Lecture NS5 2018

Chapter 11

1. Describe how the hash function can be used to provide **message authentication**

Answer: fig. 11.3, pp. 343—344

2. Describe how the hash function can be used to create **digital signature**

Answer: fig. 11.4, pp. 344—345

3. Briefly describe the five steps of the Message digest generation in SHA-512

Answer: fig. 11.9, pp. 357—359

Chapter 12

4. Describe four approaches to provide both confidentiality and encryption for a message M .
5. Given figure 12.1d explain what it describes.

Answer: Figure 12.1 pp. 384 – 388

6. Describe the HMAC algorithm

Answer: Figure 12.5 pp. 395 – 397

7. Describe working of the Galois Counter Message authentication code (GCM)

Answer: fig. 12.11, pp. 407—408

Chapter 13

8. Describe the **Elgamal digital signature** scheme.

Answer: sec. 13.2, pp. 424-425

9. Alice wants to send a message to Bob using **Elgamal digital signature**.

   Suppose q = 19, a = 10, K = 5, X_A= 16 and hash value m = 14.

   Please gives the detailed steps during interaction.

Answer: p.425