**Challenge 7A**

Closing in

RTBFX UIUHT UZWUW ZAMMT BHUGS AUZSA ZEJHU ZIILH ARTIR WBNIM HTUZS GEINA FIUFI CAFHM IYBPT BKIBZ ACCAF HJZUH PTIFI URTIR WILHT IRUCT IFRXI FWGEB RWSFA JZLBZ LUHHJ FZGAJ HGTIU GMTUH IFJGG UBZTI FNBYU XPXIN HYAGR AMUZE JHGTI TBGFI XBHUK IGUZH TISJX BSBHC IFYGT IRXIB FXPTB GZAXA KINAF HTIGA KUIHS AKIFZ YIZHG AUBYG HUXXZ AHGJF IMTAG TIMBG MAFWU ZSNAF EJHUH TUZWH TUGUG WIPUZ HIXXU SIZRI UZHTI YIBZH UYIUT BKIEI IZMBH RTUZS HTIEF UHGHT IPGII YHATB KIEII ZUZRA ZHBRH MUHTA JFNFU IZLGU ZHTIF IURTG LAWHA FBZLH TIPUZ HJFZT BKIEI IZMBH RTUZS HTINF IZRTU HGIIY GXUWI MIBFI BXXMA FWUZS BSBUZ GHAZI BZAHT IFMTU RTUFI BXXPL ULZHI OCIRH BZLSU KIZMT BHMIF IBLUZ HTINF IZRTL ARJYI ZHXBG HMIIW ULAZH HTUZW HTBHU GBRAU ZRULI ZRIYP AMZSJ IGGUG HTBHH TIFJG GUBZG WZAMM TBHUG SAUZS AZBZL HTBHA JFEIG HTACI ANJZR AKIFU ZSUHU GHAEF IBWUZ HAHTI UFTDB ZLHFP HANUZ LGAYI HTUZS HTIFI JZNAF HJZBH IXPBR RAFLU ZSHAY PGAJF RIPJF UHTIP TBKIH BWIZH AJGUZ SBZIM RUCTI FGAXU HBUFI NAFBF RTUKI GHAFB SIANH ACGIR FIHNU XIGGA IKIZU NMIYB ZBSIH AGHIB XHTIF IXIKB ZHNUX IUHMU XXHBW IBXAH ANRAY CJHUZ SHAEF IBWHT IRUCT IFUBH HBRTB EFUIN YIGGB SINFA YPJFU IZRFP CHILJ GUZSB ZBYGR ARUCT IFWIP MAFLX IZSHT UGGUO UZMTU RTTIL IGRFU EIGHT IRUCT IFUHU GKIFP RXIKI FGUYC XIHAU YCXIY IZHEJ HBLIK UXHAR FBRWB ZLYPA ZITAC IUGHT BHMIR BZBXG ANUZL HTIRU CTIFW IPMTU XIUZH TITDA FBHXI BGHCB FHANU HUCXB ZHAIZ HIFUZ HMAMI IWGAZ LIRIY EIFGU OHIIZ HTHTI FJGGU BZGBF ITAGH UZSBX BFSIC FACBS BZLBI KIZHB GCBFH ANHTI UZHIF ZBHUA ZBXIE BJBJG GHIXX JZSMU HTXIB LUZSC AXUHE JFAYI YEIFG UZBHH IZLBZ RIYAG HANHT IGIRJ FUHPH IBYMU XXEIA RRJCU ILMUH THTBH BZLTD GIRJF UHPMU XXEIF IXBHU KIXPX USTHM UHTXJ RWUMU XXSIH UZBZL AJHMU HTHTI NUXIG MIZII LHTBH ZUSTH BZLHT IZMIR BZSIH HAHTI EAHHA YANHT IMTAX IFIUR TGLAW HAFGH FBHBS IYBXX HTIEI GHTBF FP

, key=)

Charlie, I think I know what is going on, but I need to check a few things before I report. We may have an opportunity here. I checked the cipher clerk’s background and it turns out she is White Russian. Her family left Moscow in 1917, but she has relatives in the Gulag at Perm. She clearly has no love for the Soviet government so I am still not sure who she was working for, but I think this is key intelligence.   
  
In the meantime I have been watching the Brits. They seem to have been in contact with our friends in the Reichsdoktor and they in turn have been watching the French. It seems like we are all working against one another, which I really didn’t expect, and given what we read in the French document last week I don’t think that is a coincidence.   
  
My own guess is that the Russians know what is going on, and that our best hope of uncovering it is to break into their HQ and try to find something there. Unfortunately, according to my source Yuri they have taken to using a new cipher, Solitaire, for archive storage of top-secret files, so even if we manage to steal the relevant file it will take a lot of computing to break the cipher. I attach a brief message from Yuri, encrypted using an amsco cipher (keyword length is six) in which he describes the cipher. It is very clever. Simple to implement but a devil to crack, and my one hope is that we can also find the cipher key while in the HQ, or at least part of it.   
I plan to enter in two weeks, on December sixteenth. The Russians are hosting a large propaganda event as part of the Internationale Bauausstellung, with leading politburo members in attendance. Most of the security team will be occupied with that and HQ security will be relatively light. With luck I will get in and out with the files we need that night, and then we can get to the bottom of the whole Reichsdoktor stratagem.   
  
All the best, Harry

**Challenge 7B**

Solitary confinement

UOCAD EDMMA EDAEC RRSOI COIPI IFEBO BDUSI SDSBE ENTTY ANETA DCOUD KOOTT RBELE DRAOA USYYO HISNL EDDSR ISHRS HEEOS ETROS TLSEU NRSCC OUWRI MOLHN STERS EDEEA RINTE WPENN OMSFT AITOF TOILL CAPEC ESEPN DUETN DEEUS ESOMF AKOGT INLGE LYARU ITSIC RIOIR SECOR ETNEU EATMT ALIHL EICRV EASME NCIED ATHEO LKWHE OHNWO NFIMH THUBE AIBND ATTHU EKTDO OECTW ITABA OULCA QWIUP IYPOC ODEEO ONSHI TCIEE ATAIA CLTTA RCHGH OFHET DPAEC HMAHV EHLOL YARLE IKEDR ODTEI DYSKE EYCFS HFOFE HTGEJ NDBBR YPHON IOSRO LMREF RWFII GHYPH NMEHR ELASO NDEIV TDTIR HEROT URECH ORHEG YNDED MEPYT WVIID OMOUT YAION AUFUC ATWOU OKTEF LTHMU TGNEC TITAR AOWEN NGSST EFRRE SCLFS PSATO EHIHE LASTV CHIFI IUTET EYEEC STNHE OILDS TNEPM ROSTT SRAFL LRHED ISESS RETIE NASU

, key=)

Security Protocol Solitaire.   
  
Comrades, under a decree from Moscow we are confined to using a new high security stream cipher stolen from the Americans, the solitaire cipher. All files classified Top Secret and above are to be archived using this method. This new field cipher has been tested and proven to match the security of the Fialka machine without the overhead of the technology. You will need only a deck of cards to implement the cipher. The key to be used will be provided and distributed on a one-time pad and you must destroy the key as you use it. The key consists of a random shuffle of a full deck of cards, together with two distinguishable jokers. Agents should be freely able to carry this equipment without arousing suspicion.

Challenge 7B was a beast! The AMSCO cipher is a classic pencil and paper column transposition, with a twist. As we said in the hint the other day, you can read about it at <http://cryptogram.org/cdb/aca.info/aca.and.you/chapter_09.pdf#AMSCO>. It was tough, but still 281 of you cracked it which really impressed us. The solution to 7A contains a lot of intel about Challenge 8 so whether or not you tackled that last week, take a good look at the solution.

If you have cracked Challenge 7A you will have discovered that Challenge 7B is an AMSCO cipher. This is a column transposition cipher with a twist. You can find out how it works at <http://cryptogram.org/cdb/aca.info/aca.and.you/chapter_09.pdf#AMSCO>

The real security in the cipher lies in the fact that you dont know the length of the keyword, though cribs can help you to reconstruct that if you have some. If you really like a challenge you could try that first. Otherwise you could use the exceptionally useful advice from 7A where we tell you the length of the keyword. Once you have that it is possible to lay out the text in columns and use cribs and smarts to reassemble the plain text. Or it would be if you knew which of two possible conventions we have used. Pairs then singles or singles then pairs. But no hint about that I am afraid. You will have to try it for yourself.