Assignment 1 Report

Cipher 1

IC (1 alphabet) = 0.065348, therefore not polyalphabetic substitution.

Frequency distribution = equivalent to plain English, therefore transposition.

No obvious anagrams or patterns in the first 10 characters, so likely column transposition.

IC over 20 alphabets to determine period.  
 Highest IC: IC[8] = 0.08531 and IC[16] = 0.0799

Tried to brute force the cipher by getting all permutations across period 8 – since I had no clues, narrowed down to only those containing ‘the’. Still produced over 7000 pages worth of text. No progress was made.

Plaintext: Unsolved.

Cipher 2

IC (1 alphabet) = 0.040907, therefore polyalphabetic substitution.

Running Kasiski with a word length of 4:  
 Shortest values are 16 and 32; period = 4/8/16?

Frequency graph with 4 alphabets:

No obvious correlation to plain English.  
 Highest values (likely E):  
 0 = { V, C }, 1 = { X, N }, 2 = { I, T }, 3 = { F, U, D, H }  
 Vigenere (A candidates):  
 0 = { R, X }, 1 = { U, J }, 2 = { P, E }, 3 = { B, Q, Z, D }  
 Beauford (A candidates):  
 0 = { Z, G }, 1 = { C, R }, 2 = { L, X }, 3 = { J, Y, H, L }

Frequency graph with 8 alphabets:

Correlates to plain English (5 place gap, then sharp incline to the right – Vigenere)

0: A = C, 1: A = U, 2: A = P, 3: A = B  
 4: A = O, 5: A = A, 6: A = R, 7: A = D

Key: CUPBOARD

Plaintext: Grandpa in the north sends a telegram money order for five pounds for the baby Alphie. Mam wants to cash it but she can’t go far from the bed. Dad says he’ll cash it at the post office. She tells Malachy and me to go with him. He cashes it and tells us “allright boys, go home and tell your mother I’ll be home in a few minutes.”   
Malachy says “Dad, you’re not to go to the pub! Mam said you are to bring home the money. You are not to drink the pint.”  
“Now, now, son. Go home to your mother.”   
“Dad, give us the money. That money is for the baby.”

“Now Francis, don’t be a bad boy. Do what your father tells you.”  
He walks away from us and into Souths pub. Mam is sitting by the fireplace with Alphie in her arms. She shakes her head.

“He went to the pub didn’t he?”  
“He did.”  
“I want ye to go back down to that pub and read him out of it! I want ye to stand in the middle of the pub and tell every man your father is drinking the money for the baby! Ye are to tell the world there isn’t a scrap of food in this house, not a lump of coal to start the fire, not a drop of milk for the baby’s bottle!”

We walk through the streets and Malachy practices his speech at the top of his voice.  
“Dad! Dad, that five pounds is for the new baby! That’s not for the drink! The child is above in the bed bawling and roaring for his milk and you are drinking the pint!”

He’s gone from souths pub. Malachy still wants to stand and make his speech but I tell him we have to hurry and look in other pubs before Dad drinks the whole five pounds. We can’t find him in other pubs either. He knows Mam would come for him or send us and there are so many pubs at this end of limerick and beyond. We could be looking for a month. We have to tell mam there is no sign of him and she tells us we are pure useless.  
“Oh Jesus I wish I had my strength and I’d search every pub in limerick! I’d tear the mouth out of his head!”

So I would go on go back down and try all the pubs around the railway station and try Naughton’s fish and chip shop. I have to go by myself because Malachy has the runs and cant stray far from the bucket. I search all the pubs on Parnell street and around I look into the snugs where the women drink and in all the mens’ lavatories. I’m hungry but I’m afraid to go home till I find my father. He’s not in Naughton’s fish and chip shop but there’s a drunken man asleep at a table in the corner and his fish and chips are on the floor in their limerick leader wrapping and if I don’t get them the cat will. So I shove them under my jersey and I’m out the door and up the street to sit on the steps at the railway station, eat my fish and chips, watch the drunken sailors pass by with the girls that giggle, thank the drunken man in my mind for drowning the fish and chips in vinegar and smothering them in salt and then I remember that if I die tonight I’m in a state of sin for stealing and I could go straight to hell stuffed with fish and chips but its Saturday and if the priests are still in the confession boxes I can clear my soul after my feed.

The Dominican church is just up Glentworth street.  
“Bless me father for I have sinned. It’s a fortnight since my last confession.” I tell him the usual sins and then I stole fish and chips from a drunken man.  
“Why, my child?”  
“I was hungry, Father.”  
“And why were you hungry?”  
“There was nothing in my belly, Father.”  
He says nothing and even though it’s dark I know he is shaking his head.  
“My dear child, why can’t you go home and ask your mother for something?”  
“Because she sent me out looking for my father in the pubs, Father, and I couldn’t find him and she hasn’t a scrap in the house because he’s drinking the five pounds Grandpa sent from the north for the new baby and she is raging by the fire because I can’t find my father.”  
I wonder if this priest is asleep because he is very quiet till he says:  
“My child, is it here I hear the sins of the poor? I assign the penance, I bestow absolution, I should be on my knees washing their feet. Do you understand me, my child?”  
I tell him I do but I don’t go home.  
“Child, pray for me.”  
“No penance, Father?”   
“No, my child.”   
“I stole the fish and chips. I’m doomed.”   
“You’re forgiven. Go pray for me.”  
He blesses me in Latin, talks to himself in English and I wonder what I did to him.

Cipher 3

IC (1 alphabet) = 0.042431, therefore polyalphabetic substitution.

Running Kasiski with a word length of 4:  
 Shortest values are 20 and 30; period = 5/10?

Frequency graph with 5 alphabets:

No obvious correlation to plain English.

Frequency graph with 10 alphabets:

Correlates to plain English (5 place gap, then sharp incline to the left – Beauford)

0: A = I, 1: A = R, 2: A = R, 3: A = E, 4: A = L,  
5: A = E, 6: A = V, 7: A = A, 8: A = N, 9: A = T

Key = IRRELEVANT

Plaintext = Two thousand eighteen may be remembered as the year of the Facebook scandal and rightly so. The Cambridge Analytica fiasco, Mark Zuckerberg’s congressional testimony, a massive hack and revelations of corporate smear campaigns were only the tip of the iceberg. But many more companies mishandled consumer privacy too from the Strava heat map exposing military locations in January to the gigantic Marriot hack discovered in November. Companies across Silicon Valley and beyond made big mistakes with consumer data this year and law makers and the public have taken notice. Tech companies putting their profits before your privacy.

The problem that came into focus in two thousand eighteen was not just hacks breaches or unauthorized bad guys breaking into systems. Instead the worst privacy actors were the tech companies themselves. Harvesting of mountains of users’ data and employing flawed systems to use and share it. Facebook’s Cambridge Analytica scandal, for example, was the result of a feature of Facebook’s graph epi. In this case Facebook was designed to collect as much user information as possible and then share it indiscriminately with third party developers. In a set of newly revealed emails from two thousand twelve, Mark Zuckerberg acknowledged that he knew. “We leak info to developers but didn’t think there was enough strategic risk to do anything about it.”

Google’s social network didn’t perform much better. The final nails in the coffin of Google Plus came with two bugs: one quietly announced in October that exposed the personal information of half a million users, and an even bigger one revealed in December. Unlike Facebook’s Cambridge Analytica problems, these bugs were unintended engineering mistakes but they exposed users to the same risk the exposure of users’ personal information to third party developers without anything resembling informed consent. Two thousand eighteen also saw tech companies creep further into our wallets and our homes. Facebook and Google reportedly partnered with banks and bought financial data in secret, raising serious privacy concerns about giving companies access to yet another sensitive category of information.

The torrent of data related scandals this year drove new popular awareness of privacy issues. Big companies made big new investments in the internet of things with Facebook introducing Portal and Google introducing the Home hub, both designed to put their manufacturers at the center of home life.

Companies also gave users new reasons to question the privacy limits on their home assistant devices. One couple’s Amazon Alexa silently recorded one of their conversations and sent it to a colleague, and Facebook was unable to clearly say whether data collected through portal could or would be used for targeting ads. The torrent of data-related scandals this year drove new popular awareness of privacy issues. The Pew Research Center found that a whopping seventy four percent of American adults had adjusted their Facebook privacy settings taken a break from the platform or deleted its app from their phones. More broadly it also found that people are worried about their personal information online and that the vast majority of American adults say it is important to them to be in control of who can get information about them.

Cipher 4

IC (1 alphabet) = 0.066257, therefore not polyalphabetic substitution.

Frequency distribution = not equivalent to plain English, therefore non-transposition cipher.

It seems to be a monoalphabetic substitution cipher where each ciphertext letter corresponds to a plaintext letter. The next step is to study the frequency distribution to see which letters have the highest distribution. I discover that:

if ci = pi, where c is the ciphertext and p is the plaintext,  
v = T, t = A, e = E, c = D.

I then perform a Kasiski test for bigrams and trigrams, discovering:

w = O, o = I, x = N, d = G, n = R

In Microsoft Word (with case sensitivity on) I replace each of the revealed lower-case ciphertext characters with upper-case plaintext. This leaves a solid base to work out the remaining ciphertext by comparing frequency distributions, bigrams and trigrams, over the course of two hours or so.

Plaintext = Cyber security refers to a set of techniques used to protect the integrity of networks, programs and data from attack, damage or unauthorized access. According to Forbes, the global cyber security market is expected to reach hundred seventy billion by twenty twenty. This rapid market growth is being fueled by an array of technology trends, including the onslaught of initiatives with ever-evolving security requirements like bring your own device (BYOD) and the internet of things (IOT), the rapid adoption of cloud-based applications and workloads extending security needs beyond the traditional data center, and stringent data protection mandates such as the European Union’s General Data Protection Regulation and the National Institute of Security Technology (NIST) Cyber Security Framework.

Why cyber security is required: the core functionality of cyber security involves protecting information and systems from major cyber threats. These cyber threats take many forms e.g. application attacks, malware, ransomware, phishing, exploit kits. Unfortunately, cyber adversaries have learned to launch automated and sophisticated attacks using these tactics at lower and lower costs. As a result, keeping pace with cyber security strategy and operations can be a challenge, particularly in government and enterprise networks where, in their most disruptive form, cyber threats often take aim at secret political, military or infrastructural assets of a nation or its people. Some of the common threats are outlined below in more detail.

Cyberterrorism is the disruptive use of information technology by terrorist groups to further their ideological or political agenda. This takes the form of attacks on networks, computer systems and telecommunication infrastructures.

Cyberwarfare involves nation states using information technology to penetrate another nation’s networks to cause damage or disruption. In the US and many other nations, cyber warfare has been acknowledged as the fifth domain of warfare, following land, sea, air, and space. Cyber warfare attacks are primarily executed by hackers who are well-trained in exploiting the intricacies of computer networks and operate under the auspices and support of nation states. Rather than shutting down a target’s key networks, a cyber warfare attack may intrude into networks to compromise valuable data, degrade communications, impair such infrastructural services as transportation and medical services, or interrupt commerce.

Cyber espionage is the practice of using information technology to obtain secret information without permission from its owners or holders. Cyber espionage is most often used to gain strategic economic, political or military advantage and is conducted using cracking techniques and malware.