COMP6453: Week 2 Answers

1 Part 1

1.1

$(27 + 45) \mod 17 = 4$

1.2

$(2 \times 17 + 19) \mod 11 = 9$

1.3

$2^{10} \mod 7 = 2$

1.4

$A = \{0, 6, 17, 20, 26\}$ and $B = \{5, 6, 17, 19, 35\}$

|A| = 5 |B| = 5

Union: $A \cup B = \{0, 6, 17, 20, 26, 5, 19, 35\}$

Intersection: $A \cap B = \{6, 17\}$

2 Part 2

2.1 Question 5

Consider cipher M = D G H L T E W Q.

Assume letter A map to 0, B map to 1,.. and so on.

A -> 0 B -> 1 .. Z-> 25

Shifting key K = 5 that means we want to shift D = 3 + K (=5) = 8 which map to I

Answer: Text : DGHLTEWQ

Shift : 5

Cipher: ILMQYJBV

2.2 Question 6

Suppose that $K = (5, 21)$ is a key in an Affine Cipher - substitution cipher over $\mathbb{Z}_{29}$.

(a) Express the decryption function $d_K(y)$ in the form $d_K(y) = a_0 y + b_0$, where $a_0, b_0 \in \mathbb{Z}_{29}$.

Answer: We have encryption function $E_K(x) = (a_0 x + b_0) \bmod p$, $K = (5, 21)$ and $p = 29$

$E_K(x) = (5x + 21) \bmod 29$

We have the decryption function is:

$D_K(y) = a_0^{-1}(y - b_o) \bmod 29$

a_0^{-1} is the modular multiplicative inverse of a_0 modulo p. ie. satisfy equation:

$1 = a_0^{-1} a_0 \bmod p$

Note that the multiplicative inverse of a only exists if a and m are coprime.

We now want to first find the modular multiplicative inverse of $a_0 = 5$, which is a_0^{-1}. In this case, it is 6 because $5 * 6 = 30 \bmod 29 = 1$

Thus, we now have:

$D_K(y) = 6(y - 21) \bmod 29$

$<=>$ $D_K(y) = 6y - 126 \bmod 29$

$<=>$$D_K(y) = 6y + 19 \bmod 29$

(b) Prove that $d_K(e_K(x)) = x$ for $\forall x \in \mathbb{Z}_{29}$.

Answer: $d_K(e_K(x)) = a_0^{-1}(E_K(x) - b) \bmod 29$

$= a_0^{-1}(((ax + b) \bmod 29)\ -b) \bmod 29$

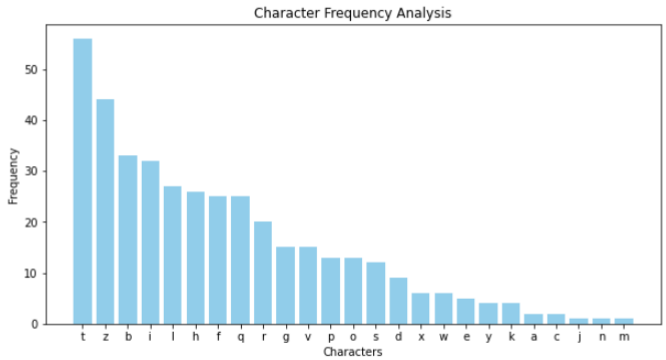
$= a_0^{-1}(ax + b - b) \bmod 29$

$= a_0^{-1}\ ax \bmod 29$

$= x \bmod 29$

$= x$

2.3 Question 7




```
Ciphertext:  ZRTFT IH PQFTHZ IQ ZRT XBGBOZIO HTQBZT. HTWTFBG ZRLPHBQV HLGBF HYHZTSH RBWT VTOGBFTV ZRTIF IQZTQZILQH ZL GTBWT ZRT
FTEPKGIO. ZRIH HTEBFBZIHZ SLWTSTQZ, PQVTF ZRT GTBVTFHRIE LD ZRT SYHZTFILPH OLPQZ VLLAP, RBH SBVT IZ VIDDIOPGZ DLF ZRT GISIZTV Q
PSKTF LD CTVI AQIXRZH ZL SBIQZBIQ ETBOT BQV LFVTF IQ ZRT XBGBJY. HTQBZLF BSIVBGB, ZRT DLFSTF NPTTQ LD QBKLL, IH FTZPFQIQX ZL ZR
T XBGBOZIO HTQBZT ZL WLZT LQ ZRT OFIZIOBG IHHPT LD OFTBZIQX BQ BFSY LD ZRT FTEPKGIO ZL BHHIHZ ZRT LWTFMRTGSTV CTVI


 Substitution Dictionary:
t -> e
z -> t
b -> a
i -> o
l -> i
h -> n
f -> s
```

2.4 Question 8

Consider a cipher which has message space, ciphertext space, and keyspace all equal to Z_p, where p is a prime. Let encryption be given by $E(k, m) = k \cdot m \pmod p$ and $D(k, c) = k^{-1} \cdot c \pmod p$. Show this cipher has perfect secrecy. What goes wrong if p is not a prime?

Answer: Given a ciphertext c and a message $m \in \mathbb{Z}_p$, the probability m encrypts to c is precisely the number of keys such that $E(k, m) = c$ divided by the total number of keys. The number of such keys is 1, so this probability is always $1/p$.

When p is not a prime, then not all keys will have a multiplicative inverse (i.e k^{-1} does not always exist). So we must restrict the keyspace to keys k which do have a multiplicative inverse. But then the size of the keyspace is smaller than the size of the message space, so we cannot have perfect security.