Math 342 Tutorial

July 30, 2025

Question 1.

(a) If the two most common letters in a long ciphertext, encrypted by an affine transformation $C \equiv aP + b$ (mod 26), are X then Q, then what are the most likely values for a and b.

(b) If the two most common letters in a long ciphertext, encrypted by an affine transformation $C \equiv aP + b$ (mod 26), are W then B, then what are the most likely values for a and b.

Question 2.

(a) Decrypt MJMZK CXUNM GWIRY VCPUW MPRRW GMIOP MSNYS RYRAZ PXMCD WPRYE YXD which was encrypted using an affine transformation.

(b) Decrypt WEZBF TBBNJ THNBT ADZQE TGTYR BZAJN ANOOZ ATWGN ABOVG FN-WZV A which was encrypted using an affine transformation.

(c) Decrypt PJXFJ SWJNX JMRTJ FVSUJ OOKWE OVAJR WHEOF JRWJO DJFFZ BJF which was encrypted using an affine transformation.

Question 3. What is the plaintext message that corresponds to the ciphertext 1213 0902 0539 1208 1234 1103 1374 that is produced using modular exponentiation with modulus $p = 2591$ and encryption key $e = 13$?

Question 4. Show that the encryption and decryption procedures are identical when encryption is done using modular exponentiation with modulus $p = 31$ and enciphering key $e = 11$.

Question 5. Suppose a cryptanalyst discovers a message P that is relatively prime to the enciphering modulus $n = pq$ used in the RSA cipher. Show the cryptanalyst can factor n.

Question 6. Show that it is extremely unlikely that a message such as that described in the previous exercise can be discovered. Do this by demonstrating that the probability that a message P is not relatively prime to n is $\frac{1}{p} + \frac{1}{q} - \frac{1}{pq}$. Assume that it is equally likely for a message to fall into each residue class modulo n.