Vigenère Ciphers

Substitution ciphers are very susceptible to attack by frequency analysis. Vigenère ciphers were an early attempt to correct for this weakness: they are not substitution ciphers. In Vigenère encryption, a particular plaintext letter may be replaced with any one of several different ciphertext letters, depending on its position in the plaintext.

The encryption key for a Vigenère cipher is a word (by "word" we mean a finite sequence of characters — or their numerical representatives — from the character set used for the plaintext messages). To describe the encryption, we again consider the following conversion table for the English alphabet:

0	1	2	3	4	5	6	7	8	9	10	11	12
A	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*

13	14	15	16	17	18	19	20	21	22	23	24	25
N	*O*	*P*	*Q*	*R*	*S*	*T*	*U*	*V*	*W*	*X*	*Y*	*Z*

Suppose we want to encrypt the message "Gene Kelly's dance" using a Vigenère cipher with encryption key *rain*.

i. Using the table, we can represent the letters in our message "Gene Kelly's dance" with their corresponding numbers: 6 4 13 4 10 4 11 11 24 18 3 0 13 2 4.

ii. Now we represent the letters in the keyword with their corresponding numbers: 17 0 8 13. Then repeat the representation of the keyword until we have a string of the same length as our message and place it below the representation of the plaintext:

6	4	13	4	10	4	11	11	24	18	3	0	13	2	4
17	0	8	13	17	0	8	13	17	0	8	13	17	0	8

iii. Now add each number in the top row to the number beneath it and reduce modulo 26 to get:

23	4	21	17	1	4	19	24	15	18	11	13	4	2	12

iv. Finally, use the table to replace the numbers from step *iii* with their corresponding letters to obtain the ciphertext: XEVRBETYPSLNECM .

For practice, try encrypting the plaintext "make your garden grow" using a Vigenère cipher with encryption key *showers* and see if you can get the ciphertext EHYACFMJNONHVFYYCS.

The following ciphertext was produced using a Vigenère cipher with encryption key *Jolson*:
FVPJSLXIDWSPUCFVGHYCYLVRQWWDGLXIDGCAFWWDGRNQCGKQBCQVOSOCOAZFBCVWS
CXBWGCXRBRXCEJPWMSORFOSBQUWDLBVWUQGFURGDGBTFVPFSINFLHFVUGSGKRAGNG
ARJZZFU.
See if you can decrypt it by reversing the encryption algorithm. (Note that the line breaks do not necessarily occur between words!)

While Vigenère ciphers are less susceptible to attack than substitution ciphers, they are by no means secure. With messages of moderate length, relatively simple attacks are well-known, and can be performed efficiently. For more on how to attack a Vigenère cipher, see (for example)

http://www.nku.edu/∼christensen/section%2012%20vigenere%20cryptanalysis.pdf

and

http://www.cs.uri.edu/cryptography/classicalvigenerecrypt.htm

or any text on classical cryptography.