cryptanalysis

cryptanalysis: The process of recovering plaintext from ciphertext without knowledge of the encryption method and key
- code breaking based on letter frequency. — one method of cryptanalysis

- most frequently used letter in English:

E, 13%
T, 9%
A, 8%
⋮

ex: suppose the intercepted ciphertext message is
25 13 10 10 6 23 17 4 7 19 23 9 12 10 25 24 25 13 10 2 20 23 18
ZNK KGXRE HOXJ MKZY ZNK CUXS
produced by a shift cipher. What was the original plaintext message?

Solution:
- Determine most frequent letter from above

Z: 3
N: 2
K: 4 ← most frequent, we assume it is the encrypted letter for E
G: 1

Find shift key

Integer associated to K is 10

" " "E is 4

$f(p) = (p+k) \bmod 26$ ← original unencrypted letter's integer

$10 = (4+k) \bmod 26$

Shift key → $K = 6$

Since we're trying to decrypt, each encrypted letter's integer should be passed through to:

$f^{-1}(p) = (p-k) \bmod 26$

↑ The encrypted letter's integer

Shift the letter's integers back by 6.

19, 7, 4....

- convert integers to letters:

THE EARLY BIRD GETS THE WORM

Because message makes sense, you're done. otherwise, if random letters try again with K mapping to T.

Block ciphers:

- Replacing blocks of letters with other blocks of letters.
- Transposition cipher:
  - Break up message into blocks
  - Re-arrange letters within each block based on rule.
  - set is $\{1, 2, \ldots, m\}$

ex: using the transposition cipher based on the permutation σ of the set

$m=4$ $\{1, 2, 3, 4\}$ with $\sigma(1)=3$, $\sigma(2)=1$, $\sigma(3)=4$, $\sigma(4)=2$

Solution:
Break up message into groups of 4, because
Pad with random letters (if necessary).

a. Encrypt PIRATE ATTACK

Solution:

Step 1: Break up in groups of m, in this case it's 4: PIRA
TEAT
TACK

Step 2: Rearrange:

I A P R E T I A A K I C

$\sigma(1)=3$ ↙ means take first letter and move to position 3

$\sigma(2)=1$ ↙ " " second " " " " " 1

⋮

of each block