Chapter 11: Hints & Answers

11.1 (a) There is not enough information in the ciphertext CBA to determine frequencies of the encrypted symbols.

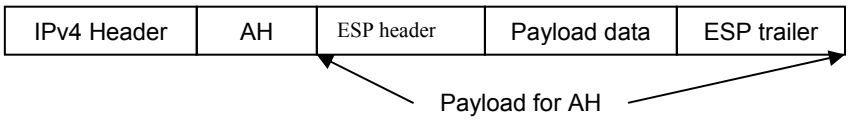
11.4 If the system authenticates users based on IDs and passwords that are transmitted in plaintext, the system is very insecure. An eavesdropper can listen and record the authentication information over the network. This information can be replayed by the intruder when attempting to access the system. If the password and ID are encrypted, the system no more secure than in the plaintext case. The intruder can still record the encrypted ID and the corresponding encrypted password. By replaying these, the intruder can gain access to the system. To be secure the encrypted password should be used only once so that it is not susceptible to the playback attack. The method were the user identifies itself followed by a nonce challenge from the server uses this approach.

11.8 (a) $n = 22$ for $P = 0.476$ and $n = 23$ for $P = 0.507$
(c) To calculate this probability we need Sterling's approximation for *N!* for large *N*:
$$N! \approx e^{-N} N^N \sqrt{2\pi N}$$

11.12 $K = 28$

11.16 The authentication header cannot cover those fields that are changed along the route of the packet, such as the header checksum, Time-to-live and fragment offset – assuming the packet didn't set the DF (don't fragment) flag. Tunnel mode or a node-to-node security association for encryption of these fields can be used to transfer the packets from one router to the next one all across the path.

11.20 (c) Transport mode: AH applied after ESP.



This mode is used when privacy of the data and authentication and integrity are needed.

11.25 It is appropriate for TLS to authenticate the client when the server is sending confidential information to the client and wants to ascertain the receiver's identity, for example, a banking statement sent to a customer (client) over the network. Telebanking and credit card purchases over the internet are other examples where authentication is required.

11.28 (c) $d = 53$ for part (b).