Homework 1

Eli Bullock-Papa

February 3, 2025

Problem 1

Stinson, 2.6: If an encryption function $e(k, p)$ is identical to the decryption function $d(k, c)$ for the same key k, then the key k is said to be an involutory key. Find all the involutory keys in the Shift Cipher over $\mathbb{Z}_{26}$.

Remember:
$e(k, p) \equiv p + k \pmod{26}$
$d(k, c) \equiv c - k \pmod{26}$

Solution:
For any plaintext p, if we encrypt and then encrypt again with an involutory key k, we should get back p:
$p \equiv e(k, e(k, p)) \pmod{26}$
$p \equiv e(k, p + k \pmod{26}) \pmod{26}$
$p \equiv (p + k) + k \pmod{26}$
$p \equiv p + 2k \pmod{26}$
$0 \equiv 2k \pmod{26}$
$k = 13, 0$
Thus, $k = 13, 0$ are the only involutory keys in the Shift Cipher over $\mathbb{Z}_{26}$.

Problem 2

Stinson, 2.26: We describe a special case of a Permutation Cipher. Let m, n be positive integers. Write out the plaintext, by rows, in $m \times n$ rectangles. For example, if $m = 3, n = 4$, then we would encrypt the plaintext "cryptography is intriguing" by forming the following rectangles:

cryp	isin
togr	trig
aphy	uing

The ciphertext would be formed by reading in columns: ctaropyghpryitusriiinngg.
(a) Describe how Bob would decrypt a ciphertext string, given values for m and n.
(b) Decrypt the following ciphertext, which was obtained by using this method of encryption (but the values of m and n are not given, nor do you know the number of rectangles, but the text fits into a whole number of rectangles without any letters left over):
MYAMRARUYIQTENCTORAHROYWDSOYEOUARRGDERNOGW

2a Solution:

1. Create a matrix of size $m\times$ row length, where row length = ciphertext length / m. This will store characters..
2. Fill the matrix column wise, such that the first m characters of the ciphertext fill the first column from top to bottom, the next m characters fill the second column, and so on, until all n columns are filled.
3. group each row in the matrix into rectangles of width n
4. Finally, reconstruct the original message by reading each rectangle column top-down left-right

2b Solution: Using a program to test all possible combinations of m and n, I found that $m = 2$ and $n = 3$ produces readable text:

MAR RYQ ECO ARY DOE URG ENG
YMA UIT NTR HOW SYO ARD ROW

The decrypted message reads: "MARY MARY QUITE CONTRARY HOW DOES YOUR GARDEN GROW"

Problem 3

This quotation was encrypted with a Substitution Cipher:

```
AOFKW GOZLP OKLUQ KLGDO BGKCL BQGHL IOCPL GDLWG LZZCP GDOGS
KONQB PLMFP GHCGH LIOCP LGDLW GLZZC PGDOG SKONQ BPIOB HLHLO GLB
```

Carefully explain how you decoded the message. If you were unable to read the message, describe your attempts in detail.

Solution:
Before starting the analysis, I removed the spaces from the ciphertext since having so many consecutive 5-letter words would be highly improbable in natural English text. This gave me:

```
AOFKWGOZLPOKLUQKLGDOBGKCLBQGHLIOCPLGDLWGLZZCPGDOGSKONQBPLMFPGHCGHLIOCPLGDLWGLZZCPGDOGSKO
```

First, I wrote a script to analyze the character frequencies in the ciphertext. The script revealed that L, G, and O are the most frequent letters, appearing 15.53%, 14.56%, and 11.65% of the time respectively.
Letter Frequencies:

- L: 15.53%
- G: 14.56%
- O: 11.65%
- ... other frequencies ...

I then wrote a program to systematically try mapping these three most frequent letters (L, G, O) to the six most common letters in English (E, T, A, O, I, N). The program generated all possible three-letter combinations and showed partial decodings where unmapped letters were represented with asterisks.
For example, if we tried mapping:

- L $\rightarrow$ E (English frequency: 12.7%)
- G $\rightarrow$ T (English frequency: 9.1%)
- O $\rightarrow$ A (English frequency: 8.2%)

The partial decoding would look like:

```
*E***TE*A*E*A***AT*E*T**A**T*A*E**AT*A*TA****T*ET**E**
```

This strategy did not reveal any obvious patterns or readable segments.

Next, I implemented a sliding window approach to try identifying common English words. The program would:
1. Take a list of common English words (e.g., THE, AND, HERE, NOT)
2. For each possible position in the ciphertext, try matching the pattern of letters against each common word
3. Generate candidate letter mappings and score them based on how well the observed letter frequencies matched expected English letter frequencies
For example, when the program found "HERE" as a possible match at position 18:

```
Found mapping from sources: [('HERE', 18)]
Probability Score: 0.711510
Common words found in decoded text: {'HERE', 'HE'}
Partial decode: *E***EE***E******EHERE***R*E...
```

However, this approach generated many plausible mappings with similar probability scores, and even when combining multiple word matches, it didn't significantly narrow down the search space. The high number of possibilities and similar probability scores made it difficult to identify the correct mapping with confidence.

Problem 4. Consider the congruence $9x \equiv 3 \pmod{12}$. If we multiply both sides by 2, we get $6x \equiv 6 \pmod{12}$, which has the solution $x \equiv 1$. But $x \equiv 1$ is not a solution to the original congruence. What happened? All we did was multiply both sides by the same amount! Identify the error in logic being exploited here.

Solution:
The error occurs because we multiplied both sides by 2, which is not coprime with the modulus 12 ($\gcd(2,12) = 2$). When multiplying congruences by a number that shares factors with the modulus, the operation is not reversible and can introduce spurious solutions. This is why $x \equiv 1$ appears as a solution to $6x \equiv 6 \pmod{12}$ but does not satisfy the original congruence $9x \equiv 3 \pmod{12}$.

Problem 5. Solve the congruence $653x \equiv 12705 \pmod{1287719}$ and show your work. You may use a CAS (Matlab, WolframAlpha, etc.) to assist with routine calculations, but not for solving the congruence directly.

Solution:
To solve this congruence, we need to find the multiplicative inverse of 653 modulo 1287719 and then multiply both sides by this inverse.
First, let's verify that gcd(653, 1287719) = 1 using the Euclidean Algorithm:

$$\begin{aligned} 1287719 &= 1972 \cdot 653 + 3 \\ 653 &= 217 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0 \end{aligned}$$

Since gcd = 1, a multiplicative inverse exists. Now we work backwards to find it:
Let k_i represent the coefficients in the linear combination. We compute:

$$\begin{aligned} k_0 &= 0 \\ k_1 &= 1 \\ k_2 &= 0 - (1 \cdot 1972) = -1972 \\ k_3 &= 1 - (-1972 \cdot 217) = 427925 \\ k_4 &= -1972 - (427925 \cdot 1) = -429897 \end{aligned}$$

Therefore, $653^{-1} \equiv 857822 \pmod{1287719}$
Now we can solve the congruence:

$$\begin{aligned} 653x &\equiv 12705 \pmod{1287719} \\ 857822 \cdot 653x &\equiv 857822 \cdot 12705 \pmod{1287719} \\ x &\equiv 857822 \cdot 12705 \pmod{1287719} \\ x &\equiv 662613 \pmod{1287719} \end{aligned}$$

To verify: $653 \cdot 662613 \equiv 12705 \pmod{1287719}$

Problem 6. Write a formal definition of the Affine Cipher.

Solution:
The Affine Cipher is defined by the 5-tuple (P, C, K, E, D) where:

- $P = C = \mathbb{Z}_{26}$ (plaintext and ciphertext spaces)
- $K = \{(a, b) \in \mathbb{Z}_{26} \times \mathbb{Z}_{26} \mid \gcd(a, 26) = 1\}$ (key space)
- For key $k = (a, b) \in K$:
  - Encryption: $E_k(x) = (ax + b) \bmod 26$
  - Decryption: $D_k(y) = a^{-1}(y - b) \bmod 26$

where a^{-1} is the multiplicative inverse of a modulo 26.