Module 3: Multiple-choice questions

1. Among the benefits from industrial cyber systems are all of the following, except for:
   a) Efficient and scalable production
   b) Optimized performance and improved flexibility and speed
   c) Improved machine intelligence
   d) All of the answers represent benefits from industrial cyber systems

2. Among the smart agriculture applications are all of the following except for:
   a) Farm vehicles
   b) Improved work ethics
   c) Irrigation systems
   d) Livestock operation

3. All of the following are true, except for:
   a) SCADA stands for “Site Control And Data Acquisition”
   b) DCS stands for “Directed Contribution Systems”
   c) SCADA and DCS started as separate systems but have grown together
   d) All of the answers are true

4. Which of the following is not element of SCADA:
   a) Communication
   b) Master Terminal Units
   c) Micro Terminal Units (MTU)
   d) RTUs/PLCs

5. All of the following are true, except for:
   a) RTU means Remote Terminal Unit
   b) RTU means Remote Telemetry Units
   c) RTUs are electronic devices with intelligent microprocessor
   d) All of the above are true

6. All of the following are true, except for:
   a) PLC stands for Programmable Logic Controller
   b) PLC stands for Programmable Logistic Controller
   c) PLC controls manufacturing process
   d) PLC is an industrial digital computer that replaced traditional relays

7. All of the following are true for a SCADA server, except for:
   a) SCADA server provides data logging
   b) SCADA server analyzes data
   c) SCADA server is a real-time decision maker
   d) SCADA server is ensuring proper communication between two devices

8. Among the security vulnerabilities in engineering systems are all of the following, except for:
   a) Remote devices are hard to upgrade
   b) There are few firewall options
   c) All traffic is on just one port
   d) All of the above are examples of vulnerabilities in engineering systems

9. Among the advanced authentication methods in engineering systems are:
   a) Digital certificates
   b) Biometrics
c) All of the above  
d) None of the above  
10. All of the following are types of ransomware except for:  
   a) Custom ransomware  
   b) Targeted ransomware  
   c) Zero-day ransomware  
   d) Common ransomware  
11. All of the following are techniques for data protection in engineering systems, except for:  
   a) Cryptology  
   b) Cryptanalysis  
   c) Crypto-mapping  
   d) Cryptography  
12. Possible attacks for engineering systems include:  
   a) Ciphertext but not known plaintext  
   b) Known plaintext but not chosen plaintext or chosen ciphertext  
   c) Chosen plaintext but not chosen ciphertext  
   d) None of the above are correct answers  
13. Which of the following is not true:  
   a) Within symmetric key cryptography, there are two types of ciphers: stream ciphers and block ciphers  
   b) Within asymmetric key cryptography, there are two types of ciphers: stream ciphers and block ciphers  
   c) In the stream ciphers the data are fed into the algorithm in small pieces (bits or characters), and the output is produced in corresponding small pieces  
   d) In the Block ciphers, a block of input bits is collected and fed into the algorithm all at once and the output is a block of bits.  
14. All of the following about public key communication are true, except for:  
   a) They are very powerful, and it might seem that they make the use of symmetric key cryptography obsolete  
   b) A downside of public key communication is that the added flexibility is not free and comes at a computational cost  
   c) Public key methods are good for encrypting large quantities of data  
   d) Public key methods should not be used for encrypting large quantities of data  
15. All of the following are cryptographic applications, except for:  
   a) Data integrity  
   b) Confidentiality  
   c) Authentication  
   d) All of the above are cryptographic applications  
16. All of the following are security design principles, except for:  
   a) Least privilege principle  
   b) Fail-safe default  
   c) Maximization of secrets  
   d) Complete mediation