

Codes Project — 2006/07

Introduction

This project is based around the cipher challenge set in “The Code Book” by Simon Singh (4th Estate). You should obtain a copy and read it as a starting point for your project.

You will be required to write an account of breaking of several ciphers. This account should include a description of the ciphers, an explanation of the breaking of the codes, with an emphasis on the mathematical aspects (such as statistics and logic), and show the steps required to break these ciphers. There is software available that can break some of these ciphers with little or no input from the user, hence it is not just the broken ciphers that is required for a successful project, but a description of how it is done using the following ciphers as examples.

As a starting point I have produced some ciphers for you to have a go at. These are not the final ciphers that you will be set for your projects. The final ciphers will be different for each student and may differ of a different type from the ones included here. I would encourage you to have a go at these now and to collaborate with each other when you get stuck.

To help you, these ciphers are available on my web pages, along with frequency tables for English, both with spaces and with spaces removed. Also supplied are some Fortran77 programmes that may be helpful. These have a README file that gives some guidance for compiling and running these on some computers at City University. It is possible to break these ciphers without the use of these programmes. They are provided as an optional aid.

If you all get stuck then you can email me for hints. If you do so, then let me know how far you have got with the given cipher so I can give focussed help.

Cipher 1

CQRB RB J LNJBBA LRYQNA. CQN WNGC XWN RB J VXXJUYQJKNCR
LBDKBCRCDCRXW FQRLQ QJB QRWCB OXA CQN XCQNA LRYQNAB.

Cipher 2

FVC TDAADJWEI WX R XWKWARO NWZVCO FD FVWX QGF JWFV XZRNCX NADXC
B GZ. XDKCFWKCX FVC XZRNCX ROC OCZARNCB QP XDKC ACFFCO, TDO CHRKZAC H,
QCTDOC CENWZVCOWEI. FVWX KRM CX AWTC SGWFC R QWF VROBCO. FVC TDGOFV FRXM
WEUDAUCX FVC UWICECOC NWZVCO. BD EDF TDOICF FD ADDM TDO OCZCRFCB FVOCC
DO TDGO ACFFCO IODGZX REB NDGEF FD TWEB ZDXXWQAC ACEIFVX DT FVC MCP. FVC
TWTFV FRXM WX R KDEDRAZVRQCFWN NWZVCO JWFV VKDZVDECX, XDKC NDKKDE ACFFCOX
JWAA QC CENWZVCOCB QP KDOC FVRE DEC ACFFCO DO XPKQDA. FVC ARXF DT FVCXC
FRXXM WEUDAUCX FVC ZARPTRWO NWZVCO. TDO FVWX ARXF FRXM, REB ZDXXWQAP FVC
ZOCUWDGX DEC R FRQAC DT TOCSGCENWCX DT ACFFCO ZRWOX JWFV REB JWFVDGF IRZX
WX UCOP GXCTGA. DEC DT FVCXC WX RFFRNVCB FD FVWX KCXXRIC. VRZZP NVOWXFKRX.

Cipher 3

KHCCIODCFBCQLALJDJLXAHBPODKLOBTHDPFDDHRLCFKLOBTZFBLCFKLSEOBTSSEQLENLDXQL
TDQLBHPPLRCHBOBTQOTJROELRCOBTDLBLYLRESFTEIOCFNNDFSLTHILBDGJDFKERFFKIHDQ
OJHLXLFXOBTZLOBTJGDHDFBDQLDOSZLDQLBHCLDTFIBHBOXQOHRSEDQLIHBTFIOTDRHLTD
FDQHBAFNCFKLDQHBPXQLLRNGZSGDHDIORBDBFGCLHNLZDCFZFBLCFKLHKFCDIHCQLTHIOCTL
OTDQLCDORCILRLCQHBHBPOBTDLZLOYLCRGCDZLTHBDQLIFFTCLYLRCFKFGRBNGZOBTHQLOR
TOBFIZOIOEFNNIQFIQFFHBPOSFGDCFKLSFTEDQODIOCTLTOBTTOIQHJJFIHZZOBTOTFPXREH
BPOSFGDCFKLSFTEDQOIHBTOCDREHBPDFIQHCJLRCFKLDQHBPDKLOBTHXFGZTBDKOALFGDI
QODHDIOCOBTCFHDKOTLDQLXFZTCQHYLCRGRBFYLRKLDQLBOIOEFGDHBBDQLIFFTCHQLORTDQO
DAHBTFNOCFGBTDQODOPQFCDKOALCIBLBDIOBDCDFDLZZOSFGDCFKLDQHBPDQODCFBHDCKHB
TOBTXOBDKOALHDCLZNGBTLRCDFFTOBTFCXOBDRLCDLOCEHBHDCPROYLOBTQOCDFFPFSFGDDQ
ODIOELYLREBHPQDPRHLYHBPHPDFCFTFIBQLORDLTOBTCXORLTHHTIHCQHQTFCFKLXFKJOBE
JRLDDECFBBOCJHTLRILBDXROI ZHBPGJKECQFGZTLROBTHNZHJJLTHDFNNOBTHDZHDHBDQLXO
BTZLOBTSLNFRLLHXFGZTSGTPLHDIOCOZZCQRHYLZLTGJHTHTBDBLLTOBESFTEDFDLZZKLDQOD
DQODIOCOBOINGZSOTCHPBOBTIFGZTNLDXQKLCFKLSOTZGXACFHIOCCXORLTOTBTKFCDCQFFAD
QLXZFDQLCFNNFNKLHPFDGJOBTDGRBLTORFGBTHBKEDROXACDQRLLDHKLCOBTXRFCCLTKESRL
OCDLYLREDHKLOBTDQLBHDHLTGJOZHDDZLZFXAFNKEQOHRIDHDQODQRLDTDFALLJIHDXQLCOIO
ESGDHQOTBDBFXFBNHTLBXLEFGTFDQODIQLBEFGYLZFCDOQFRCLCQFLDQODEFGYLNFBGTHBCD
LOTFNBOHZHBPHDGJFYLRDQLTFFRSGDHQOTBDLYLRQLORTOBESFTECOEHDIOCOBEIOEDFALLJ
FNNSOTZGXAIQLBEFGTAHZZLTOCJHTLRHCLDTFIBOPOHBOCQOAHBPOZZFYLRBOTPFDFGDKJH
JLNFROCKFALNFRDQLQFGCLIOCOZZOCCDHZZOCTLODQBFIOBTCFDQLIHTFIIIFGZTBDABFIILZ
ZONDLROZFBPDHKLHQLORTDQLXZFXAOIOEFNNHBDQLDFIBPFSFFKSFFKSFFKDILZYLZHXACOB
TOZZCDHZZOPOHBCDHZZLRDQOBLYLRLDDECFBHQLORTODIHPBOJTTFIBHBDQLTORAOKFBP
CDDQLDRLLCCFKLDQHBPICOCDHRRHBPHCLCDHZZOBTZHCDLBLTTHRLXDZEHXFGZTWGCDSOR
LZEQLOROKLEFIKLEFTIFBDQLRLDQODIOCPFFTCOECHKLEFIKLEFTIOCCFNDOCHFGDDQLZHPQ
DOBTCXROKSZLTFGDFNDQLIHBTFI BDFDQLCQLTDQLBHCZHJJLTTFIBDFDQLPRFGBTOBTXROI
ZLTHBOKFBPDQLDRLLCOBTCGRLLBFGPQDQLRLIOCDFKCOIELRIOHDHBPNNFRKL

Cipher 4

LFSPBORPDJKI5YYNVEAVZH3BAEHK7RIUJS3NMYFPB8A1RM3NWNOR8LPQ75KH50NPLJSPY7AD
CAVZMJ4MAHGNZMLJSOPXBOEJDP3BAEPB8A1RIWNOLH7SUG8LHLFSP7BEIZFKIKFIK7RI4A4Y
7HGNVEIAHK7ADCMAI75EPDJKP10AREIK7RPUFS3RI37BOX8LIBDEPWNOLIBVZOA8LHBHCDJK
M35AEIB8A1NH58Q5L3MORBELIKFMU5CRM7N03R84IS3R4S8MBDEP8FFCAVZMBD2AJS38LMBG
JSKI7NOPJ7PEFP8NKIURP7R8XMKJISVEJIAKMAH37B88PEFMDJY7ADZIF4MK7NI3JOKH3BAE
IK7RHUJS3RPZRKYADZPSXMBVEMQ58CAVZH5Q5LILFSIAV3S8KHUNIGLPK58CADZM3S17IDFV
3ND3RIAIEAEDKMURBDIAKMX8RBENEPXFJOIB8A1RMGSYHLFSONI3FHR53A8LIJ44NDENEILF
SICVJQHY7NMUJS3NIJVB8LIZOJQ8NEHAVPORX8LIX8RB3NI1FURPGB1CM5DEI4AVA37HLJSOH
3YJOLPB8A1RI1588NEH54YNOPAKMBVEHK7NPFY7R03IB88H9JADREPAVP17FOS3PLR3MX8R5
3RPEJPGSKHY7RHUFS3RIJD8LM37FFCIAK3P7RBEIAUX5YARDY8LIBDEM38CREH5I8AYK8RM
TSA1CN0IQ75YI5PXAYLMAYMQJS8EDYH3YBLI3AZ7REPY7NP8FOLH53M3JJDH53PAKHQB3PTS
AYNHJSYPF4P3AZ7KI5DEP5VPF8EM1OBGHKFJCPY7NIFXXFOYSDAKLMF4H35LAVZPKFI7NOME
BSZ7YNOHB7MULMENBOI8NYIY7A3IGRHP8R33FVHKFHLJSHVNWROIYJH8J3NPLJSOPKRUXRO
M7J8EPLFSOMKFDZSNMUBM35AEIK7NMLFSDZH105GIBH8AYK8RP3V5XXA378LILFSONIRVFSZ
7MKJHKOLMK7NPXBKARD1NPF4M5VPFL3YROMAIQA37HAP75EHJSOMEAVB7H7NONMAMCVFPAP
EFP3BAEMB8A1NMB8JSEIBEEOR33AVZHVFGJELPAVHXBOKA1S85OP37NEM3FFDM4NK17MAYHG
B1CP5VEMQ7FMA3HEAD57PA4HAUIAZ7YPWRVKSONPYFH53CMY7NPTS3KAFVI3BAEPK7RP8JO
LHB8A1NMONX8ANEMR5ZR08LI4JOI37RHQB3MB8Q5L3ION5ELMKFHY58CM5GJSKI7ROHXRKIE
ADB73PFSOM15YM5DEM37N3I3S17I5P15XAK58MJVNM4JOM1BY17AVZIU1NHLFSH15DYIK7A
VCPBDEHF7MAPQA37MLJSH1FS8EM3RRP7ROM54KNOPK7RIGA0E3MQ7LH37R88INBYHBP8AYK8
NPGA0EIB3H3FJVIB3M8JFCH5KHAKIY7A3H3XNR17M15S3NEP5IORUB0CBG8RI3RD35KAJDIB
UJDZMK7NPX5OYLM3JUNMF4IK7NPGA0E3H7S00AREPF44P5KIJV1RIJDNP8EUI5ZXARPGNZ5
DHQ05XXAVZHAY3R84PSXMWNOLM15ON4S88LHORU50CAVZPAPONB88LHUS3KMGNI3ZNYAVZH7
JURMY7RPDAZ7Y5AOHEJN3DKP3SAKIULMK70J5YIBVEMBH15D5OLI1588REIJSYMADH5HYONU
G8AVZHWJA1RMKJIAK3I17A8EONDP1JUNIBQBLIULPER503HAK3M7AZ7MYAURPLFSMQNORM58
8MAVHGREHJDIW5OAJ3IXORKR2Y3HY7RLP588IUFWNEHF44PBVEI58A1RMQB3P3JJVH8R4YP
58JDRH

Cipher 5

HTVGWJIGHGZYMKUHPNGUWFPQLLRAXJXELAAWXHTDBVPSVFLBEQIRZWZQEAWZ
PMMFOUINWSACXZMQIJLHPGIJADRQUWVLMMDMGXUXJTJXGNWLRXNTEMFOZMGZ
XJFSVNIELTDFOOMQXUHETKSTMGLREAKVHAVFLNFTTIWOPLGUASSFRUMEIYHF
VVHLWKMFWRVEKMGTKLVCVLPHCJXJTRKDWRQLLMXKIGNUSBFKXEEDWZIEBF
VGMDMRJONAAUMFOXTNRSGUAZMUIVMZPUWGTLXGEWQLWAVHWMGQVXZIWSAXU
DLPVAFEEVWAPLWTSJNGUNZRYQWQHLLWRZWZXRGAWGVAZMQMGPSHRCGCQKUH
HVTDIBMAZSIYMVMDRQLWTBAABKSGAWGYSMAHWNGVWRZWNRVTHLIVRLPHANRG
JKEYILRVMOFJSDLHRBNYWESOIQHKKWPCWVRYTAXDIRGJRHLEAKVHAVLXONL
HTVGWJIGAWDKLWZUSBFKQVMFODPYEWIFYLIVSSYARVWLPHCNKVLRWKGEEDL
WRXWDHRFVJDFKWEKSXGWLZXKMYIERKIFRWEDWSTACKSYZRTRPAIYLAKEAWK
IYIXWJEAWXGFWLRLHGYPPSSMBWLRUDPTOGTKNMWLRRCGNWLRAGJJILPDXVMK
TVQWLDWVYLWVVKWVLYFHXYIYIOMDXUXJHRXAVPSHKFULPEMGMGTLXFRGVWLRMZ
GVWZWOHAHOXKMKIIEPMLWRXLPHVRPSHESLPLRTTLPCPHIUXVVMARVSJRYGMZ
TBRGKNIEHFYIIVWRVRQUTGXLPDXVMOPJZWZBPNKYTZXAADPFHSURGLBKEGLU
GFSYMKEQLWTEMLVLKUMSCUQGZQMAZVJIMFOKMFPZDCIJMVMQXFRVMFBKEGID
PTISTVSGASIJGJWRKRASSRWDQWXYXGUNLSBLWPTDAVHXIQGLTTDLXZQPEFTF
NDEFQQXUXUXKCGNOSAWGCVZWVLRPEMSZRYEKMPAAHRFGTGABKVIYIUWUTBKS
IZSFIOHRKETEEFLOMIXJNCILQWEYLGQVFGZQIVGEXEHLDPXFVJDFKWPDAHL
QVWLWZIQHFTKLGCJLGHFBRVDMBVGUTYMKTDWGFCKMGVRJUBKHVZWVBINKK
SVEVXDVGWGWKLSBDJGXJCFSEFIQHGAWCCILIQCZTFTOTDILRGHETZJZMFEAAG
LZXZISTRGWSKLSBVGEHGVVLSDLRTAAHBIQQXUXDDTOGNWLRWGDWSELRGAW
ZESUSHVJBLWFYLLQWWHGVTIKQQKNGQXEXWZPIQBSIVTJWFIFLGUTLSVJIAHL
PBRGKNIEUMIDEJTHCFYSRVQSZOILLXPTIABZEFGGIZRAUSIAXLGRFDMVLNWG
LRWLPHSGAWGFFBMBFXBFIYIYIUIHJXJTSYLPDHNWAHDEDTLKUMSQFYLLQWPDW
PSEVTRFFMWGZRS�DVXVWACEJQWANLFDKEFOUCBKXTISUQRYFUMICSGSHHNMK
RISGOHEFFSGCIQCVIQMGAFSCELXUZZDJXDGVTRVLPWPWAWYEGWSLTMXRRVMK
VYSKBOCSHJTYISLWLRASXIASAFYEBGJJQAWMEKWSRWANECOKWPKLGZKSGTA
GRRVBKSHZZIYIWHGWJXJTNMVMRTRGLWVCOMUICXJUVGLTBQBMADWPVAVXUTL
PEHABVPVOASTSDWXVZTVTZXZWUVVUDTSYLQWWUHJGFVKMHQRWLDIAVVTVMW
DWXZMIEPXSCUFWRRQBLHTSFBUSYKSIYIJBKEATHPIXGNLXFHOCVBHZZHWFBG
C

Cipher 6

HMOPDPZLNVXTGBLZCGMWKNOKITYUCOHULEAGTFBCLLPLOAKMWEAMWAKDAMT
MGKAOLFSQPTSOLUTXKLDOLAVPBHMXARGMTPCAQLWATLMMWWOFTGRGTAB
KLEPOHPTOMRDWHGWHUTNTPGHMTTRIMKMOHULOHOHNAKAPTRGPZLNLTDLWHGC
RNHEBTADKLLPBWTEKASTOMADOLWYIHAVPHMXBIUZPLIOCOKAWHGWDAFONKON
BNNTMTUETDAUADULXANOMWPDDTUANDEOHTDWTGRTHMLPNHMHUAFONOLWD
PCOFTDAPGWMTDAGDIECLLGTGCGCOMQSMITDTWGNNGCQSKANDMTPGCACRPHCOH
ULONTXRILGLUAZAKAPDQDWYFZCQAWDMIACMHNGDPOFMTUEONRPMWOUTIOFLG
COXDULWOPCDXONIQTMTDKLOEOMWAACBILOGTOFULWBULGLTCMWAKECAVPHGW
TDMWUALRCADPOFMTGPHDICGMWEOFMTCGLNQMVGWTHOUWTMBILKPCMTLOAU
NGNOCONMTHABTDEOAOAXLCDQSQNGTDCKHMNDLNQMGWLDGTMUTSWMRUIOTHAP
GPDIHPPBTDIEMTPKDHANHECUCOLDOHAMWWNZLOHULULUWTMQSCYHECBHGXMUL
GLOPDPQHRACGIOMWXTQPPAACDITIOFLGCOKAHMULONGCNOMTAGMTLGQIPHDT
HOAZAGDYDCDOMTPENOGCONDMULKHHPTSGWLTKEKLGTRUKCAVACLNWDDIULON
NDCOFSGNEFAKXWAGCLNOMHNGNDMTAZPCDILMHUGCQFDTEFKPOFMWEEATDUA
ONKBDAGCDPOFDWADMWDAMTUZHMLMCGSMGLGPMGTGRUTDRAHTLFCAPWOMOM
ULUHXOBAAGKMDPOFTWKPLIQPMGWNOMRTSQFGAZPKKLKPPETHGWMTPANOXDNO
CUCUKLOHULLCHOTPNLIBGNLTCOBAADCOXTQSCYNOUCHHUPKQILOAUULWHRU
UAGTDITRKEVULFIADAUULMGWNBAMKCAHDWUCKPOMHUCGDOMTDDHUIDIKL
PTTKNUCGDAGMDPPBADULTWOCETHCFNFMWSOPDHNPCCOGBIPOCOSTBIAOGDMTLU
COBAAGBMSKQAOMTLMHURUDTFPLGDTMWSULGPGLZCHAHQMWRULGPLPHAKET
STVHZCGNKETHOCDCBITWGRTHLMTCKAFNANICCOTWRYNAMS LGTDCUNOPEACTN
ONIKCVMTCKOKLDNGLMTTDPOTSQSMHCHMHNGUHRUHDALRGKLI OAZCGDPMW
IDPHZUTHIFPADCOFQSOYGCWBPHZUTHFIPDUALVIMMTUKLWATWLPDKPXTOPQM
OMGPOMNFMWIMPKAPLXMWEKDPAVEHRMLOUCKAYAPLMHGWECEMTQNTWRNDOMTNO
GTRUCVBOCGLMAKDNBLGRDDIMWCEQMGOCKIKMWOUADEDPKULAHLCOFBDTOF
MWRKNGGCHAPKDPOFBIPAVAPDQDINATDLMPDUILMOPUAOLDQBIPEGTABPSMT
ULLBPTOLOFEAADULDBIPECTPUOCOFACXFNRGNOMULKPDOHAPCAVPBATZUXT
DQBIPGPDMIOGMWRULGDCEPDAMTLKCEDEOFEIDOMHGWULLBCOFBKLDNGLHMG
AVCHSQSSAZEAPTUCXDGTLMWRULGBIGTABLGXNTEGLGNHDCGDAGWAUMHGWXN
HGKATDTLGLXNTKNXGTFGNRRITDNAAREFHMSQTLCLCDIIOPAZLANUCANUCDA
KLXDULGLFWGTKPOPHMMWOCNARGWLGNMTTDDNRASQBVNXULAVHVUENGAUNW
HUUCOHNGCOBTPAPBDTXMULGLGNRIUEKUDQKPPKTRHEFOIOPMTDNOTHUMHP
AHTHBPTDLUGTOLHAPCDIULEKPKKPDITLDARCNFLBMWBACZRNHEFDUKLCOFUL
BOTDULOLXRTSTLQHGWMATAKONOWACGAKFVMTCPUDUAOGCXOCVMPKGNOCOTDWU
TYUCOHNGDPTSTWKPLISQWMZLORNGKALVIMULDPDOHDADTRTNDCCRURWTAPMT
SQQHQSDTMHNHGRNOGMDNOGNOICOSTRNBTLZZCDAARGDGTMSQFQLTUIBVAUGC
ODMTCOBUMHQMWDNOLAVACAVPRLOSBDAWMTLGDNOWAOWTXDADULTCQSFPTRQY
GUOCOFISZUXAIMBNADBLHKSHKOCZLTFGPORIAUIDLNSIMIGLKPDPFULKLOE
WYTGMLGWKPZLOLAHAZIDGLKCOVWHGWIKDALMCLUAWBCOBLGKPPULGLGPUH
RUMDMWXDULTY