Math 406 – Fall 2025 – Harry Tamvakis
PROBLEM SET 9 – Due Thursday, November 13, 2025

Reading for this week: the cryptography notes from class, and pages 83–89 from Section 11.

Problems

From the cryptography notes, Section 10.1, #3, 5, 11, 12, 13, 14, 15. In addition, do the following problems:

A1) Use frequency analysis and the knowledge that the message was enciphered using a shift transformation to decifer

PXAHE WMAXL XMKNM ALMHU XLXEY XOBWX GMMAT MTEEF XGTKX VKXTM XWXJN TEMAT MMAXR TKXXG WHPXW URMAX BKVKX TMHKP BMAVX KMTBG NGTEB XGTUE XKBZA MLMAT MTFHG ZMAXL XTKXE BYXEB UXKMR TGWMA XINKL NBMHY ATIIB GXLLQ

A2) If the two most common letters in a long ciphertext which was enciphered by an affine transformation $C \equiv aP + b \pmod{26}$ are V and A respectively, then what are the two most likely values for a and b?

A3) Decipher the message IEXXK FZKXC UUKZC STKJW that was enciphered using the affine transformation $C \equiv 11P + 18 \pmod{26}$.

A4) Let p be an odd prime and $(a, p) = 1$. Show that the quadratic congruence $ax^2 + bx + c \equiv 0 \pmod{p}$ has a solution in x if and only if $b^2 - 4ac$ is either zero or a quadratic residue of p.

A5) If $p = 2^k + 1$ is prime, show that every quadratic nonresidue of p is a primitive root of p. [Hint: Apply Euler's Criterion.]