COMP6453 Assignment I: Q4

Joules Patman

July 9, 2025

Q4)

a) The maximum number of calls to the SHA-1 function is if we take the first 40 bits (5 bytes) and try to find a collsion for $H(m_1) = H(m_k)$. This is the worst case scenario and 2^{40} calls will be required

b) But By using the birthday attack we can use the fact that the actual bits of security will be $2^{n/2}$ where is the number of bits, until we find a collision with probability of 50%. Thus we will need to compare 2^{20} bits instead.

c) Pseudocode:

Algorithm 1 Find Colliding Hash

```
Define function:
    Define HashTable {hash table stores (hash, message) pairs}
    $(m_1, h_1) \leftarrow$ get40BitsFromSha1()
    didFindHash $\leftarrow$ HashTable.get($h_1$)
if didFindHash $\neq$ null then
        HashTable.add($h_1$)
else if $m_1 ==$ val then
        skip
else
        $m_2 \leftarrow$ didFindHash
end if
return $(h_1, m_1, m_2)$
```