinge mails andco ntact lists weret

alkin gourm edica tions habit sandd ailya ctivi tiesl estyo

uthin kdata broke ringe xists asafr ingei ndust rymad eupof

afewd ereli ctsan dfrus trate dform erhac kerst hetru thisd

atabr okeri ngisa hugei ndust rycon sisti ngoft housa ndsof

compa niesb uying andse lling ourpr ivacy toadv ertis ersth

egove rnmen tando therb roker stheg overn mentd oesnt drive

thisi ndust ryasm uchas willi nglyp artic ipate withi nitth

ereal guilt ypart iesar ether esear chers adver tiser sandi

ntern etcom panie swhoe ncour agesu chbeh avior ifnot state

their finan cialr evenu emode lenti relyu ponit sixty minut

esfor examp lepoi ntedo uthow thela rgest datab roker hasco

llect edona verag efift eenhu ndred tidbi tsofi nform ation

onmor ethan twohu ndred milli oname rican sthes earen otsus

pecte dterr orist sbutr ather every dayci tizen shavi ngthe

ironl inedi aries soldu ndern eatht hemwi thout their knowl

edgeo rappr ovala sthis situa tionc omest oligh teven furth

erwem ustas kours elves twoqu estio nsare weoka yhavi ngour

onlin eacti vitie sandc onten tmine dandm oreim porta ntwha

tcanw edoab outit snowd enand other sargu ethat thebe stwea

ponwo uldbe aneww orldi ntern etord erinw hiche ndtoe ndenc

rypti onsol ution smake theme ansem ploye dbyth ensaa ndoth

ersim poesi lsb

Plain English:

"The NSA is setting fire to the future of the Internet,” Snowden declared during a live chat at the South by Southwest Interactive Festival on March tenth. Speaking directly to the American people for the first time since fleeing the country in June of last year, Snowden took the opportunity to reiterate his strongly held belief that our federal government has burned the parchment on which our fourth amendment rights of freedom and democracy were transcribed by our forefathers centuries ago.

Regardless of your take on Snowden, his saga is just a small chapter in a larger story. The night before Snowden’s appearance, the CBS news show Sixty aired a riveting and frightening expose’ on data brokers - organizations that collect, analyze, and sell our personal information as a commodity. We’re not just talking emails and contact lists; we’re talking our medications, habits, and daily activities. Lest you think data brokering exists as a fringe industry made up of a few derelicts and frustrated former hackers, the truth is data brokering is a huge industry consisting of thousands of companies buying and selling our privacy to advertisers, the government, and other brokers.

The government doesn’t drive this industry as much as willingly participate within it. The real guilty parties are the researchers, advertisers, and Internet companies who encourage such behavior -- if not state their financial revenue model entirely upon it. Sixty Minutes for example

pointed out how the largest data broker has collected on average fifteen hundred tidbits of information on more than two hundred million Americans. These are not suspected terrorists but rather everyday citizens having their online diaries sold underneath them without their knowledge or approval. As this situation comes to light even further, we must ask ourselves two questions: are we okay having our online activities and content mined? And, more important, what can we do about it? Snowden and others argue that the best weapon would be a new world internet order in which end-to-end encryption solutions make the means employed by the NSA and others impoesilsb (sic).

**Cipher 3:**

Ran frequency distribution: clearly polyalphabetic substitution

IC = 0.04202 = period of about 8

Kasiski with 5-size words = intervals are 594, 444, 564 and 276 – all divide by 6

Ran frequency distribution over 6 alphabets – each alphabet was a clear shift cipher, therefore it’s a Vigenere cipher. Key = POLISH

Cipher Text:

theba ckdoo rmalw aredi scove redon aserv erata usman ufact

uring compa nywas spott edand clean edupw ithin twent yfour

hours ofits impla ntati onand byall accou ntsth atpar ticul

arcyb eresp ionag eatta ckhad beent hwart edbut thene xtday

twone wback doors weres potte dontw oothe rserv ersan dthec

ompan yreal izedi tsinc ident respo nseop erati onhad notbe

ensos ucces sfula ftera llwek newth etroj anont hatfi rstsy

stemb utwem issed outon acoup leofo therm achin esass oonas

wecle anedu ptheo nemac hinet heret heywe rethe nextd aysay

sthei rsecu rityt eamme mbera tthem anufa cturi ngfir mwhos

pokeo nthec ondit ionth athis compa nynot benam edthe yhadm

ovedl atera llyan dinst alled twoco mplet elydi ffere ntbac

kdoor ssoio csind icato rsofc ompro mises ignat uresw ereus

eless wemad eadec ision tooqu ickly youha vetob equic kandt

horou ghthi swasa learn ingle ssonf orusn owtha torga nizat

ionsa ndthe secur ityin dustr yfort hemos tpart havea ccept

edthe uglyt rutht hatbr eache sarei nevit ablea ndthe badgu

ysare going tofin daway toget insid ethen ewfoc usiso nhowy

oures pondt oanat tacko ratta ckatt empta ndmin imize theda

magem egare taile rtarg etsmi sstep sinit spost breac hoper

ation haved riven homea newse nseof urgen cyine stabl ishin

gasol idinc ident respo nseop erati ontha tisas mucha boutp

rotec tingd ataas itisa boutp rotec tingt hecor porat eimag

einci dentr espon seiri sbeco mingp artan dparc elofa secur

ityst rateg yexpe rtssa ymore thans ixtyp ercen tofor ganiz

ation ssayt heyha veirp lansi nplac eacco rding toare centr

eport byarb ornet works andth eecon omist intel ligen ceuni

twhic hsurv eyeds ometh reehu ndred sixty cleve lorbo ardle

velbu sines sexec utive sarou ndthe globe onthe irinc ident

respo nsepo sture sacco rding tothe dataa round twoth irdso

ftheo rgani zatio nssay asucc essfu lands mooth incid entre

spons eoper ation inthe faceo fabre achco uldul timat elyen

hance their reput ation thesa vingf acepi eceis bigsa ysdan

holde ndire ctoro farbo rsase rt

Plain English:

The backdoor malware discovered on a server at a US manufacturing company was spotted and cleaned up within twenty-four hours of its implantation, and by all accounts that particular cyber espionage attack had been thwarted but the next day two new backdoors were spotted on two other servers and the company realized its incident response operation had not been so successful after all.

“We knew the trojan on that first system but we missed out on a couple of other machines. As soon as we cleaned up the one machine, there they were the next day,” says the IR security team member at the manufacturing firm who spoke on the condition that his company not be named. “They had moved laterally and installed two completely different backdoors so IOCs (indicators of compromise) signatures were useless. We made a decision too quickly. You have to be quick and thorough. This was a learning lesson for us.”

Now that organizations and the security industry for the most part have accepted the ugly truth that breaches are inevitable and the bad guys are going to find a way to get inside, the new focus is on how you respond to an attack or attack attempt and minimize the damage. Mega retailer Target’s missteps in its post-breach operation have driven home a new sense of urgency in establishing a solid incident response operation that is as much about protecting data as it is about protecting the corporate image.

Incident response (IR) is becoming part and parcel of a security strategy, experts say. More than sixty percent of organizations say they have IR plans in place, according to a recent report by Arbor networks and the economist intelligence unit which surveyed some three hundred sixty C-level or board level business executives around the globe on their incident response postures. According to the data, around two thirds of the organizations say a successful and smooth incident response operation in the face of a breach could ultimately enhance their reputation. “The saving face piece is big,” says Dan Holden, director of Arbor’s ASERT

**Cipher 4:**

IC = 0.0652331, so monoalphabetic.

Frequency distribution does not match English. The general distribution of the columns suggests a substitution cipher, thus monoalphabetic substitution cipher

1, I assumed the letter with the highest frequency to be equal to e, in this case l with 144 occurrences

2, I did a kasiski search of 4 letters and found 'pEEx' and 'kEEg' were both seen 2 times.

3, I looked at the frequency graph and noticed 'p' and 'x' were of the more common letter groups, so I compared this to the 8 other (excluding 'E') more common letters from the normal alphabet frequency.

4, p could be 'a,h,i,n,o,r,s,t' and x could be 'a,h,i,n,o,r,s,t' (p != x)

5, the only English-like word I could find was 'SEEN', So I let S = p and N = x

6, I noticed now that the 'kEEg' in the cipher text was potentially a word 'SdkkEEg' because it is extremely uncommon for repeating letters to happen two times in a row that are not a part of a word.

7, The only word that can match that criteria I could think of was 'SUCCEED', so I let U = d, C = k and D = g

8, I didn't find any other words that could represent another word so I decided to let the second highest frequency letter 'a' be the second highest normal alphabet frequency letter 'T' as it seemed logical, thus T = a.

9, The phrase 'SUCCEED rN' appeared and the logical assumption I made was that I = r for 'SUCCEED IN'

10, I saw 'DISEoSE' and I mad the logical assumption that the word is disease, thus A = o

11, I was looking through different repeated strings using kasisiki search and when i came to string length 13 I found 'SUyEiSTITIsUS' repeated three times and this looks exactly like 'superstitious'. So I let P = y, R = i, O = s.

12, At the start, the phrase 'I Au A' looks like 'I AM A' so I let M = u

13, 'I AM A SICb MAN', assuming K = b

14, 'SPITEhUw' = 'SPITEFUL', thus F = h, L = w

15, 'UNATTRACTIzE MAN I fELIEzE' = 'UNATTRACTIVE MAN I BELIEVE', thus V = z, B = f

16, 'I jAVE SEEN MeSELF TjAT I ONLe cANTED' = 'I HAVE SEEN MYSELF THAT I ONLY WANTED', thus H = j, Y = e, W = c

17, 'THOUtH OFCOURSE I CANT EmPLAIN' = 'THOUGH OFCOURSE I CANT EXPLAIN', thus G = t, X = m

18, 'INqURING' = 'INJURING', thus J = q

19, v and n were not found in the cipher text so they must be either v or n each.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| o | f | k | g | l | h | t | j | r | q | b | w | u | x | s | y | v,n | i | p | a | d | z | c | m | e | n,v |

Plain English:

I am a sick man. I am a spiteful man. I am an unattractive man. I believe my liver is diseased, however I know nothing at all about my disease and do not know for certain what ails me. I don’t consult a doctor for it and never have, though I have a respect for medicine and doctors.

Besides, I am extremely superstitious, sufficiently so to respect medicine anyway. I am well educated enough not to be superstitious, but I am superstitious. No, I refuse to consult a doctor from spite that you probably will not understand. Well, I understand it, though of course I can’t explain who it is precisely that I am mortifying in this case by my spite. I am perfectly well aware that I cannot pay out the doctors by not consulting them. I know better than anyone that by all this I am only injuring myself and no one else, but still if I don’t consult a doctor it is from spite.

My liver is bad. Well, let it get worse I have been going on like that for a long time - twenty years now. I am forty. I used to be in the government service but am no longer. I was a spiteful official. I was rude and took pleasure in being so. I did not take bribes you see, so I was bound to find a recompense in that at least a poor jest. But I will not scratch it out. I wrote it thinking it would sound very witty, but now that I have seen myself that I only wanted to show off in a despicable way. I will not scratch it out on purpose.

When petitioners used to come for information, to the table at which is at. I used to grind my teeth at them and felt intense enjoyment when I succeeded in making anybody unhappy. I almost did succeed for the most part, they were all timid people of course. They were petitioners.