Answer Key for 3rd Quiz.

Q1

(A) MIME content Transfer Encoding indicates the type of transformation that has been used to represent the body of the message in a way that is acceptable for mail transport.

In other words: Transfer encoding enables the conversion of any content format into a form that is protected from alteration by the email system in transport.

(B) Reason: Use of session key requires to perform session-key distribution first. So it is an overhead and not a trivial task. Instead, the system uses one-time content encryption key to encrypt a message, and this one-time key is encrypted using the public key of the receiver. So, a combination of symmetric and public-key encryption solves the requirement of session-key distribution problem.

How?

(1) Sender generates a message and a random 128-bit number to be used as a content-encryption key for this message only.

(2) Message is encrypted using the content encryption key.

(3) The content-encryption key is encrypted with RSA using the recipient's public key, and is attached with the message

(4) Encrypted message + Encrypted key are sent to receiver

(5) The receiver uses RSA with its private key to decrypt and recover the content-encryption key.

(6) The content-encryption key is used to decrypt the message.

Answer Key Quiz 3

Q2.

(A) Use of application level gateway: It relays and monitors the exchange of information for application level traffic. For example, checking SMTP e-mail for spam, HTTP web requests to allowed sites only, etc. In addition, it is easy to log and audit all incoming traffic at the application level.

(B) Suitable IDS for

(i) Masqueraders: → statistical anomaly detection as it is unlikely that masqueraders mimic the behavior patterns of the accounts they appropriate.

(ii) Misfeasors: → Rule-based approaches are suitable as it can be able to recognize events and sequences that, in context, reveal penetration.