

## WEDNESDAY– BUILD YOUR OWN CIPHER

**1.** Your job is simple, build your own cipher that can be worked by hand (with some sort of code-phrase). You could do Vigenere + Columnar Transposition, or Substitution+Vigenere, or Caesar Shift + Scytale, or your own variant (can you think of a way to make your cipher resistant to letter frequency attacks?).

Write it down here (each person should have a copy). Explain carefully each step. Run it by me or Andrew.

**2.** Practice using your cipher, choose a common code-phrase. Break off into pairs. Each pair of people should choose a key and encrypt a sentence. Pass the other pair your code phrase and the ciphertext. They will do the same. Decrypt theirs while they decrypt yours.

**3.** Find another country who has also built their own cipher. Explain it to them, and have them explain to you theirs. Fix any problems if necessary.

**4.** Now, have your team encrypt a message using their cipher, they will do the same. Send them the message with their code, they will do likewise. Decrypt theirs while they decrypt yours.

**5.** Talk to me about implementing your cipher into the computer (I will do so if feasible).