Topics in Discrete Mathematics - Cryptography
Problem Sheet 1

Daniel P. Martin

University of Bristol 2018-2019

1 Caesar Cipher

Question 1. Encrypt the following:

I came, I saw, I conquered.

Question 2. Decrypt the following:

Qr rqh lv vr eudyh wkdw kh lv qrw glvwxuehg eb vrphwklqj xqhashfwhg.

2 Shift Cipher

Question 3. Let $k = 13$, encrypt the following:

Life is what happens when youre busy making other plans.

Question 4. Let $k = 13$, decrypt the following:

Punyyratrf ner jung znxr yvsr vagrerfgvat naq birepbzvat gurz vf jung znxrf yvsr zrnavatshy.

When $k = 13$ the cipher is referred to as ROT13 and has the property that encryption is the same as decryption. This makes it a favoured choice of obfuscation on online message boards.

Question 5. Use brute force to solve the following:

Cn cm iol wbicwym, nbun mbiq qbun qy nlofs uly, zul gily nbuh iol uvcfcncym.

Question 6. Show that a shift cipher encryption under key k_1, followed by an encryption under key k_2 is the same as a single shift cipher encryption under $k_1 + k_2$.

3 Substitution Cipher

For the following two questions, use the mapping given in the table.

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
S	Z	D	U	F	R	B	K	L	M	J	V	G	N	A	Q	O	Y	W	I	E	C	T	H	P	X

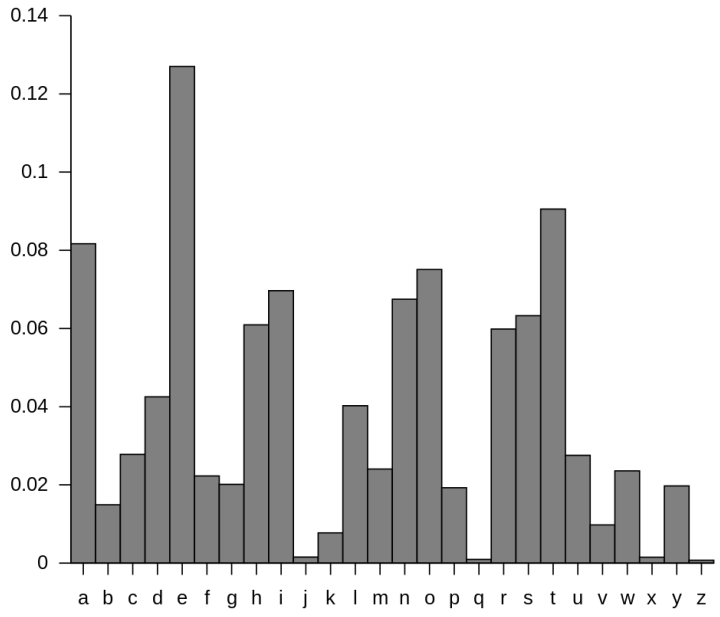
Question 7. Encrypt the following:

> Pure mathematics is, in its way,the poetry of logical ideas.

Question 8. Decrypt the following:

> FCFYPANF LW S BFNLEW. ZEI LR PAE MEUBF S RLWK ZP LIW SZLVLIP IA DVLGZ S IYFF, LI TLVV VLCF LIW TKAVF VLRF ZFVLFCLNB IKSI LI LW WIEQLU.

Frequency analysis is a method for decoding a message encrypted with a substitution cipher without knowing the key. Frequency analysis works because each letter in the ciphertext corresponds one-to-one with a letter in the plaintext. Therefore, the most frequent character in the ciphertext corresponds to the most frequent character in the plaintext, which is likely to correspond to the most frequent letter used in the English language.[1] The histogram for the English language letter frequency can be seen below.



[1] You can assume that all questions in this course have the answer given in English.

Question 9. Use frequency analysis to solve the following:

3 NVC. OGDXAGXZ. QBHX NTWGRL VX 8:35 K.N, MW 1DX NVC, VAAGYGWP VX YGBWWV BVAQC WBEX NMAWGWP; DLMTQI LVYB VAAGYBI VX 6:46, OTX XAVGW UVD VW LMTA QVXB. OTIV-KBDXL DBBND V UMWIBAHTQ KQVRB, HAMN XLB PQGNKDB ULGRL G PMX MH GX HAMN XLB XAVGW VWI XLB QGXXQB G RMTQI UVQJ XLAMTPL XLB DXABBXD. G HBVABI XM PM YBAC HVA HAMN XLB DXVXGMW, VD UB LVI VAAGYBI QVXB VWI UMTQI DXVAX VD WBVA XLB RMAABRX XGNB VD KMDDGOQB. XLB GNKABDDGMW G LVI UVD XLVX UB UBAB QBVYGWP XLB UBDX VWI BWXBAGWP XLB BVDX; XLB NMDX UBDXBAW MH DKQBWIGI OAGIPBD MYBA XLB IVWTOB, ULGRL GD LBAB MH WMOQB UGIXL VWI IBKXL, XMMJ TD VNMWP XLB XAVIGXGMWD MH XTAJGDL ATQB.

UB QBHX GW KABXXC PMMI XGNB, VWI RVNB VHXBA WGPLXHVQQ XM JQVTDBWOTAPL. LBAB G DXMKKBI HMA XLB WGPLX VX XLB LMXBQ AMCVQB. G LVI HMA IGWWBA, MA AVXLBA DTKKBA, V RLGRJBW IMWB TK DMNB UVC UGXL ABI KBKKBA, ULGRL UVD YBAC PMMI OTX XLGADXC. (NBN. PBX ABRGKB HMA NGWV.) G VDJBI XLB UVGXBA, VWI LB DVGI GX UVD RVQQBI "KVKAGJV LBWIQ," VWI XLVX, VD GX UVD V WVXGMWVQ IGDL, G DLMTQI OB VOQB XM PBX GX VWCULBAB VQMWP XLB RVAKVXLGVWD.

G HMTWI NC DNVXXBAGWP MH PBANVW YBAC TDBHTQ LBAB, GWIBBI, G IMW'X JWMU LMU G DLMTQI OB VOQB XM PBX MW UGXLMTX GX.

LVYGWP LVI DMNB XGNB VX NC IGDKMDVQ ULBW GW QMWIMW, G LVI YGDGXBI XLB OAGXGDL NTDBTN, VWI NVIB DBVARL VNMWP XLB OMMJD VWI NVKD GW XLB QGOAVAC ABPVAIGWP XAVWDCQYVWGV; GX LVI DXATRJ NB XLVX DMNB HMABJWMUQBIPB MH XLB RMTWXAC RMTQI LVAIQC HVGQ XM LVYB DMNB GNKMAXVWRB GW IBVQGWP UGXL V WMOQBNVW MH XLVX RMTWXAC.

G HGWI XLVX XLB IGDXAGRX LB WVNBI GD GW XLB BEXABNB BVDX MH XLB RMTWXAC, FTDX MW XLB OMAIBAD MH XLABB DXVXBD, XAVWDCQYVWGV, NMQIVYGV, VWI OTJMYGWV, GW XLB NGIDX MH XLB RVAKVXLGVW NMTWXVGWD; MWB MH XLB UGQIBDX VWI QBVDX JWMUW KMAXGMWD MH BTAMKB. G UVD WMX VOQB XM QGPLX MW VWC NVK MA UMAJ PGYGWP XLB BEVRX QMRVQGXC MH XLB RVDXQB IAVRTQV, VD XLBAB VAB WM NVKD MH XLGD RMTWXAC VD CBX XM RMNKVAB UGXL MTA MUW MAIVWRB DTAYBC NVKD; OTX G HMTWI XLVX OGDXAGXZ, XLB KMDX XMUW WVNBI OC RMTWX IAVRTQV, GD V HVGAQC UBQQ-JWMUW KQVRB. G DLVQQ BWXBA LBAB DMNB MH NC WMXBD, VD XLBC NVC ABHABDL NC NBNMAC ULBW G XVQJ MYBA NC XAVYBQD UGXL NGWV.

GW XLB KMKTQVXGMW MH XAVWDCQYVWGV XLBAB VAB HMTA IGDXGWRX WVXGMWVQGXGBD: DVEMWD GW XLB DMTXL, VWI NGEBI UGXL XLBN XLB UVQQVRLD, ULM VAB XLB IBDRBWIVWXD MH XLB IVRGVWD; NVPCVAD GW XLB UBDX, VWI DZBJBQCD GW XLB BVDX VWI WMAXL. G VN PMGWP VNMWP XLB QVXXBA, ULM RQVGN XM OB IBDRBWIBI HAMN VXXGQV VWI XLB LTWD. XLGD NVC OB DM, HMA ULBW XLB NVPCVAD RMWSTBABI XLB RMTWXAC GW XLB BQBYBWXL RBWXTAC XLBC HMTWI XLB LTWD DBXXQBI GW GX.

Question 10. Show that a substitution cipher encryption under key π_1, followed by an encryption under key π_2 is the same as a single substitution cipher encryption under $\pi_2 \circ \pi_1$.

4 Viginere Cipher

For the following, the key used to encrypt the message was MATH.

Question 11. Encrypt the following:

Computer Science is no more about computers than astronomy is about telescopes.

Question 12. Decrypt the following:

n diucvnme phkr cyig ny ig dbmft, vcg jn ent hw zbnku giz zf ub xjws oprqah