Homework 1

Q1: Consider an automated teller machine (ATM) in which users provide a personal identification number (PIN) and a card for account access. Give examples of confidentiality, integrity, and availability requirements associated with the system and, in each case, indicate the degree of importance of the requirement.

Q2: For each of the following assets, assign a low, moderate, or high impact level for the loss of confidentiality, availability, and integrity, respectively. Justify your answers.

a. An organization managing public information on its Web server.

b. A law enforcement organization managing extremely sensitive investigative information.

c. A financial organization managing routine administrative information (not privacy related information).

d. An information system used for large acquisitions in a contracting organization contains both sensitive, pre-solicitation phase contract information and routine administrative information. Assess the impact for the two data sets separately and the information system as a whole.

e. A power plant contains a SCADA (supervisory control and data acquisition) system controlling the distribution of electric power for a large military installation. The SCADA system contains both real-time sensor data and routine administrative information. Assess the impact for the two data sets separately and the information system as a whole.

Q3: Briefly define the Caesar cipher.

Q4: Briefly define the monoalphabetic cipher.

Q5: Briefly define the Playfair cipher.

Q6: What is the difference between a monoalphabetic cipher and a polyalphabetic

cipher?

Q7 What are two problems with the one-time pad?

Q8: What is a transposition cipher?

Q9: What is steganography?

Q10: Encrypt the following message using Playfair cipher?

Plaintext: “HE WENT TO THE STORE”

Key is "PROBLEMS"?