The following correction applies to page 476 of the *CISA Review Questions, Answers & Explanations Manual 11th Edition*.
Question A5-261 Choice D has been corrected. The correction is circled.

A5-259 Neural networks are effective in detecting fraud because they can:

A. discover new trends because they are inherently linear.
B solve problems where large and general sets of training data are not obtainable.
C attack problems that require consideration of a large number of input variables.
D. make assumptions about the shape of any curve relating variables to the output.

C is the correct answer.

Justification:
A. Neural networks are inherently nonlinear.
B. Neural networks will not work well at solving problems for which sufficiently large and general sets of training data are not obtainable.
C. Neural networks can be used to attack problems that require consideration of numerous input variables. They are capable of capturing relationships and patterns often missed by other statistical methods, but they will not discover new trends.
D. Neural networks make no assumption about the shape of any curve relating variables to the output.

A5-260 Which of the following **BEST** encrypts data on mobile devices?

A. Elliptical curve cryptography (ECC)
B. Data encryption standard (DES)
C. Advanced encryption standard (AES)
D. The Blowfish algorithm

A is the correct answer.

Justification:
A. Elliptical curve cryptography (ECC) requires limited bandwidth resources and is suitable for encrypting mobile devices.
B. Data encryption standard (DES) uses less processing power when compared with advanced encryption standard (AES), but ECC is more suitable for encrypting data on mobile devices.
C. AES is a symmetric algorithm and has the problem of key management and distribution. ECC is an asymmetric algorithm and is better suited for a mobile environment.
D. The use of the Blowfish algorithm consumes too much processing power.

A5-261 Which of the following can be used to help ensure confidentiality of transmitted data? Encrypting the:

A. message digest with the sender's private key.
B. session key with the sender's public key.
C. message with the receiver's private key.
D. session key with the receiver's public key.

D is the correct answer.

Justification:
A. This will ensure authentication and nonrepudiation.
B. This will make the message accessible to only the sender.
C. Ideally, a sender cannot have access to a receiver's private key.
D. Access to the session key can only be obtained using the receiver's public key.