Vignère Ciphers

A Vignère Cipher is like a Caesar Cipher, but instead of every letter getting shifted by the same amount, a repeating pattern “secret key” specifies how much every letter should be shifted.

For example, a secret key “12 21 11 5” means that the first character should be shifted 12 letters in the alphabet (i.e. A becomes L), the second character should be shifted by 21 letters, third character 11, fourth character 5, then the 5th character by 12 again, and so on.

The secret key needs to be known by both the message sender and the receiver. To make the repeating pattern easier for the message sender and receiver to remember, the each number in the pattern could be replaced with the corresponding letter. “12 21 11 5” could be represented as the 12th, 21st, 11th and 5th letters of the alphabet: “LUKE”.

Vignère Ciphers can be sigificantly harder to crack than Caesar Ciphers, especially if the pattern is long and rarely repeats. However, if you know the length of the repeating pattern and if the message is long enough, you can still use frequency analysis to crack the code; for example if the pattern is only 4 values long, you would need to perform frequency analysis on every 4th letter separately.

WLZDS: EDDSP ER OZ ARDLLD. EZJ'S NLGD NP ZDTENNZ JKT. ZZQ CP YKS ZPP QFLHHAP UNVC ELQZNSBYYD. ZZQ GBGA NOWU AFRQM UZ ZHTNKUFC UNVC LNXPN. IPTJ LF LJC J HEKM NKLQWASF JKTS ENZJYEMH. HESI ZQQ DZIAJYAC TENDORPG, XP YZO PJC USER EPOSSFYSJGA BPYBKJNP ZOO XQJYC NSOAQ UZ PGF RWKBIU.

KVVA: H'MW JDWPN IPTJ XPF!

RZEPN: HG JKT PYHX LYAV USA OPHAQ PQ PGF OWQL DECF. ZXH-XLJ MFGAQ UZHC ZZQ VILP GBALDOPZ SP JKTS QWSIPN.

KVVA: GF EKKE XA DOZQFI! TP VBD UNV HDN LTHKFO DHN.

GWCFC: JN. J LI XPFN EBEDDS.

DDNDVAC, MFGD MZKJT LP UBOAQ JY QSUPN CJDXDMTAE.

MFGD: OZ. JN. USWS'T YKS UCQD! USWS'T TIOPDOHCWA!

UBOAQ: TPWQDS UNVC BDFWEMHD. UNV VJNX TP SP MA SSFA.

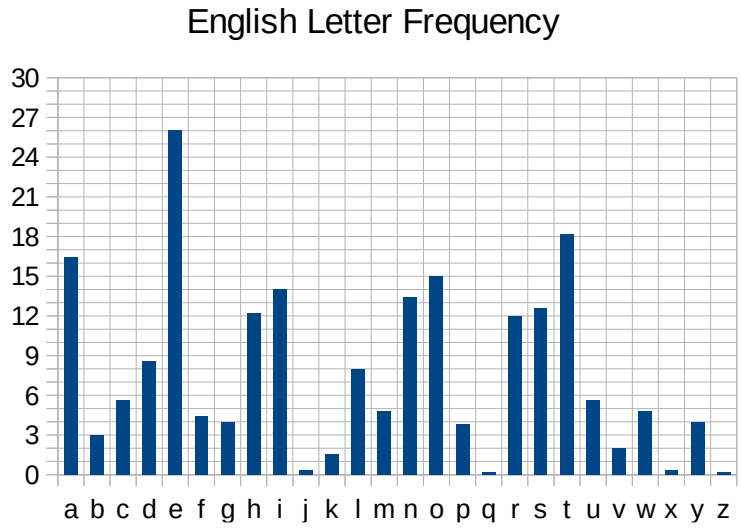
KVVA: MP! YK! MP!

GWCFC: HTLP. UNV NWM EPOSSZU SIP ALQPNNS. SA GBD BNSPODFY PGJD. ES JD UNVC ZDTEEMZ. UKHO XA, ZOO PNHPPGFC
SD DLJ QVWA SIP CZMLTX BD BZUSAQ BYZ RPY. YNNP SHUS ID. JE ER USA NOWU VBJ.

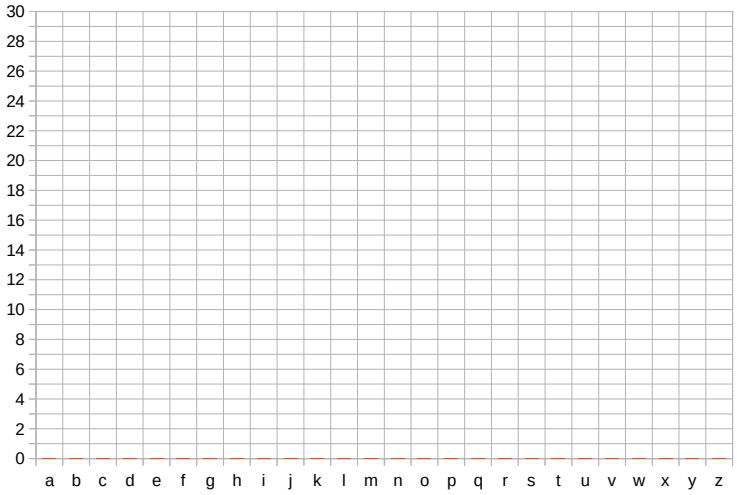
PGF NKCF ADQBDA HT JKCB.

- How could you deduce that the secret key is probably 4 long in this message?
- What is the secret key?
- How you make really long secret keys? (at one extreme, read about “one-time pads”)

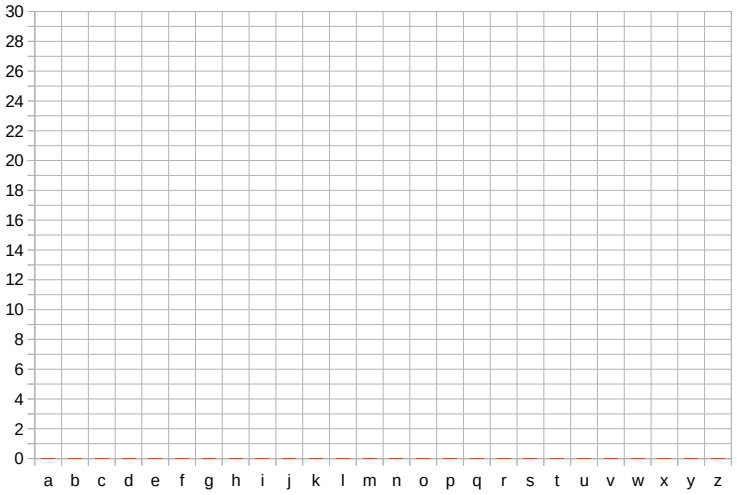
Worksheet



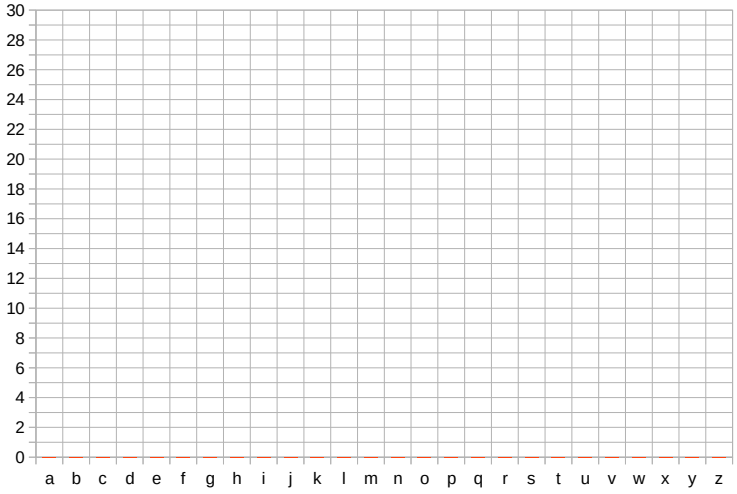
Frequency #1



Frequency #2



Frequency #3



Frequency #4