

## Factoring Example

Consider the following ciphertext:

SIJYU MNVCA ISPJL RBZEY QWYEU LWMGW ICJCI MTZEI MIBKN  
QWBRI VWYIG BWNBQ QCGQH IWJKA GEGXN IDMRU VEZYG QIGVN  
CTGYO BPDBL VCGXG BKZZG IVXCU NTZAO BWFEQ QLFCO MTYZT  
 CCBYQ OPDKA GDGIG VPWMR QIIEW ICGXG BLGQQ VBGRS MYJJY  
 QVFWY RWNFL GXNFW MCJKX IDDRU OPJQQ ZRHCN VWDYQ RDGDG  
 BXDBN PXFPU YXNFG MPJEL SANCD SEZZG IBEYU KDHCA MBJJF  
 KILCJ MFDZT CTJRD MIYZQ ACJRR SBGZN QYAHQ VEDCQ LXNCL  
 LVVCS QWBII IVJRN WNBRI VPJEL TAGDN IRGQP ATYEW CBYZT  
 EVGQU VPYHL LRZNQ XINBA IKWJQ RDZYF KWFZL GWFJQ QWJYQ  
 IBWRX

The principal repetitions of three or more letters have been underlined in the message and the factors (up to 20 only) of the intervals between them are as follows:

<u>Fragment</u>	<u>Distance</u>	<u>Factors</u>
CGXGB	60	2,3,4,5,6,10,12,15,20
PJEL	95	5,19
BRI	285	3,5,15,19
QRD	165	3,5,15
QWB	275	5,11
WIC	130	2,5,10,13
XNF	45	3,5,9,15
YZT	225	3,5,15
ZGI	145	5

The factor 5 is common to all of these repetitions, and there seems to be every indication that five alphabets are involved. Certainly, this is not a proof that five alphabets were used — it is only a working hypothesis.