1 Warmup for Frequency Analysis

1. The most frequently occuring word in the text is *the*.
2. The longest word in the text is *Nationalgymnasiummuseumsanatoriumandsuspensoriumsordinaryprivatdocentgeneralhistoryspecialprofessordoctor*.
3. The longest word that occurs more than 25 times in the text is *with*.

2 Basic Encryption

1. The key used to encrypt the transmission was *snowboard*.
2. The second transmission was an encrypted version of section 13 of the text.

3 Breaking Viginére

1. The length of the key is 5.
2. The key is *SWING*.

4 Breaking a Two-Time Pad

4.1 Figuring out the pad

In order to break the two-time pad one can rely on the properties of the *XOR* operation. Consider two streams of ciphertext C_1 and C_2 of equal length. These two ciphers were produced by the message streams M_1 and M_2 by performing the following operations:

$$C_1[i] = M_1[i] \oplus P[i]$$
$$C_2[i] = M_2[i] \oplus P[i]$$

where $X[i]$ denotes the i_{th} byte of the stream X and P denotes the pad stream. Thus given both C_1 and C_2 we can compute:

$$B[i] = C_1[i] \oplus C_2[i]$$
$$B[i] = M_1[i] \oplus P[i] \oplus M_2[i] \oplus P[i]$$

then by the commutativity and associativity of $\oplus$ we obtain:

$$B[i] = M_1[i] \oplus M_2[i] \oplus P[i] \oplus P[i]$$

then by the identity $v \oplus v = 0$ and the fact that 0 acts as an identity under $\oplus$ we can write:

$$B[i] = M_1[i] \oplus M_2[i]$$

Now suppose that we know that a particular series of bytes occurs in M_1, let this series of bytes be called K with length n. Then there exists some i such that:

$$B[i + t] \oplus K[t] = M_2[i] \qquad \forall\, t \in \{1..n\}$$

Thus if we can determine some stream of bytes K that exists in either M_1 or M_2 we can begin to decrypt both of the messages. In this case we know that the most frequent word in the text is *the*. Thus we compute $B[i + t] \oplus K[t]$ for $K = \{$' ', 't', 'h', 'e', ' '$\}$ for all $i \in l$ where l is the length of B. The results of this computation are then scanned for streams of length 5 that could plausibly appear in either M_1 or M_2. In our case this is straightforward since the possible message space for the plaintext is relatively small, in this

case the text of *ulysses*.

In my case I noticed that the characters *emmed* were one of the results of the computation detailed above. This series of characters appears in only two places in *ulysses*. As such, I *XOR*'d both portions of the *ulysses* which began with *emmed* with the portion of the keystream that yielded this series of characters when *XOR*'d with the the text *the*. One of these yielded a jumble of nonprintable ASCII while the other yielded an excerpt from *ulysses*. From this point, determining the contents of both M_1 and M_2 is fairly straightforward.

A Two-Time Pad Decryption

A.1 First Message

May I trespass on your valuable space. That doctrine of laissez faire which so often in our history. Our cattle trade. The way of all our old industries. Liverpool ring which jockeyed the Galway harbour scheme. European conflagration. Grain supplies through the narrow waters of the channel. The pluterperfect imperturbability of the department of agriculture. Pardoned a classical allusion. Cassandra. By a woman who was no better than she should be. To come to the point at issue. —I don't mince words, do I? Mr Deasy asked as Stephen read on. Foot and mouth disease. Known as Koch's preparation. Serum and virus. Percentage of salted horses. Rinderpest. Emperor's horses at Mürzsteg, lower Austria. Veterinary surgeons. Mr Henry Blackwood Price. Courteous offer a fair trial. Dictates of common sense. Allimportant question. In every sense of the word take the bull by the horns. Thanking you for the hospitality of your columns. —I want that to be printed and read, Mr Deasy said. You will see at the next outbreak they will put an embargo on Irish cattle. And it can be cured. It is cured. My cousin, Blackwood Price, writes to me it is regularly treated and cured in Austria by cattledoctors there. They offer to come over here. I am trying to work up influence with the department. Now I'm going to try publicity. I am surrounded by difficulties, by... intrigues by... backstairs influence by... He raised his forefinger and beat the air oldly before his voice spoke. —Mark my words, Mr Dedalus, he said. England is in the hands of the jews. In all the highest places: her finance, her press. And they are the signs of a nation's decay. Wherever they gather they eat up the nation's vital strength. I have seen it coming these years. As sure as we are standing here the jew merchants are already at their work of destruction. Old England is dying. He stepped swiftly off, his eyes coming to blue life as they passed a broad sunbeam. He faced about and back again. —Dying, he said again, if not dead by now. The harlot's cry from street to street Shall weave old England's windingsheet. His eyes open wide in vision stared sternly across the sunbeam in which he halted. —A merchant, Stephen said, is one who buys cheap and sells dear, jew or gentile, is he not? —They sinned against the light, Mr Deasy said gravely. And you can see the darkness in their eyes. And that is why they are wanderers on the earth to this day. On the steps of the Paris stock exchange the goldskinned men quoting prices on their gemmed fingers. Gabble of geese. They swarmed loud, uncouth about the temple, their heads thickplotting under maladroit silk hats. Not theirs: these clothes, this speech, these gestures. Their full slow eyes belied the words, the gestures eager and unoffending, but knew the rancours massed about them and knew their zeal was vain. Vain patience to heap and hoard. Time surely would scatter all. A hoard heaped by the roadside: plundered and passing on. Their eyes knew their years of wandering and, patient, knew the dishonours of their flesh. —Who has not? Stephen said. —What do you mean? Mr Deasy asked. He came forward a pace and stood by the table. His underjaw fell sideways open uncertainly. Is this old wisdom? He waits to hear from me. —History, Stephen said, is a nightmare from which I am trying to awake. From the playfield the boys raised a shout. A whirring whistle: goal. What if that nightmare gave you a back kick? —The ways of the Creator are not our ways, Mr Deasy said. All human history moves towards one great goal, the manifestation of God. Stephen jerked his thumb towards the window, saying: —That is God. Hooray! Ay! Whrrwhee! —What? Mr Deasy asked. —A shout in the street, Stephen answered, shrugging his shoulders. Mr Deasy looked down and held for awhile the wings of his nose tweaked between his fingers. Looking up again he set them free. —I am happier than you are, he said. We have committed many errors and many sins. A woman brought sin into the world. For a woman who was no better than she should be, Helen, the runaway wife of Menelaus, ten years the Greeks made war on Troy. A faithless wife first brought the strangers to our shore here, MacMurrough's wife and her leman, O'Rourke, prince of Breffni. A woman too

brought Parnell low. Many errors, many failures but not the one sin. I am a struggler now at the end of my days. But I will fight for the right till the end. For Ulster will fight And Ulster will be right. Stephen raised the sheets in his hand. —Well, sir, he began. —I foresee, Mr Deasy said, that you will not remain here very long at this work. You were not born to be a teacher, I think. Perhaps I am wrong. —A learner rather, Stephen said. And here what will you learn more? Mr Deasy shook his head. —Who knows? he said. To learn one must be humble. But life is the great teacher. Stephen rustled the sheets again. —As regards these, he began. —Yes, Mr Deasy said. You have two copies there. If you can have them published at once. Telegraph. Irish Homestead. —I will try, Stephen said, and let you know tomorrow. I know two editors slightly. —That will do, Mr Deasy said briskly. I wrote last night to Mr Field, M.P. There is a meeting of the cattletraders' association today at the City Arms hotel. I asked him to lay my letter before the meeting. You see if you can get it into your two papers. What are they? —The Evening Telegraph... —That will do, Mr Deasy said. There is no time to lose. Now I have to answer that letter from my cousin. —Good morning, sir, Stephen said, putting the sheets in his pocket. Thank you. —Not at all, Mr Deasy said as he searched the papers on his desk. I like to break a lance with you, old as I am. —Good morning, sir, Stephen said again, bowing to his bent back. He went out by the open porch and down the gravel path under the trees, hearing the cries of voices and crack of sticks from the playfield. The lions couchant on the pillars as he passed out through the gate: toothless terrors. Still I will help him in his fight. Mulligan will dub me a new name: the bullockbefriending bard. —Mr Dedalus! Running after me. No more letters, I hope. —Just one moment. —Yes, sir, Stephen said, turning back at the gate. Mr Deasy halted, breathing hard and swallowing his breath. —I just wanted to say, he said. Ireland, they say, has the honour of being the only country which never persecuted the jews. Do you know that? No. And do you know why? He frowned sternly on the bright air. —Why, sir? Stephen asked, beginning to smile. —Because she never let them in, Mr Deasy said solemnly. A coughball of laughter leaped from his throat dragging after it a rattling chain of phlegm. He turned back quickly, coughing, laughing, his lifted arms waving to the air. —She never let them in, he cried again through his laughter as he stamped on gaitered feet over the gravel of the path. That's why. On his wise shoulders through the checkerwork of leaves the sun flung spangles, dancing coins. [3] Ineluctable modality of the visible: at least that if no more, thought through my eyes. Signatures of all things I am here to read, seaspawn and seawrack, the nearing tide, that rusty boot. Snotgreen, bluesilver, rust: coloured signs. Limits of the diaphane. But he adds: in bodies. Then he was aware of them bodies before of them coloured. How? By knocking his sconce against them, sure. Go easy. Bald he was and a millionaire, maestro di color che sanno. Limit of the diaphane in. Why in? Diaphane, adiaphane. If you can put your five fingers through it it is a gate, if not a door. Shut your eyes and see. Stephen closed his eyes to hear his boots crush crackling wrack and shells. You are walking through it howsomever. I am, a stride at a time. A very short space of time through very short times of space. Five, six: the nacheinander. Exactly: and that is the ineluctable modality of the audible. Open your eyes. No. Jesus! If I fell over a cliff that beetles o'er his base, fell through the nebeneinander ineluctably! I am getting on nicely in the dark. My ash sword hangs at my side. Tap with it: they do. My two feet in his boots are at the ends of his legs, nebeneinander. Sounds solid: made by the mallet of Los Demiurgos. Am I walking into eternity along Sandymount strand? Crush, crack, crick, crick. Wild sea money. Dominie Deasy kens them a'. Won't you come to Sandymount, Madeline the mare? Rhythm begins, you see. I hear. A catalectic tetrameter of iambs marching. No, agallop: deline the mare. Open your eyes now. I will. One moment. Has all vanished since? If I open and am for ever in the black adiaphane. Basta! I will see if I can see. See now. There all the time without you: and ever shall be, world without end. They came down the steps from Leahy's terrace prudently, Frauenzimmer: and down the shelving shore flabbily, their splayed feet sinking in the silted sand. Like me, like Algy, coming down to our mighty mother. Number one swung lourdily her midwife's bag, the other's gamp poked in the beach. From the liberties, out for the day. Mrs Florence MacCabe, relict of the late Patk MacCabe, deeply lamented, of Bride Street. One of her sisterhood lugged me squealing into life. Creation from nothing. What has she in the bag? A misbirth with a trailing navelcord, hushed in ruddy wool. The cords of all link back, strandentwining cable of all flesh. That is why mystic monks. Will you be as gods? Gaze in your omphalos. Hello. Kinch here. Put me on to Edenville. Aleph, alpha: nought, nought, one. Spouse and helpmate of Adam Kadmo

A.2 Second Message

My kneecap is hurting me. Ow. That's better. The priest took a stick with a knob at the end of it out of the boy's bucket and shook it over the coffin. Then he walked to the other end and shook it again. Then he came back and put it back in the bucket. As you were before you rested. It's all written down: he has to do it. —Et ne nos inducas in tentationem. The server piped the answers in the treble. I often thought it would be better to have boy servants. Up to fifteen or so. After that, of course ... Holy water that was, I expect. Shaking sleep out of it. He must be fed up with that job, shaking that thing over all the corpses they trot up. What harm if he could see what he was shaking it over. Every mortal day a fresh batch: middleaged men, old women, children, women dead in childbirth, men with beards, baldheaded businessmen, consumptive girls with little sparrows' breasts. All the year round he prayed the same thing over them all and shook water on top of them: sleep. On Dignam now. —In paradisum. Said he was going to paradise or is in paradise. Says that over everybody. Tiresome kind of a job. But he has to say something. The priest closed his book and went off, followed by the server. Corny Kelleher opened the sidedoors and the gravediggers came in, hoisted the coffin again, carried it out and shoved it on their cart. Corny Kelleher gave one wreath to the boy and one to the brother-in-law. All followed them out of the sidedoors into the mild grey air. Mr Bloom came last folding his paper again into his pocket. He gazed gravely at the ground till the coffincart wheeled off to the left. The metal wheels ground the gravel with a sharp grating cry and the pack of blunt boots followed the trundled barrow along a lane of sepulchres. The ree the ra the ree the ra the roo. Lord, I mustn't lilt here. —The O'Connell circle, Mr Dedalus said about him. Mr Power's soft eyes went up to the apex of the lofty cone. —He's at rest, he said, in the middle of his people, old Dan O'. But his heart is buried in Rome. How many broken hearts are buried here, Simon! —Her grave is over there, Jack, Mr Dedalus said. I'll soon be stretched beside her. Let Him take me whenever He likes. Breaking down, he began to weep to himself quietly, stumbling a little in his walk. Mr Power took his arm. —She's better where she is, he said kindly. —I suppose so, Mr Dedalus said with a weak gasp. I suppose she is in heaven if there is a heaven. Corny Kelleher stepped aside from his rank and allowed the mourners to plod by. —Sad occasions, Mr Kernan began politely. Mr Bloom closed his eyes and sadly twice bowed his head. —The others are putting on their hats, Mr Kernan said. I suppose we can do so too. We are the last. This cemetery is a treacherous place. They covered their heads. —The reverend gentleman read the service too quickly, don't you think? Mr Kernan said with reproof. Mr Bloom nodded gravely looking in the quick bloodshot eyes. Secret eyes, secretsearching. Mason, I think: not sure. Beside him again. We are the last. In the same boat. Hope he'll say something else. Mr Kernan added: —The service of the Irish church used in Mount Jerome is simpler, more impressive I must say. Mr Bloom gave prudent assent. The language of course was another thing. Mr Kernan said with solemnity: —I am the resurrection and the life. That touches a man's inmost heart. —It does, Mr Bloom said. Your heart perhaps but what price the fellow in the six feet by two with his toes to the daisies? No touching that. Seat of the affections. Broken heart. A pump after all, pumping thousands of gallons of blood every day. One fine day it gets bunged up: and there you are. Lots of them lying around here: lungs, hearts, livers. Old rusty pumps: damn the thing else. The resurrection and the life. Once you are dead you are dead. That last day idea. Knocking them all up out of their graves. Come forth, Lazarus! And he came fifth and lost the job. Get up! Last day! Then every fellow mousing around for his liver and his lights and the rest of his traps. Find damn all of himself that morning. Pennyweight of powder in a skull. Twelve grammes one pennyweight. Troy measure. Corny Kelleher fell into step at their side. —Everything went off A1, he said. What? He looked on them from his drawling eye. Policeman's shoulders. With your tooraloom tooraloom. —As it should be, Mr Kernan said. —What? Eh? Corny Kelleher said. Mr Kernan assured him. —Who is that chap behind with Tom Kernan? John Henry Menton asked. I know his face. Ned Lambert glanced back. —Bloom, he said, Madame Marion Tweedy that was, is, I mean, the soprano. She's his wife. —O, to be sure, John Henry Menton said. I haven't seen her for some time. She was a finelooking woman. I danced with her, wait, fifteen seventeen golden years ago, at Mat Dillon's in Roundtown. And a good armful she was. He looked behind through the others. —What is he? he asked. What does he do? Wasn't he in the stationery line? I fell foul of him one evening, I remember, at bowls. Ned Lambert smiled. —Yes, he was, he said, in Wisdom Hely's. A traveller for blottingpaper. —In God's name, John Henry Menton said, what did she marry a coon like that for? She had plenty of game in her then. —Has still, Ned Lambert said. He does some canvassing for ads. John Henry Menton's large eyes stared ahead. The barrow turned into a side lane. A portly man, ambushed among the grasses, raised his hat in

homage. The gravediggers touched their caps. —John O'Connell, Mr Power said pleased. He never forgets a friend. Mr O'Connell shook all their hands in silence. Mr Dedalus said: —I am come to pay you another visit. —My dear Simon, the caretaker answered in a low voice. I don't want your custom at all. Saluting Ned Lambert and John Henry Menton he walked on at Martin Cunningham's side puzzling two long keys at his back. —Did you hear that one, he asked them, about Mulcahy from the Coombe? —I did not, Martin Cunningham said. They bent their silk hats in concert and Hynes inclined his ear. The caretaker hung his thumbs in the loops of his gold watchchain and spoke in a discreet tone to their vacant smiles. —They tell the story, he said, that two drunks came out here one foggy evening to look for the grave of a friend of theirs. They asked for Mulcahy from the Coombe and were told where he was buried. After traipsing about in the fog they found the grave sure enough. One of the drunks spelt out the name: Terence Mulcahy. The other drunk was blinking up at a statue of Our Saviour the widow had got put up. The caretaker blinked up at one of the sepulchres they passed. He resumed: —And, after blinking up at the sacred figure, Not a bloody bit like the man, says he. That's not Mulcahy, says he, whoever done it. Rewarded by smiles he fell back and spoke with Corny Kelleher, accepting the dockets given him, turning them over and scanning them as he walked. —That's all done with a purpose, Martin Cunningham explained to Hynes. —I know, Hynes said. I know that. —To cheer a fellow up, Martin Cunningham said. It's pure goodheartedness: damn the thing else. Mr Bloom admired the caretaker's prosperous bulk. All want to be on good terms with him. Decent fellow, John O'Connell, real good sort. Keys: like Keyes's ad: no fear of anyone getting out. No passout checks. Habeas corpus. I must see about that ad after the funeral. Did I write Ballsbridge on the envelope I took to cover when she disturbed me writing to Martha? Hope it's not chucked in the dead letter office. Be the better of a shave. Grey sprouting beard. That's the first sign when the hairs come out grey. And temper getting cross. Silver threads among the grey. Fancy being his wife. Wonder he had the gumption to propose to any girl. Come out and live in the graveyard. Dangle that before her. It might thrill her first. Courting death. Shades of night hovering here with all the dead stretched about. The shadows of the tombs when churchyards yawn and Daniel O'Connell must be a descendant I suppose who is this used to say he was a queer breedy man great catholic all the same like a big giant in the dark. Will o' the wisp. Gas of graves. Want to keep her mind off it to conceive at all. Women especially are so touchy. Tell her a ghost story in bed to make her sleep. Have you ever seen a ghost? Well, I have. It was a pitchdark night. The clock was on the stroke of twelve. Still they'd kiss all right if properly keyed up. Whores in Turkish graveyards. Learn anything if taken young. You might pick up a young widow here. Men like that. Love among the tombstones. Romeo. Spice of pleasure. In the midst of death we are in life. Both ends meet. Tantalising for the poor dead. Smell of grilled beefsteaks to the starving. Gnawing their vitals. Desire to grig people. Molly wanting to do it at the window. Eight children he has anyway. He has seen a fair share go under in his time, lying around him field after field. Holy fields. More room if they buried them standing. Sitting or kneeling you couldn't. Standing? His head might come up some day above ground in a landslip with his hand pointing. All honeycombed the ground must be: oblong cells. And very neat he keeps it too: trim grass and edgings. His garden Major Gamble calls Mount Jerome. Well, so it is. Ought to be flowers of sleep. Chinese cemeteries with giant poppies growing produce the best opium Mastiansky told me. The Botanic Gardens are just over there. It's the blood sinking in the earth gives new life. Same idea those jews they said killed the christian boy.