Cryptography Part 1

Cryptography is the science of secret writing. **Encryption** is the scrambling of a message. One way to scramble a message is by substitution of whole words or phrases (**encoding**) or of letters (**enciphering**)

What advantage does each offer?

Examine the following enciphered message and see if you can determine the monoalphabetic cipher used to encrypt it:

“Adp jtr bi rml tiumdprlg oduewdrlpq ja rml tiadqmbjidofl lig ja rml wlqrlpi qkbpdf dph ja rml Sdfdxy fblq d qhdff tiplsdpglg ylffjw qti. Jpobrbis rmbq dr d gbqrdiul ja pjtsmfy ibilry-rwj hbffbji hbflq bq di trrlpfy biqbsibabudir fbrrfl oftl splli kfdilr wmjql dkl-glquliglg fbal ajphq dpl qj dhdzbisfy kpbhbrbvl rmdr rmly qrbff rmbie gbsbrdf wdrumlq dpl d kplrry ildr bgld.”   
Gjtsfdq Dgdhq, Rml Mbrummbelp'q Stbgl rj rml Sdfdxy

How can cryptographers make enciphered messages more difficult for cryptanalysts to decipher?

* Inserting nulls in the ciphertext
* Dalibrit maspahleng mex freekwinsy uhnalsiss duhfhekult

Frequency Analysis

Al Kindi wrote a treatise, Deciphering Cryptographic Messages, in the ninth century:

*"One way to solve an encrypted message, if we know its language, is to find a different plaintext of the same language long enough to fill one sheet or so, and then we count the occurrences of each letter. We call the most frequently occurring letter the ‘first', the next most occurring letter the ‘second', the following most occurring the ‘third', and so on, until we account for all the different letters in the plaintext sample.*

*Then we look at the cipher text we want to solve and we also classify its symbols. We find the most occurring symbol and change it to the form of the ‘first' letter of the plaintext sample, the next most common symbol is changed to the form of the ‘second' letter, and so on, until we account for all symbols of the cryptogram we want to solve"*

This became known as frequency analysis.

For your interest:

www.counton.org/explorer/codebreaking/pigpen-cipher.php

www.dcode.fr