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.

LTRO FXSM RJNA ZXHU OWLR DLIY CXEK HERI NZGS XINZ UVJC AQFS RCOA LVPG ETNV PTOX NSYX HKMG TINZ CWEA OXEM YKOT NLPH EBCG PGOJ YRLQ EJNL ZXHU LENP ENUW MIET YBEV ESYP JYSK ZYWA ENIT PXOA MIEL EYWM PRTO MXDP OBYS QPIU HIWQ OJYP EVAO HWLW LKPI CEGK FEEI RZBM DWUS GICG OTNM YYEZ IOPI PAME ATRG CWPH OLUR JVER UXPH DKPI WSPS YREW YUOV NSNI FYDM OTNL LXTN YHPZ IIYG ZQBO HIDI LKGI YXSU ZUFE NZOQ NSMV OXPV SCCX SVEJ UGEI DOMZ PVYO HXCM GACR RTLK UWPG OTZM CQTN CWTJ PUMW TFLK BEGI YUOQ LHEG HCAV OMLI DWGG CRTR GKHX CCIT NSEL EIFE DWIL CIOJ IRYW SILJ UXEL EUZJ TGEU ZRLZ ARLI DIAX WLHI BKFM PZEZ BINS DKMA PWET NCZY WOFP ZRLE LIXE ITPE WMDL IVDM XZYI YQOX YHLC SVFI LWEO HJZV MAMS QENE XMQJ IIOP EMEY SSFI NIIY YXEX NLPY PIIQ TRGM LEOY AZCS YGEX YQZR IKMQ LCPX IZTH EEIY NIRZ UMYS PVIV EYNO NMPW PRYE DIDU HSEW QAUR OIRZ BIXA ENUZ PVEI YMGI DXYT ZVTY IJJS UIFE TQIT AVPM MHOV DIMK HXPB PKHW PWFU LPLV GKUQ ZYNZ MSQM CKWV PEMV FILW EXYQ PQBK LXSE TZBI DCNJ CGLX EUHP JTRU PMOI SXYM XFUX MIXI NZZS CPEM CXTQ AZYF FWIT YWDI XVYR DISL CRLP LEQI HSUR XPTO EEIY ESIT PMEI YUOX ZNOO HXSI UVWS XMNM MCYH IIUX PWOL NFLP LZYE XAEN UZPE NKRG TXIT AWNL EJOP PXHO MCPE RGHH HIAX YRPI DUZQ ZVEL YQLP EVFE JIRY MTZX SGLI QMLR CRRY PLUW EENJ IYCJ IXMX REMK UKLM NYNO LSSO MSYQ AEMI NSNJ NLTW YKUV HIWO FPXE KKUF TKPA MLES WOHX SIAK MSWS RGFP PZIR MINV EZIV RENO TEEM OTFI LKUK FIEY SQHS HMFE IYLV EOHX PVEY NIOF YGJV TPTN CVEI ETNL