Cryptography and cryptanalysis I: Fun and games.

Exercise 1. Try to decipher the following cipher text, encrypted with a CAESAR cypher:

VLPS OHFL SKHU VDUH QRWY HUBV HFXU H.

Exercise 2. Decipher the following text, encrypted with a monoalphabetic substitution:

SBKG SYOS KGYX GUSD EYXF.

Exercise 3. The following text has been encrypted with a Vigenère cipher of period 5 such that no letter is ever encoded by itself, and the word "thunderstorm" appears in the text. Can you decipher it?

HHYO IYIC NRKS MLXV GHLW HEKK

SHQC BRNU YMYU RYKG VKYK

Exercise 3. One more: can you decipher the following text? It is encrypted with another Vigenère cypher of period at most 4.

LTHV NDFE RVAQ CAMG STIF HFID

QTER RZVT ZWEL HNSW OAHT QXES

KASL FHVN NWFZ OSDL NNWH DUWN

UDRD SSDT DPEM WIRH ISKE QWRT

HOQH AKVE

Some frequencies of letters and groups of letters: In a typical English language text, the most common letters are {etoani} followed by {rsh} {dl} {ucwmfygpb}. The most common two-letter combinations (called *bigrams*) are /an/, /at/, /er/, /es/, /he/, /in/, /is/, /nd/, /nt/, /on/, /or/, /re/, /st/, /th/, /ti/, /to/. Bigrams that are much more common than their reverses are /th/, /he/, /ea/, /nd/, /nt/, ha/, /ou/, /ng/, /hi/, /eo/, /ft/, /sc/, and /rs/. The most common trigrams are /the/, /ing/, /and/.