

Recap of the lecture on the Civil War Vigenere discovery

Recently a Civil War encrypted message was discovered (see <http://www.aolnews.com/2010/12/25/civil-war-message-in-a-bottle-opened-decoded/>). We will now decode it, using just a little knowledge of the event. The original message even had punctuation, which we will not need to use.

```
In[48]:= encryptedmessage = ToUpperCase [
    "seanwieuiiuzhdtgcnplbhxgkozbjqbfegtzzbwjjoytkfhrtpzwkpvrursqvoupzxggoephckuas :
    fkipwplvoji zhmnvnaeudxyfdur jbovpasfmlvfyyrdelvp lwagjfsxgjfxsbcuahapmcmphi :
    jmvbtasetovbocajdsvqu" ]

Out[48]= SEANWIEUIIUZHDTGCNPLBHXGKOZBJQBFEGTZZBWJJOYTKFHRTPTZWKPVURYSQVOUPZXGGOEPHCKUASFKI :
    PWPLVOJIZHMNNVAEUDXYFDURJBOVPASFMLVFYYRDELVPLWAGJFSXGJFXSBCUHAHAPMCMPHIJMVBTA SE :
    TOVBOCAJDSVQU
```

The news story stated that this message was sent to General Pemberton. It is not unreasonable to guess that the message started with something like "Dear General Pemberton". After a few false starts, one could try "genlpemberton" as the opening line, and see what the key would be. We found (by subtracting mod 26) that the key would have to start with the characters

MANCHESTERBLU

A very nice guess is that the key is MANCHESTERBLUES or MANCHESTERBLUFF. Since the latter was one of the 3 main key words the Confederacy used (and it seems they sent the message) during the Civil war, we will use that. See http://en.wikipedia.org/wiki/Vigen%C3%A8re_cipher for a discussion of this weakness. In fact, knowing that there were only 3 key words and the spacing between the words was given makes it very easy for the code to be cracked. Then with this knowledge, we then decoded the rest of the message:

genlpembertonyoucanexpectnohelpfromthissideoftheriverletgenljohnstonknowifpossiblewhenyoucanattackthesamepointontheenemyslinesinformmealsoandiwillendeavortomakeadiversionihavesentsomecapsexplosivedevicesisubjoinadespatchfromgeneraljohnston