COMP6453 Week 2 Tutorial

1 Part 1: Basic Maths

Compute the following:

1. $(27 + 45) \mod 17 = ?$
2. $(2 \times 17 + 19) \mod 11 = ?$
3. $2^{10} \mod 7 = ?$
4. If $A = \{0, 6, 17, 20, 26\}$ and $B = \{5, 6, 17, 19, 35\}$, calculate,
   (a) Cardinality of the sets, denoted $|A|$ and $|B|$?
   (b) $A \bigcup B$
   (c) $A \cap B$.

2 Part 2: Ciphers

5. Consider the following Plaintext. $M = DGHLTEWQ$. What is the ciphertext when the shift key is 5?
6. Suppose that $K = (5, 21)$ is a key in an Affine Cipher over Z_{29}.
   (a) Express the decryption function $d_K(y)$ in the form $d_K(y) = a_0 y + b_0$, where $a_0, b_0 \in Z_{29}$.
   (b) Prove that $d_K(e_K(x)) = x$ for $\forall x \in Z_{29}$.
7. 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?

8. Use frequency analysis to decrypt the following text.
   ZRTFT IH PQFTHZ IQ ZRT XBGBOZIO HTQBZT. HTWTFBG ZRLPH-
   BQV 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 QPSKTF LD CTVI AQIXRZH ZL SBIQZBIQ ETBOT BQV LFVTF IQ ZRT XBGBJY. HTQBZLF BSIVBGB, ZRT DLFSTF NPTTQ LD QBKLL, IH FTZPFQIQX ZL ZRT XBGBOZIO HTQBZT ZL WLZT LQ ZRT OFIZIOBG IHHPT LD OFTBZIQX BQ BFSY LD ZRT FTEPKGIO ZL BHHIHZ ZRT LWTFM-RTGSTV CTVI