TUESDAY AFTERNOON BREAKING VIGENÉRE CIPHERS

History: we learned earlier that Vigenére ciphers were considered unbreakable from the 16th until the 19th century (they started to be broken in the mid 19th century). Remember, a Vigenére cipher is just a set of Caesar shifts, and this can be quite easy to break if you know the length of the key phrase (you can analyze each shift independently).

The main goal should first be to figure out the key length. One simple strategy to do this is called *autocorrelation*. Basically, you take your cipher text, for instance

```
HYEZ QVVC PZHX TZBP WLRC VHXP HOSO QCYJ TYRP RREV LOPJ ZLRR EVPR GTUL RPCS JMAS SYW
```

One then shifts the text over by 1, 2, 3, etc. After each shift, one counts the number of letters that are in the same position. For example.

H	Y	E	Z	Q	V	**V**	C	P	Z	H	X	T	Z	B	P	W	L	R	C	V	H	X	P	H	O	S	O	Q	C	Y	J	T	Y	R	P	R	**R**	E	V	L	O	P	J	Z	L	R	**R**	E	V	P	R	G	T	U	L	R	P	C	S	J	M	A	S	**S**	Y	W
W	H	Y	E	Z	Q	**V**	V	C	P	Z	H	X	T	Z	B	P	W	L	R	C	V	H	X	P	H	O	S	O	Q	C	Y	J	T	Y	R	P	**R**	R	E	V	L	O	P	J	Z	L	**R**	R	E	V	P	R	G	T	U	L	R	P	C	S	J	M	A	**S**	S	Y

One then looks for columns where both letters match. Count these columns. In this example, the count is 4. Generally, if you shift by the key length (or a multiple of the key length), then the autocorrelation will be large. This works better for large texts, although in this example you get an autocorrelation of 9 for a shift of 10, which means that 10 is probably a multiple of the key length (or equal to the key length). The actual key length in this example was 5.

1. Below is another communication to the Assassin which has been intercepted. We believe they are using a simple Vigénere encryption scheme. Please find the key and decrypt the message. Lives are at stake. A digital version of the ciphertext is available on a usb key.

SDWB MTST JRYP PTSZ MGFG EFZF JHJX OARP FHGE BNOP JRTP OYJZ MFWX DEYE JSUH STZY LVJL DIPY LWXM XOCV ABLH OTSP VSAB DENZ VSST NEOE ZCYA PRLN DSMT TBPP FSCM SEXP DMZL FFFW OSMH QEEZ MGJM IEDN ASSM JSED DCAX PFWT GBJE NOOP DHWT JNDL KZJO FRLR WZFM FRES AGXN NMPC UCSM JNFP LCPX FPFD SDUK BIDP VCKT OYCP DOYX EDPG WZTI NEYE KMTN SCZY UZZL JOYE ZOYM IEOP NWHX DOXM ABJL FLPX WBYL PFBF SBYN NCZX HIYX SSHT LVWX EANE WRNL WECJ ABYK JGFT FUUE FADP UCSY JRXE ZWXB GPZD KWGE FHLG WMTN NAOP SBDI SORC WGXZ BIYT FUJG URJT FHTM IENW SGXB GIPO XWQX THPW VOYM IEZQ XWHX PFYL NOQK FSPL JQMP FBPW ASAX UHPN GRJL XEDP FHDH VWTW DCSE ZRPX SWSO BLTO XCWL JXEP WBRH SEOL QGUE FADP ABKH SMFD GTFG ZDTQ XWHN MTTP KMTN FNNZ MBYX STSP MDHH NIYR YFFW VAET GBHX SEXZ FWJL NAJA JCAB EEJZ MQJK UATY GDUH STFY AHNX TPWP SGJW PNZE KEZT ODPC LVJF XESL NSWX DETG WRWX QOCE KCKR PUNW SWRB OGCP AAGN SSPX WBYX YPPY KSXY PRWL JUJT NOFY LGTY JCPN JSFF QLPL KSWX NEXM WFYA BTES WGDG EINL LSTG MYAC GJNW FSCP AAGN SSPX WBYY PRWP YWYB NAEP TIXB OEDD WLUX OSPD XWST MLJH WKTN MDWT CSDH VTZT FJNM FYZF LCOH JNES WIUV PMTY YGDG EINL LSXH GTML DZYX BMHP ZOAX BNPI UWYB OGDN ZSIN MEES AGDX BRLY VKJT SEYP WRTY NOCP EOQX QLLJ WFXL QOED SFJY JLWT FUZI GADE SBIH VRQT JGYZ BMPL YONG TTVL GGNL PNXL QGJV PNOE ZWXR FACH WKNE MMLV WOGB HPFD ZHTP JNES WOJL PLZC SZQX WIWD WQWX UOCR SBQB AAET GBQX BGFP DSYN TKYZ OWKR PULC WWSM FRPD LSIU ZAAC AZYA JREP WBYA