COMP6453 Week 1-2 Practice Exercises

1 Maths

1. (a) $(7503) \mod 81$
   (b) $(-7503) \mod 81$
   (c) $(2^19) \mod 81$
2. $\forall a \in Z_{19}^*$, find a^{-1}. $Z_n^* = \{1, 2, \cdots, n-1\}$.

2 Classical Ciphers

1. Use exhaustive key search to decrypt the following ciphertext, which was encrypted using a Shift Cipher:
   BEEAKFYDJXUQYHYJIQRYHTYJIQFBQDUYJIIKFUHCQD
2. Below are given 2 examples of ciphertext, obtained from Substitution and Affine ciphers. Provide the plaintext and explain how you obtained the solution.

   (a) Substitution Cipher.

   Ptxt: Ctxt: EMGLOSUDCGDNCUSWYSFHNSFCYKDPUMLWGYICOXYSIPJCK QPKUGKMGOLICGINCGACKSNISACYKZSCKXECJCKSHYSXCG OIDP-KZCNKSHICGIWYGKKGKGOLDSILKGOIUSIGLEDSPWZU GFZCC-NDGYYSFUSZCNXEOJNCGYEOWEUPXEZGACGNFGLKNS ACIGOIY-CKXCJUCIUZCFZCCNDGYYSFEUEKUZCSOCFZCCNC IACZEJNC-SHFZEJZEGMXCYHCJUMGKUCY

   (b) Affine Cipher: Ctxt: KQEREJEBCPPCJCRKIEACUZBKRVPKRB-CIBQCARBJCVFCUP KRIOFKPACUZQEPBKRXPEIIEABDKPBCPFCD-CCAFIEABDKP BCPFEQPKAZBKRHAIBKAPCCIBURCCDKDCCJ-CIDFUIXPAFF ERBICZDFKABICBBENEFCUPJCVKABPCYDCCDP-KBCOCPERK IVKSCPICBRKIJPKABI

3 Perfect Secrecy

1. Let $E = (E; D)$ be a Shannon cipher defined over $(\mathcal{K}; \mathcal{M}; \mathcal{C})$. If E is perfectly secure, then prove that $\mathcal{K} \geq \mathcal{M}$.