2 hours

UNIVERSITY OF MANCHESTER

CYBER SECURITY

19 May 2023

14:00-16:00

Answer 3 of 3 questions

Electronic calculators are **not** permitted

The use of books or course notes is **not** permitted

Question 1

Message encryption functions and cryptographic hash functions are among the most commonly used cryptographic functions. Message encryption functions can be further classified into symmetric-key based and asymmetric-key based.

(a) Contrast these different types of cryptographic functions, i.e. *hash functions*, *symmetric-key based message encryption functions* and *asymmetric-key based message encryption functions*, in terms of their respective properties, advantages (or merits) and disadvantages (or limitations).

[6 marks]

(b) For each type of the functions named in (a), name one application they are commonly used for. In your answer, you should also make clear the security property they each provide in the named application.

[6 marks]

(c) Explain what an authenticator is. For each type of the functions named in (a), explain whether, and if yes, how, the function can be used to construct an authenticator. Also make clear if any of the authenticators you have constructed can be used to protect against false denial of the origin of a message. Justify your answer.

[8 marks]

[Please Turn Over]

Question 2

Key management is an important part of a cyber security solution.

(a) Give two reasons why key management is important, and name two factors which impact on the strength of a secret key.

[4 marks]

(b) Name *five* functions a key management system should comprise. For each of the functions named, highlight any considerations that should be considered to ensure the security of the keys being managed.

[5 marks]

(c) With the use of a diagram, describe a protocol that allows *Alice* and *Bob* to securely establish a shared secret over the Internet without any assistance of a public-key cipher. It is assumed that *Alice* and *Bob* have never met before, and that they are both registered with a trusted third party.

[4 marks]

(d) Repeat (c) but with the assistance of a public-key cipher.

[4 marks]

(e) Contrast the two protocols designed in (c) and (d).

[3 marks]

[Please Turn Over]

Question 3

IPSec is a network layer (the Internet Protocol layer or IP layer) security package, whereas Pretty Good Privacy (PGP) is an application layer (email) security package.

(a) Explain what a Security Association (SA) is and why it is needed in IPSec. With the help of a diagram, show how an SA is established between two entities.

[5 marks]

(b) Describe the purposes of the Tunnel and Transport modes of IPSec, and use diagrams to illustrate the IPv4 packet format used by the ESP (Encapsulating Security Payload) protocol in each of the Tunnel and Transport modes. In your diagrams, you should clearly indicate the scope of security protections provided by the ESP protocol.

[7 marks]

(c) Contrast the data (traffic) security services provided by the two security packages (i.e. the IPSec and PGP), making clear their similarities and/or differences.

[5 marks]

(d) Which of these two security packages, IPSec or PGP, is more resilient to DoS (Denial of Service) attacks? Justify your answer.

[3 marks]

END OF EXAMINATION