The University of Newcastle
School of Electrical Engineering and Computer Science

COMP3260 Data Security

GAME 10 Solutions

16th May 2017

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

Calculators not allowed.

	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.

Solution: Figures bellow illustrate a variety of ways in which a hash code can be used to provide message authentication, as follows.

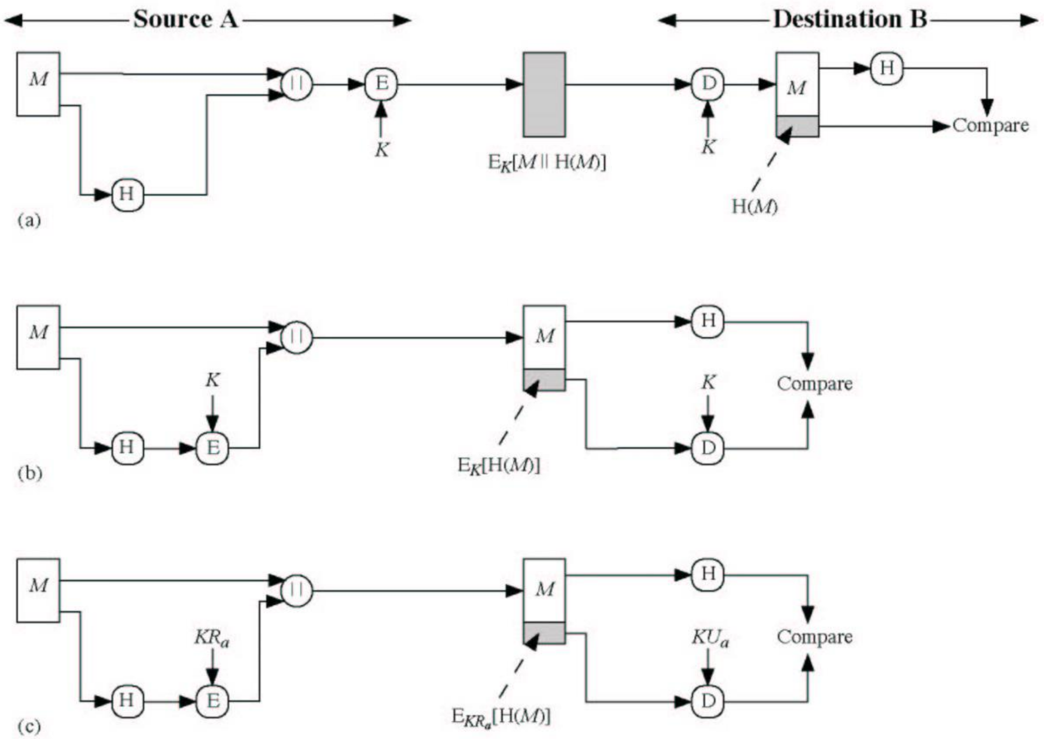


Figure 11.5 Basic Uses of Hash Function (page 1 of 2)

a. The message plus concatenated hash code is encrypted using symmetric encryption.

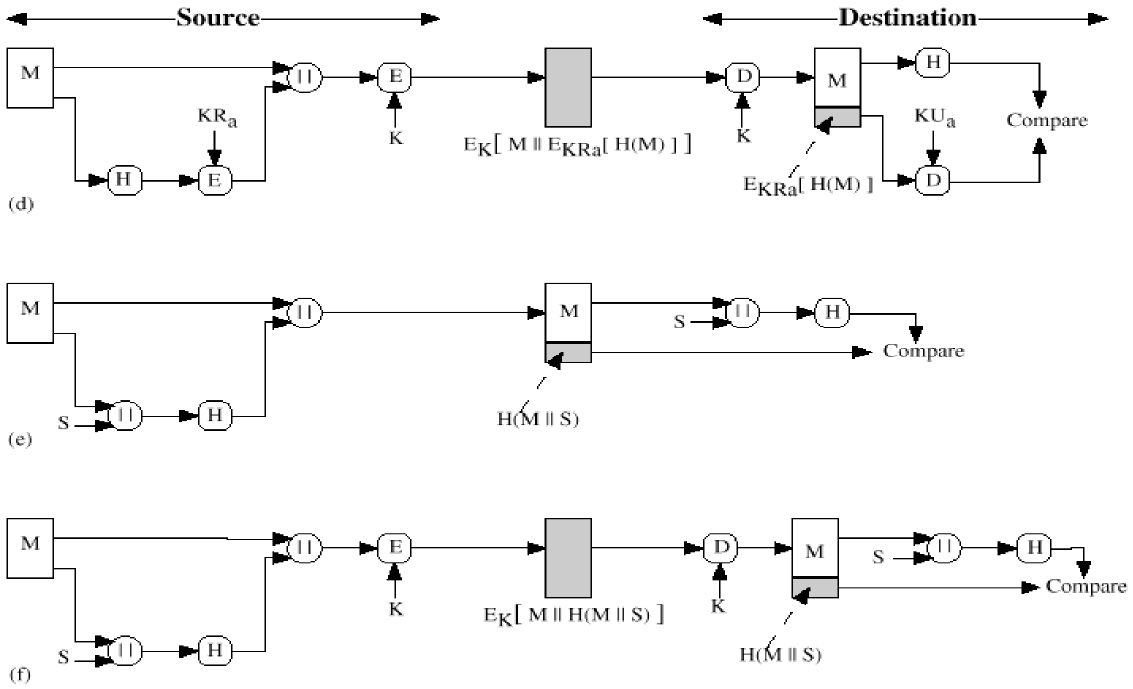
b. Only the hash code is encrypted, using symmetric encryption.

c. Only the hash code is encrypted, using public-key encryption and using the sender's private key.

d. If confidentiality as well as a digital signature is desired, then the message plus the public-key-encrypted hash code can be encrypted using a symmetric secret key.

e. This technique uses a hash function but no encryption for message authentication. The technique assumes that the two communicating parties share a common secret value S. A computes the hash value over the concatenation of M and S and appends the resulting hash value to M. Because B possesses S, it can recompute the hash value to verify.

f. Confidentiality can be added to the approach of (e) by encrypting the entire message plus the hash code.



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

Solution:
Masquerade: Insertion of messages into the network from a fraudulent source. This includes the creation of messages by an opponent that are purported to come from an authorized entity. Also included are fraudulent acknowledgments of message receipt or nonreceipt by someone other than the message recipient.

Content modification: Changes to the contents of a message, including insertion, deletion, transposition, and modification.

Sequence modification: Any modification to a sequence of messages between parties, including insertion, deletion, and reordering.

Timing modification: Delay or replay of messages. In a connection-oriented application, an entire session or sequence of messages could be a replay of some previous valid session, or individual messages in the sequence could be delayed or replayed. In a connectionless application, an individual message (e.g., datagram) could be delayed or replayed.

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)

Solution:
Message authentication is designed to protect two parties exchanging messages from a third party interfering with their communications (Content modification, sequence modification, timing modification). Message authentication is not designed to protect two parties from each other. Digital signatures protect two communicating parties from each other where there is

not perfect trust. A digital signature is designed to prevent message forgery and denial of sending a message.

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.

Solution:
A hash function can be used as the round function F in a Feistel cipher. There is no requirement that the round function in a Feistel cipher be reversable, as the data always flows through it in the same direction, both in the encrypt and decrypt processes. What changes is the order in which the keys are applied.

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. $B \rightarrow T$: $B, \{A, N_A, T_B\}_{\mathbf{KBT}}, N_B$
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.

Solution
A Paradox attack as described in this paper: *https://doi.org/10.1016/0020-0190(95)00177-E*

An eavesdropper can send $\{A, N_A, T_B\}_{\mathbf{KBT}}$ in place of $\{A, K_{AB}, T_B\}_{KBT}$ at step 4, replacing the session key with A's Nonce. B is not able to distinguish between these two, as they have the same number of bits, and there is nothing in the protocol disallowing the session key from being identical to the Nonce.

In notation, a wiretapper W could subvert the scheme as follows:

1. $A \rightarrow B$: A, N_A
2. $B \rightarrow T$: $B, \{A, N_A, T_B\}_{\mathbf{KBT}}, N_B$
3. $T \rightarrow A$: (ignore)
4. $W \rightarrow B$: $\{A, N_A, T_B\}_{KBT}, \{N_B\}_{KAB}$

At this point, W has successfully replaced the session key with a value he knows. W can also make use of this attack even where A does not initiate the communications, by generating a fake N_A.