Module 3: True-or-false questions

1. T/F The term Industry 4.0 marks a rapid transformation of industry and that the virtual worlds of information technology, the physical world of machines, and the Internet have become one.
2. T/F The term Industry 2.0 marks a rapid transformation of industry and that the virtual worlds of information technology, the physical world of machines, and the Internet have become one.
3. T/F Among the smart energy applications are pipelines, exploration, distribution, renewable energy.
4. T/F Among the smart agriculture applications are irrigation systems and farm vehicles but not livestock operation.
5. T/F SCADA and DCS started as separate systems but have grown together.
6. T/F SCADA and DCS started as one system but have grown apart and are now separate.
7. T/F The terms DCS contains only the function of control while SCADA includes also data acquisition.
8. T/F The terms DCS contains only the function of control while SCADA includes data acquisition but not the control function.
9. T/F Elements of SCADA are RTUs/PLCs, sensors and actuators, communication, and Master Terminal Units (MTU).
10. T/F Elements of SCADA are RTUs/PLCs, sensors and actuators, communication, and Micro Terminal Units (MTU).
11. T/F RTU can mean “Remote Terminal Unit” or “Remote Telemetry Units”.
12. T/F RTU means “Remote Terminal Unit” but not “Remote Telemetry Units”.
13. T/F PLC means Programmable Logic Controller.
14. T/F PLC means Programmable Logistic Controller.
15. T/F PLC is an industrial digital computer that replaced traditional relays.
16. T/F The SCADA server provides data logging, data analysis and is a real-time decision-maker.
17. T/F IoT devices are not among the cyber vulnerabilities of engineering systems.
18. T/F One of the vulnerabilities of engineering systems is that each device is a potential entry point for a cyber attack.
19. T/F Among the security vulnerabilities in engineering systems are weak physical protection, the fact that there are a few firewall options, and that remote devices are hard to upgrade.
20. T/F The fact that all traffic is on just one port is not among the security vulnerabilities in engineering systems.
21. T/F Advanced authentication methods in cyber engineering systems include simple static passwords, digital certificates, and biometrics.
22. T/F Advanced authentication methods in cyber engineering systems include simple static passwords, digital certificates, but not biometrics.
23. T/F Three types of ransomware in cyber engineering systems are common ransomware, targeted ransomware and zero-day ransomware.
24. T/F Three types of ransomware in cyber engineering systems are common ransomware, custom ransomware and zero-day ransomware.
25. T/F Network security in engineering cyber system is challenging due to a wider range of protocols, standards, and device capabilities.

26. T/F Techniques for data protection include cryptography, cryptanalysis, and cryptology.
27. T/F Techniques for data protection include cryptography, cryptanalysis, cryptomapping, and cryptology.
28. T/F Cryptography is the process of designing systems to do data protection.
29. T/F Cryptanalysis deals with breaking systems for information security.
30. T/F Cryptology is an all-inclusive term for the study of communication over non-secure channels, and related problems.
31. T/F Cryptography is an all-inclusive term for the study of communication over non-secure channels, and related problems.
32. T/F Possible attacks against cyber engineering systems can include ciphertext, known plaintext, chosen plaintext, chosen ciphertext.
33. T/F Possible attacks against cyber engineering systems can include ciphertext, known plaintext, chosen plaintext, chosen ciphertext.
34. T/F Kerckhoffs's principle states that in assessing the security of a cryptosystem, one should always assume the enemy knows the method being used.
35. T/F Kerckhoffs's principle states that the security of the system should be based on the key and not on the obscurity of the algorithm used.
36. T/F Kerckhoffs's principle states that the security of the system should be based on the algorithm used and not on the key.
37. T/F All of the classical (pre-1970) cryptosystems are symmetric, as are the more recent Data Encryption Standard (DES) and Advanced Encryption Standard (AES).
38. T/F All of the classical (pre-1970) cryptosystems are asymmetrical, as are the more recent Data Encryption Standard (DES) and Advanced Encryption Standard (AES).
39. T/F Within symmetric key cryptography, there are two types of ciphers: stream ciphers and block ciphers.
40. T/F Within symmetric key cryptography, there are two types of ciphers: stream ciphers, neutral ciphers, and block ciphers.
41. T/F Within asymmetrical key cryptography, there are two types of ciphers: stream ciphers and block ciphers.
42. T/F In 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.
43. T/F In stream ciphers, the data are fed into the algorithm in small pieces (bits or characters), and the output is produced in corresponding small pieces
44. T/F In stream ciphers, a block of input bits is collected and fed into the algorithm all at once, and the output is a block of bits.
45. T/F In block ciphers, the data are fed into the algorithm in small pieces (bits or characters), and the output is produced in corresponding small pieces.
46. T/F Public Key Communication is very powerful, and it might seem that it makes the use of symmetric key cryptography obsolete.
47. T/F Public key methods should not be used for encrypting large quantities of data.
48. T/F Public key methods is good for encrypting large quantities of data.
49. T/F Cryptographic applications include principles of confidentiality, data integrity, authentication and non-repudiation.
50. T/F Non-repudiation is particularly important in electronic commerce applications.