Alan Palayil

A20447935

Homework #3

ECE 543

Due Date: 2/26/23

2) No, this is not a good message digest function. Combining message chunks in this way doesn't provide adequate diffusion and makes it susceptible to collision attacks. A good message digest function should provide a high degree of entropy and be designed to resist preimage, second preimage, and collision attacks.

3) According to 5.1, Bob creates 2^{32} messages for each type, and matches the two lists. The likelihood of a Type 2 message sharing the same message digest as one of the 2^{32} Type 1 messages is approximately $2^{32}/2^{64} \approx 1/2^{32}$. As a result, it is probable that one of the 2^{32} Type 2 messages will match one of the 2^{32} Type 1 messages.

12) No, we would not theoretically have to test fewer 2000-bit messages than 1000-bit messages to find one that has a message digest of d. The probability of finding a collision should be proportional to the square of the no. of possible message inputs, so the fact that there are more 2000-bit messages that map to a particular 128-bit message digest than 1000-bit messages doesn't necessarily make it easier to find a message that has a message digest of d.

16) MD2 appends a message checksum to the entire padded message before computing the hash. Therefore, if you want to compute $MD2(K_{AB} | m | n)$ incrementally, starting with $MD2(K_{AB} | m)$, you need to include the padding and message checksum for $K_{AB} | m$ in n. However, since we don't know K_{AB}, we can't compute the message checksum.

19) Given K_{AB}, IV, and ciphertexts (c_is), it is possible to compute the corresponding message digests (b_is). Using the formula: $p_i = c_i \oplus b_i$, it is then possible to recover the plaintext (p_i).