

EE4215 Cybersecurity Technology

Assignment 2 (Solution)

- a) The guessed value of $m[0]$ is 45 (hexadecimal) with its frequency of occurrence equal to 46.
- b) The network-layer protocol is IPv4. In the header of IPv4, the first byte consists of two fields. The first field is the version number, which is equal to 4. The second field is the header length, which is usually equal to 5 (i.e., 5×32 bits = 160 bits or 20 bytes). Hence, the first byte is 45 (hexadecimal), which agrees with the answer in (a).
- c) The guessed value of $k[0]$ is 1a (hexadecimal) with its frequency of occurrence equal to 20.
- d) The 13-byte long-term key is 1a2bccd4ef054d10a08c7e1a0b.