Math 342 Tutorial

July 30, 2025

Question 1.

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

(a) E and T are the most common letters. $E = 4$, $T = 19$, $Q = 16$, and $X = 23$. We suspect that $a4 + b \equiv 23 \pmod{26}$ $a19 + b \equiv 16 \pmod{26}$, which has the solution $a = 3$ and $b = 11$.

(b) E and T are the most common letters. $E = 4$, $T = 19$, $W = 22$, and $B = 1$. We have $22 \equiv a4 + b \pmod{26}$ and $1 \equiv a19 + b \pmod{26}$. This system has the solution $a = 9$ and $b = 12$.

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 FNWZV 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.

(a) Try $J \to E$ and $O \to T$. Solve $9 \equiv a4 + b$ and $14 \equiv a19 + b$ to get $P \equiv 3C + 3$. Then the message becomes WEUSE FREQU ENCIE SOFLE TTERS TODEC RYPTS ECRET MESSA GES.

(b) We solve to get $P \equiv 5C + 13$. The message decrypts as THISM ESSAG EWASE NCIPH EREDU SINGA NAFFI NETRA NSFOR MATIO N.

(c) Solve $9 \equiv a4 + b$ and $14 \equiv a19 + b$ to get $a = 9$ and $b = 25$. Then we solve $C \equiv 9P + 25$ to get $P \equiv 3C + 3$. The message decrypts as WEUSE FREQU ENCIE SOFLE TTERS TODEC RYPTS ECRET MESSA GES.

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 $e = 13$?

The inverse of 13 modulo 2590 is 797. The planetext blocks are then given by $P \equiv C^{797} \pmod{2591}$. Decyphering, we get DO NO TR EA DT HI SX.

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 $e = 11$.

We have that $11 \cdot 11 \equiv 1 \pmod{30}$.

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.

Since a block of ciphertext p is less than n, we must have $(p, n) = p$ or q. Therefore the cryptanalyst has a factor of 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.

The probability that an integer in the range $0, \ldots, n-1$ is divisible by p is $1/p$ since there are q integers in the range pq that are divisible by p. Similarly, and integer is divisible by q with propability $1/q$. The probability that it is divisible by both p and q is $1/pq$ since only 0 is divisible by pq in the range $0, \ldots, n-1$. Therefore, the probability that $(P, n) > 1$ is $1/p + 1/q - 1/pq$, as desired.