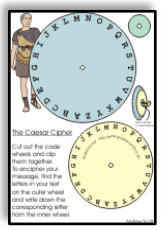
# Caesar Cipher



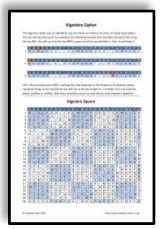
One of the simplest forms of cipher is the *Caesar Shift cipher*. This is a simple *mono-alphabetic* substitution cipher where each letter in an input message is replaced by another letter from a single *cipher alphabet*. The cipher alphabet is formed by shifting or rotating the characters A-Z by a known number of places. The cipher key is simply the number of places the characters have been moved, 1 to 25.

Breaking such a code can be done by noting the widely differing usage frequencies of letters in English, or even just brute force. To make the task of breaking such a code more complex the cipher alphabet could have the letters randomly shuffled giving 400,000,000,000,000,000,000,000,000 possible alphabets rather than 25. The following is a simple shift substitution of a well known text.

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| FANQA | DZAFF | ANQFT | MFUEF | TQCGQ | EFUAZ | ITQFT | QDFUE | ZANXQ | DUZFT | QYUZP | FAEGR | RQDFT |
| QEXUZ | SEMZP | MDDAI | EARAG | FDMSQ | AGERA | DFGZQ | ADFAF | MWQMD | YEMSM | UZEFM | EQMAR | FDAGN |
| XQEMZ | PNKAB | BAEUZ | SQZPF | TQYFA | PUQFA | EXQQB | ZAYAD | QMZPN | KMEXQ | QBFAE | MKIQQ | ZPFTQ |
| TQMDF | MOTQM | ZPFTQ | FTAGE | MZPZM | FGDMX | ETAOW | EFTMF | RXQET | UETQU | DFAFU | EMOAZ | EGYYM |
| FUAZP | QHAGF | XKFAN | QIUET | PFAPU | QFAEX | QQBFA | EXQQB | BQDOT | MZOQF | APDQM | YMKFT | QDQEF |
| TQDGN | RADUZ | FTMFE | XQQBA | RPQMF | TITMF | PDQMY | EYMKO | AYQIT | QZIQT | MHQET | GRRXQ | PARRF |
| TUEYA | DFMXO | AUXYG | EFSUH | QGEBM | GEQFT | QDQEF | TQDQE | BQOFF | TMFYM | WQEOM | XMYUF | KAREA |
| XAZSX | URQRA | DITAI | AGXPN | QMDFT | QITUB | EMZPE | OADZE | ARFUY | QFTAB | BDQEE | ADEID | AZSFT |
| QBDAG | PYMZE | OAZFG | YQXKF | TQBMZ | SEARP | QEBUE | PXAHQ | FTQXM | IEPQX | MKFTQ | UZEAX | QZOQA |
| RARRU | OQMZP | FTQEB | GDZEF | TMFBM | FUQZF | YQDUF | ARFTG | ZIADF | TKFMW | QEITQ | ZTQTU | YEQXR |
| YUSTF | TUECG | UQFGE | YMWQI | UFTMN | MDQNA | PWUZI | TAIAG | XPFTQ | EQRMD | PQXEN | QMDFA | SDGZF |
| MZPEI | QMFGZ | PQDMI | QMDKX | URQNG | FFTMF | FTQPD | QMPAR | EAYQF | TUZSM | RFQDP | QMFTF | TQGZP |
| UEOAH | QDPOA | GZFDK | RDAYI | TAEQN | AGDZZ | AFDMH | QXXQD | DQFGD | ZEBGL | LXQEF | TQIUX | XMZPY |
| MWQEG | EDMFT | QDNQM | DFTAE | QUXXE | IQTMH | QFTMZ | RXKFA | AFTQD | EFTMF | IQWZA | IZAFA | RFTGE |
| OAZEO | UQZOQ | PAQEY | MWQOA | IMDPE | ARGEM | XXMZP | FTGEF | TQZMF | UHQTG | QARDQ | EAXGF | UAZUE |
| EUOWX | UQPAQ | DIUFT | FTQBM | XQOME | FARFT | AGSTF | MZPQZ | FQDBD | UEQEA | RSDQM | FBUFT | MZPYA |
| YQZFI | UFTFT | UEDQS | MDPFT | QUDOG | DDQZF | EFGDZ | MIDKM | ZPXAE | QFTQZ | MYQAR | MOFUA | ZEARF |
| KAGZA | IFTQR | MUDAB | TQXUM | ZKYBT | UZFTK | ADUEA | ZENQM | XXYKE | UZEDQ | YQYND | QPMZP | DQIEO |

## Vigenère Cipher

The Caesar cipher is easy to crack using simple frequency analysis, or even just a brute force attack. To make things harder one can use a *poly-alphabetic cipher* where a different alphabet is used to encipher each character – approximating a *one time pad*. For practical purposes a repeating set of alphabets are used; the first letter of each alphabet forming the *key* or *keyword*.



As the cipher alphabet changes for each input character, simple frequency analysis no longer works. A method of deciphering this type of system was first discovered by Charles Babbage – although, as the cipher was in common use, he didn't publish.

The weakness of this type of cipher is that the key, and thus the set of alphabets repeat. This means that common words will be repeatedly enciphered with the same set of cipher alphabets. Spotting repeated groups of letters in the enciphered text gives a good indication of the key length (or a multiple of it), and also the likely keyword itself by considering the frequency of common words and letter groupings. For example, by far the most common word in English is *the*, and the *th* pairing of characters is itself by far the most common combination of letters – these should show up regularly in any enciphered text. Given a known (or maybe assumed) key length, the problem becomes one of a set of mono-alphabetic, Caesar shift ciphers.

The following enciphered text is a well known passage from a popular English novel. The passage and the key have been chosen to show up the flaws in the Vigenère cipher and make cracking the code relatively easy.

# Vigenère Cipher

| BHLIU | MVTJG | LHDNV | BATAK | MKPAV | ASLWT | LHDNV | BATAK | MKPAV | ASPOG | HTLQU | WCBQV | POHBJ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| XOVMQ | YTDWN | BGWVG | LGXBY | TGIPG | XDDKJ | HTQMN | BSUQV | POHBJ | XSEWE | ACUQP | VFTLW | EWIGK |
| MKPAV | ASHMC | LCCWH | EWVPV | BHLIU | MVTAG | TGDVQ | YRPZM | GSHAK | MKPAV | ASHXT | BBVWH | ACEMK |
| MKPAV | ASLQP | MSGWH | WSHXC | BFLMJ | TRTDG | KMIPK | GUQMH | HFTCU | PSWIF | GCIPK | GUQMH | HFTCU |
| PSLMT | XOATI | HWCOF | BFTKV | MCWMC | OSCEG | PSGMC | EZVWK | GUSQT | XQIBJ | XCIPG | KKPGK | GGWWT |
| MHWMR | XFXWF | POHAQ | YOGTK | DSIPG | IFTAG | GHEMT | BCSBJ | THHWO | XCUQV | LBDQU | BSHBC | NHWWT |
| BHXMU | BBHQU | MSSWP | BHHJG | BBVZG | VSXDG | WTDZI | HCSWT | YCGMX | BZXVV | ASHCR | XFAIV | BJTLG |
| ZFTMQ | YQDUR | TFXAQ | GCCTA | MVTZG | PSGMC | DWCOY | BHWIN | TFVML | TKPVF | TEJMG | GKXBJ | TDAIK |
| GTPKG | HBIPG | MVGWP | XCUMP | ZZPVF | MVTZG | PSGMC | DWCOY | BHWIN | TFVML | TKPVF | TEJMG | GKXBJ |
| TTPQT | YORMQ | GHWMV | AFDVG | HTUZC | GQTQP | UCIPE | HICBT | BSHQV | POHKN | XOGMT | MVPVE | KMHBC |
| EHDBJ | XZDZF | LCUBJ | XGIIV | XDGMU | XFKMU | HTAWC | OSHIP | WTXAJ | XGIPC | MHWQP | ZGXVI | XBTZC |
| EKTZG | LSIBN | XRUWT | XJTZK | MKPAV | ASNMC | KCUWW | KZDZF | HBTBJ | HIHIP | WGTDG | GVJVF | KSSIP |
| WGTDG | GHNNK | OSHXK | KWICC | EFTDG | EOIQQ | GGLMT | XQDVE | XRTLV | HSCON | TBSIV | MVPBH | TJDCT |
| XREMT | BCSIU | THIPK | LAGAU | HIIPE | HHIPC | WFTKG | GHAGC | MHPQP | XRWMT | YWKMC | GRIEG | GHXMV |
| APAMU | LSSJK | KHWLC | RCUEJ | HAPXT | HDWMV | BQEZK | OOIMK | GHWMN | BTTOW | TFSAJ | TRWMT | TZSMF |
| MVTAW | UZXUG | TDEMC | KOCKG | UMPVP | HICKK | GUIPC | MOGZC | GUTUG | GHHEG | KSBIF | XTDZV | ASHEC |
| EZDEK | GUJXQ | YZDVF | HBPVF | PSHBO | BBHBG | KSKMP | MVTKQ | VYAIP | XUWWU | MVPLD | XSCTC | BRDVN |
| ROGWW | GRSWB | XBDNA | XOGAC | YHTZT | TDEQP | ZCJBK | MGBMU | LOVMU | TGIPG | LDXZK | MGDNV | AWHDG |
| KMNMC | KZPAV | IOHBU | NDTZP | THJZC | EZNLG | YWRQG | GHXVQ | KWVQP | TZXBA | KOEXG | WCJBV | ASXZU |
| FSGMO | XGHII | XGXVV | ASTIT | MVAGQ | KRTZQ | YSKMP | MGWIF | EOIMN | RQDUG | MCIPG | XBVTK | LVRZQ |
| PBPVF | ISDXN | XTGWO | TQDVI | KSHAQ | YPGQV | BGWAW | UXTKV | LWCIO | XFXKC | PVXKJ | LHGIP | ZSIWT |
| XZPBG | AOKMR | KCKMF | FCGMK | FDDZV | TBIBQ | MVTPW | FOCZC | VSIPC | GOCGE | HABCP | BQPBK | HBHGG |
| MFTKG | BJTLV | AFDCI | AOCGQ | YHWME | AWRSG | GGDNV | ASRWE | DZPVG | UFDWF | YFPVE | XZTAU | YOKWW |
| KSSWP | MVTEJ | HZTIU | MCBIV | MSGAU | IWGQV | NOABJ | TBWMT | LWHBG | KCUBJ | XGWQG | ERPVF | MFXLG |
| GHGWN | ESSEK | MVTFE | XSSQP | ZGBWQ | MVCMU | LRDEP | AWATO | TYXVI | IOEMT | FCCMA | TBSAR | XBSQP |
| ZWICP | WSGBJ | XUJQF | TBRMQ | YVTZE | AFXAV | BOCXC | LHDZU | LVTMP | MSGBC | BBTLJ | XFHMN | YPTAK |
| WSHEK | MVHCE | AVJUC | GSPKJ | BSKMO | XBIAC | LGTVV | XBRQP | ZONWW | MVIWJ | TJTPK | LVPVF | LQJBQ |
| YTWQU | MCCOW | XHDZP | HIIEK | MVEQP | VSGAC | GRWQU | UCSGD | NFCMF | TZXDG | USRIW | LSWMJ | TRCWV |
| DBTMN | XRSWY | GWCBJ | XFPQP | MCSWJ | HBDCT | MCPLK | KHNXT | HQTAU | BCCWH | FCCSU | PVXKJ | IOHAG |
| WKXBJ | BBWQU | OWTEC | MOSQU | MOCKG | HTHWO | XTXNV | RCGAK | QHNGC | KRHQV | BGAQM | XZNMP | HIVPV |
| AOIZQ | HHTLK | GHWMY | HCSAQ | YTGIP | VSPVF | GCGEC | RHWMT | XKTZG | ZFDEK | GUIZG | XGLPG | GHWIV |
| LIUNG | KSGEC | LDJBV | HRTIV | AOAZG | TRNUC | KYTLD | RHWMY | HCSUC | GTPBG | MCRWO | XRDEP | TBSJG |
| LOLVK | GHDJQ | TFSAV | HAPSG | TQTZV | TWCUQ | OOQTG | YFPUG | PCGSY | BHWIU | TQZIP | WOZVK | YSXVK |
| MHTZT | BPAMK | GVXAV | HFNQV | BGAQM | XZNMP | HIVPV | AOIQP | MVTZQ | NUWWW | MVDCU | XGDNU | HATBK |
| EZTZU | HTIPG | ASPDA | EOCLU | TRYIE | XBIBQ | IOGQU | MVTZG | PSGMU | ASABG | KSSNT | HAIPG | PSPBJ |
| XFIPC | MJTZA | WONZW | WSRIT | MGQMU | IOIBG | KSSEK | MVGCU | MWRUK | KSHVW | YTTLC | UCJBD | RDXOU |
| TBSZQ | HGIMF | BBQGR | HIABT | RKWQE | AHWMH | TFBMT | WSPBJ | AOSIN | KSPLA | LSIIR | TFIBQ | USWQU |
| MIBJT | BZHWH | MVTZG | OCACV | BCCJW | MHWIV | PCDLO | TBPVF | MVPBH | TFBMT | MVDCI | AHWMA | PCGSW |
| GQTIU | BBVTA | PCGSU | BZTVV | EMPVF | GCDVG | ASPZF | MVTUC | LHWMA | PSCBC | UCJBY | BHWUW | YTAMF |
| MFTIF | MVTZC | MVTZH | HFPAO | NQWIU | MCTVV | XFIIK | GOCGU | NGEQE | BCCBJ | THIPG | RKTZG | TKPSG |
| POHBQ | USPBJ | XWHBK | VOAIP | WHGIK | MCGWW | LWCMP | ZZPVF | MVTZG | POHAE | TFRMN | ROCIO | HICBQ |
| YCGLG | KOCLR | KCIME | MWDVV | HXJAV | BTNUW | VVCIV | BCCIN | UCPAV | BBVLC | KWCOD | NFVTC | KWTAD |
| ROGUG | WATVC | GRWQI | AKPGT | HPQMT | BSHBQ | HYETC | VSXVV | ASRIR | BHPTK | MGTTH | XJTZA | GWVPV |
| YOBQN | BSHEG | KSECD | EWRTA | VOJBK | HBTLP | HHIWI | HCJBQ | YHDEP | PWIPQ | NHGMO | HJXVI | MVTQT |
| YIGVK | MIGMV | HIEPQ | EGIMT | XFHEC | KSWWW | LSHNQ | KGTKW | KWIGV | ASWQI | AKPGO | TBXVV | ASSIT |
| DKPAC | VWIGV | KOSMU | FOCQP | MVTTK | ZVIIP | WPTQP | ZFTKQ | ZBXAG | WOCLE | AOATG | GUTLD | RVXAH |
| XZAWY | MFPLG | LAPVY | ACBPG | LHDXR | XRXVJ | BGRPC | KORBG | KCUBJ | XQPXV | TWCOC | EZPVV | EMHPQ |
| MVXUV | AFDCI | AHWMJ | XOSIP | WFDLG | TKPGV | ASBIK | EKPAY | TMAIK | WPNAG | OSCZQ | UPTZU | TBSBJ |
| XUJIT | WGWWV | MVGMG | WSPLC | GRIPG | GUDBU | ACILG | TRWQO | LSAND | RHWMQ | MVTZH | HIGQP | VCCAG |
| JITVE | XCUBJ | XTPQN | NFTWH | AWHIO | FICQV | BCCIH | MSGEJ | BQWBJ | XAPQN | POHZQ | UPTLK | GDTIE |
| XHWIV | FOVVK | YWRMP | MDDBG | GHPBG | MVTTQ | KRBIA | HFDNN | HBSWP | POHUC | WSIWU | MOCLC | GRSMN |
| BJTZQ | GHJZP | AOBOT | XSCJA | HBTPK | ZVLIA | FOCEJ | HRTAR | HWAMF | MVTQN | EIHBT | BCJAE | KSPBW |
| KSXVU | BUWBQ | YOATJ | BGGMV | BBJMR | KWHWP | XFHQP | ECCLQ | GUPWN | LTDCI | AHQIV | MZTAY | BHWBJ |
| XWGBW | KBZMA | LOCLV | ASBIL | XGIGQ | YHWMN | TKUQT | XRQTW | GRTZD | NGHMU | BBPUQ | GUIPG | FZDIF |
| XRLQV | AFDCP | WGDNU | ACIIP | WPPTN | MVXMX | XGHVK | IDTLQ | YTSQC | FCCLE | KCHAG | LTGWO | MVTVG |
| VYHWH | GCQTG | ECGLU | THRWW | KHSZC | PWCOT | HCBAO | NGZMV | XSGAY | XBIQP | MCHBI | BZTAU | MCHMC |
| KQWNQ | KQDVV | KOQIP | WUDWF | LOCLV | ASBWD | YWGMF | HBIPG | FIHSG | MSTZU | TBSBJ | XAJAM | XHTMT |
| LTXZG | WCCBJ | XADJC | GRCWD | HRNBJ | HIVPV | TBNWH | MVTAG | HQRCT | KSCKG | LAJKJ | HIIWH | MVTKQ |
| FADVY | TMXVV | ASBQF | LHDNV | ASBBJ | XVPVI | FOCMX | XFQCU | ROCLG | OSGEQ | KGTBJ | TBJAG | ESHAY |
| TGXVE | HBHBC | GHGMS | NWHQV | BCCVQ | PGIZK | GUXVI | NDAWP | ZFDEU | HTBQU | VSATC | GSDCU | VFXUK |
| GOAAP | HKWIP | ZWCOC | ACJAG | UFTIM | XFDVU | THJZF | TMLPQ | AOSJG | XBIIM | XBDVV | NSHLC | RBDED |
| NFCQP | ZDTWR | ESXVV | ASWIP | WOIVG | PUPBG | UMIPG | WCOMP | TBSVQ | PPJZP | BBVXC | FDWTG | MGPBV |
| ASSWQ | KCUEG | LHBQP | LHTZJ | TZABQ | WONBC | DWCOV | ASAQH | XCUIP | THGWE | BCJAO | NFSMT | XFPVF |
| MCBWT | KCLWH | TKGMV | VVTLR | BZUMT | XFLPQ | AOSZQ | UPTLC | YOGUG | KGQWA | HTHQZ | ISCKG | TZABJ |
| XGTBJ | BBVAC | GRPBJ | HIHIP | WZXSG | MVTUE | TATBQ | IOHAK | GOCLE | ECHMW | ICCBJ | XRTIT | HZSGG |
| TFDVG | MVDCU | TBSAG | OSCPW | GRGMF | TBSAG | OSCBA | YWKMG | GJXZQ | GSSJA | MVTUY | AWAMV | ASLWQ |
| WAPVC | GRIPG | YOGUG | KKDZM | XRJVJ | XSSMF | MVDAG | MKDWH | MVTTC | KUTRC | PGPVF | MVDAG | HHWMT |
| MKDWH | MVTXN | TWCIP | WHWMH | TWGNC | VSHBT | HRLQV | AGIQT | XBDCI | AOCLE | TFGQG | WHWMK | KRXDK |
| GSGQI | AHHEK | MVPPK | ZVWIP | WHWCU | WWSBJ | XMTIT | HBTBJ | HIHIP | WGTDG | GVJVF | KSSIP | WGTDG |
| GHNNK | OSRWP | WIRBV | ASXZI | KSPBP | XGHMU | TBSUA | KWPLU | HTHUC | EZRZG | THJZG | LHWME | KSPBW |
| KSHWH | MVXAE | AFDVK | VZTIO | HBVBJ | XFTAV | TZDVI | MVTZQ | TRHBJ | THAIA | USUWT | XHWMO | LQDBV |