

1. Break this ciphertext that was enciphered using Vigenere with a two letter keyword (the keyword will not necessarily be a real dictionary word):

VJ GO QP MG AF QG UP QV NK MG DC PC PC U

given that “bananas” appears in it.

2. Find q, r with $0 \leq r < a$, so that $b = a \cdot q + r$ with:

(a) $a = 304236, b = 2961857$

(b) $a = 483425, b = -1512570$.

(c) $a = 363537, b = 65441$.

3. Find the inverse of 10 (mod 38) (that is, find c such that $10c \equiv 1 \pmod{38}$) or explain why it does not exist.
4. Break the message:

DIYC LXIV UCFX ONNC BIYC LXIV

knowing it was encoded with an affine cipher and contains the word “affine”.

5. Use the vigenere applet at

<http://math.ucsd.edu/~crypto/java/EARLYCIPHERS/Vigenere.html>.

Choose a random ciphertext and try to break it. Write down the keyword.

6. Prove that if $d|a$ and $d|b$ then $d|a + b$ and $d|a - b$.
7. Prove that if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ then $a+c \equiv b+d \pmod{m}$, $a-c \equiv b-d \pmod{m}$ and $ac \equiv bd \pmod{m}$.