The University of Newcastle
School of Electrical Engineering and Computer Science

COMP3260 Data Security

GAME 10

23th May 2019

Number of Questions: 5
Time allowed: 50min
Total mark: 5

	Student Number	***Student Name***
Student 1		
Student 2		
Student 3		
Student 4		
Student 5		
Student 6		
Student 7		

Question 1	***Question 2***	***Question 3***	***Question 4***	***Question 5***	***TOTAL***

1. With the aid of diagrams explain in what ways a hash value can be secured so as to provide message authentication.

2. What types of attacks are addressed by message authentication?

3. What protection does a digital signature provide which is not provided by message authentication? (i.e. What is the difference between a digital signature system and a message authentication system)

4. Is it possible to use a hash function to construct a Feistel cipher? If yes, explain how it is possible considering that a hash function is not reversible and a Feistel cipher must be reversible.

5. The following is a version of the Neuman-Stubblebine protocol for key exchange proposed in 1993 that employs a trusted third party and symmetric encryption.

A, B, T	Alice, Bob and the trusted third party (TTP), respectively
N_A, N_B	Nonce created by Alice and Bob, respectively
T_B	Timestamp create by Bob
K_{AT}, K_{BT}, K_{AB}	Key shared by Alice and TTP, Bob and TTP, and Alice and Bob, respectively

1. $A \rightarrow B$ **:** A, N_A
2. $B \rightarrow T$ **:** $B, \{A,N_A,T_B\}_{K\boldsymbol{BT}},N_B$
3. $T \rightarrow A$ **:** $\{B, N_A, K_{AB}, T_B\}_{KAT}, \{A, K_{AB}, T_B\}_{KBT}, N_B$
4. $A \rightarrow B$ **:** $\{A, K_{AB}, T_B\}_{KBT}, \{N_B\}_{KAB}$

Show how an intruder can subvert the protocol if the following two conditions are satisfied:

- the keys and the nonces have the same number of bits, and
- the intruder can eavesdrop on messages 1 and 2, intercept message 4, and send his own message 4 to Bob, pretending it is from Alice.