Caesar Cipher

*If he had anything confidential to say, he wrote it in cipher, that is, by so changing the order of the letters of the alphabet, that not a word could be made out. If anyone wishes to decipher these, and get at their meaning, he must substitute the fourth letter of the alphabet, namely D, for A, and so with the others.*

– Suetonius, Life of Julius Caesar

**Protocol**
Shift each letter of the plaintext forward in the alphabet by a given amount to encrypt.

**Example**
Shifted by 3, so that A becomes D, B becomes E, and so on.

plaintext: IF VOTING CHANGED ANYTHING IT WOULD BE ILLEGAL

ciphertext: LI YRWLPK FKDOQKHG DQBWKLKP LW ZRXOG EH LOOHKDO
Vigenère Cipher

Protocol
Given a word, shift the first letter of the ciphertext by an amount corresponding to the first letter of the word’s place in the alphabet, the second letter of the cipher according to the place of the second letter of the given word, and so on. When you have used all the letters of the given word up, start at the beginning of the word again.

Example
Given the word ACT:

plaintext:   RESPECT EXISTENCE OR EXPECT RESISTENCE

plaintext:   RGLPGVT GQIUMEPVE QK EZIEEM RGLIUMAPVE
Rail-fence Cipher

Protocol
The plain text is written downwards and diagonally on successive ”rails” of an imaginary fence, then moving up when we reach the bottom rail. When we reach the top rail, the message is written downwards again until the whole plaintext is written out. The message is then read off in rows.

Example

plaintext: ATONETIMEINtheworldtherewerewoodsthatnooneowned


ciphertext: ANIIHODEWEOTTOOETEMNERTREWDHNNWDOTETWHLHEROSAOEN
One-time pad

Protocol
Given a random sequence of letters (the “one-time pad”) as long as your plaintext, shift the $k^{th}$ letter of the plaintext by an amount in the alphabet corresponding to the $k^{th}$ letter of the one-time pad.

Example
Given the above-right pad:

plaintext: ANOTHER WORLD IS POSSIBLE

ciphertext: LSVAFDR DGSUU VP ZGQFNWVS
Protocol

Start with an initial, given placement of each rotor. Before encoding each letter:

1. If the notch on either the left or middle rotor is at the rotor setting line, rotate all three rotors rotate up one position.
2. If only the rightmost rotor has its notch at the rotor setting line, then the middle and right rotors rotate up one position.
3. Otherwise, only the right rotor rotates up one position.

Once the rotation is complete, find the desired letter on the INPUT/OUTPUT panel and follow the connected wires across the 3 rotors, around the reflector, and back across the rotors to the corresponding letter on the INPUT/OUTPUT panel.

Example

Using the paper Enigma model with rotors set LDO along the rotor setting line:

plaintext: SLOW
ciphertext: RANE