Assignment # 1 Thomas Boyko

We are given the ciphertext:

K0EREJEBCPPCJCRKIEACUZBKRVPKRBCIB0CARBJCVFCUPKRI0FKPACUZ0EPBKRXPEIIEAB DKPBCPFCDCCAFIEABDKPBCPFEQPKAZBKRHAIBKAPCCIBURCCDKDCCJCIDFUIXPAFFERBIC ZDFKABICBBENEFCUPJCVKABPCYDCCDPKBCOCPERKIVKSCPICBRKIJPKABI

A simple internet tool gives us the letter distribution:

C-32

B-21

K-20

P-20

I-16

E-13

A-13

R-12

F-10 D-9

J-6

U-6

0-4

Z-4

V - 4 0-2

X-2

H-1 N-1

Y-1

S-1

We are instructed to follow the English distributions, so we suppose that the function E_k maps E to C, and we must take a guess which of B,K,P is mapped to T. After trying to solve the associated systems of congruences, we find that only one system produces a valid plaintext:

$$19a + b \equiv 1 \pmod{26}$$

$$4a + b \equiv 2 \pmod{26}$$

Subtracting the equivalences, we get:

$$11a \equiv 1 \pmod{26}$$
.

And we solve for $\alpha \equiv 19 \pmod{26}$ using the Extended Euclidean Algorithm. Substituting back into our original congruences, we find $b \equiv 4 \pmod{26}$. Then we can use an online decryption tool to decrypt our ciphertext:

ocan adater redenos a ieux ton frontest ceint defleurons glorieux cart on brassa it porter al contrator de la contrator de lle pee il sait porter la croix ton histoire est une epope e desplus brillants exploits et tavant de la constant de la constaaleurdefoitrempeeprotegeranosfoyersetnosdroits

A Canadaian elementary student would be ashamed to not recognize the French national anthem!