Math 3 - Discrete math (V3020) Exercises, week 4 (due Sep 30th, 2025)

1. Can you crack the coded message

   ZAHYA CVYRPUN VU AOL OVTL LDHT WYVQLJA

   that's been created using an unknown shift cipher? The message is in English and uses the English alphabet.

2. You receive an encrypted message from your friend stating

   25151440 13535569 4998754

   You remember that earlier you had talked about a cryptography protocol introduced at a math lecture, and that you had told your friend of a public key with $k = 86123123$ and $m = 94642061$. Only you know that you used two primes $p_1 = 10093$ and $p_2 = 9377$ to generate the key $m = p_1 p_2$.

   Since the primes you used are so small, you assume that each block of the message is encrypted separately using the protocol. Can you decipher what your friend sent you? The original message was encrypted from the decimal representation of the ASCII characters (065 = A, 066 = B, etc.).