**V. EXERCISES**

**Exercise 1. Make up questions based on the text.**

1. What is advantage of tokens?
2. What kind of security measures are there?
3. When is encryption use?
4. Who is authenticated user?
5. Why is key required for decryption/encryption?
6. Where can the token be used?
7. How is ciphertext transformed into a plain text?
8. How long is data encrypted?
9. How many data is encrypted every second in the world?
10. How important is data security?

**Exercise 3. Complete the definitions of the terms from the text by filling in the blanks. Note *the verbs* which are usually used to define something.**

1. decryption **is** the process of using an algorithm to transform ciphertext back to its original plain text format.
2. A database which stores the relationship between the sensitive value and the token **is known as** a token vault.
3. A value that is applied using an algorithm to a plain text to produce encrypted text **is known as** key.
4. The practices of protecting cryptographic keys from unauthorized access and use **are called** the cryptographic key.
5. The process of turning a meaningful piece of data into a random string of characters **is called** encryption.
6. A substitute for the real data which has no meaning is called a token value.
7. Encryption **refers to** the process of using an algorithm to transform plain text information into a non-readable form.
8. Data security **refers to** the process of protecting data from unauthorized access and data corruption throughout its lifecycle.

**Exercise 5. Fill in the blanks with vocabulary words in appropriate form.**

1. Real-time access to log data will allow you to filter and locate that one event that could be the cause of a **security breach**.
2. Company management is often not **awaring(?)** of some security **measures**.
3. On your website you can define the rule to allow only **authorize** **user** to access specific services.
4. In this company all data security measures are **retrieving** to changing passwords once a week.
5. Special software allows you to **log access** to sensitive data.
6. Is there a log file I can set up to **keeping track** of who accessed what files and what they did with them – i.e. deleted, changed and so on?
7. Financial-related personal data has higher **degree** **of sensitivity**.
8. Improper shutdowns of a computer may cause **data corruption**.