Answer Key

1.	**A, B**	11.	**D**	21.	**A**	31.	**D**
2.	**A**	12.	**D**	22.	**C**	32.	**A, C**
3.	**A, C**	13.	**A**	23.	**C**	33.	**B**
4.	**A**	14.	**A, B**	24.	**A**	34.	**D**
5.	**B**	15.	**C**	25.	**D**	35.	**B, C**
6.	**C**	16.	**A**	26.	**B**	36.	**B**
7.	**D**	17.	**D**	27.	**A**	37.	**C**
8.	**C**	18.	**B**	28.	**D**	38.	**A**
9.	**D**	19.	**A**	29.	**D**	39.	**B**
10.	**D**	20.	**A**	30.	**B**	40.	**D**

Answers Explained

1. **(A), (B)** GPS is used to determine location. GPS determines the position of the start and end for the path, allowing the computer to map a path from there. GPS also determines the position of the user and the nearby points of interest so they can be found and mapped, allowing the user to navigate to them more easily.

   (C) describes data about points of interest that do NOT include location.

   (D) is possible (by placing messages at specific geographic locations) but does not have a major effect on navigation.

2. **(A)** The pressure sensors in the pads are used to interact with certain aspects of the environment, such as moving parts or sound effects.

   (B) The interaction (e.g., sending a security guard to a store being robbed) is not triggered by a sensor.

   (C) and (D) The system is used only for organization and nonbinding communication, not as a stimulus for interaction.

3. **(A), (C)** Public key algorithms use two different keys for encryption and decryption. The two keys cannot be derived from each other. Public key encryption can transmit data securely without the need for sharing key data. Symmetric key encryption uses one key that is shared with both the sender and receiver. Symmetric key encryption is generally faster than asymmetric encryption.

4. **(A)** A Caesar cipher uses the same key to encrypt the data and to decrypt the data. The use of one key is symmetric key encryption.

   Choices II and III refer to the same encryption method. Public key or asymmetric key encryption uses two separate keys and does not require a secure channel for exchanging keys.

5. **(B)** If the private key is discovered, all messages can be decrypted.

   (A) The public key can be made public. With the public key, anybody can encrypt data. However, a separate private key is needed to decrypt the data.

   (C) Although open standards are used when encrypting data, they were designed to keep encrypted data secure. The open standards do not help in decrypting.

   (D) If encrypted data are intercepted before decryption, they do not take on a usable form.