**h4 ETAOIN**

**x) Read and summarize**

The method and technique of keeping the messages secure is called cryptography. Along with confidentiality, it also offers non-repudiation, authentication, and integrity. Along with the algorithm, plaintext, ciphertext, and keys, a cryptosystem is also given. Algorithms used in cryptography, often known as ciphers, are mathematical operations that are used for encryption and decoding. It is a limited algorithm if the algorithm's security is kept a secret. A key is used for both encryption and decryption in modern cryptography methods. Cryptosystem is an algorithm system with all possible plain text, keys and ciphertexts.

There are actually two primary kinds of encryption. Steganography is the practice of hiding messages with other messages. Transposition encryption keys: Same plaintext, but characters are in a different order.

The security of algorithms depends on how difficult it is to break them; there are various types of breaking. Break total, subtract globally, deduct instances, subtract information. Data complexity, computational complexity, and storage needs can all be used to gauge how complicated an attack could be. Few common attack types are:

Ciphertext (only attack)

Known (plaintext attack)

Chosen (plain text attack)

Adaptive (chosen plaintext attack)

Chosen (ciphertext attack)

Chosen (key attack)

Rubber (hose cryptoanalysis)

**y) Find out frequency distribution of letters for a language that you know (other than English). What are the six most common letters?**

The Arabic alphabet consists of 28 primary letters. Arabic uses a system called Abjad, where each letter stands for a consonant (i.e., there are no vowel letters). While Arabic doesn't officially have vowel letters, it does have ways of making long and short vowel sounds.

The frequency distribution of letters for a Arabic language are given below.

ا------- 12.50%

ل------ 12.07%

م------ 6.52%

ن------ 6.61%

ه------ 5.08%

و------ 5.80%

ي------ 6.36%

Source: <https://en.wikipedia.org/wiki/Arabic_letter_frequency>

**z) Choose a password manager. Explain:**

Keeper Security **(** [**https://www.keepersecurity.com/**](https://www.keepersecurity.com/)**)**

**What threats does it protect against?**

Keeper security have zero-trust security framework, it can protect data from insider threats, external attacks, and other security risks. It provides users extra security in the case where master password or device is compromised. To do this it generates TOTPs (Time-based One-Time Passwords). It also protects Brute force attacks and Data breaches.

**What information is encrypted, what's not?**

Keeper security, encryption and decryption occurs only on the user's device upon logging into the vault. Each individual record stored in the user's vault is encrypted with a random 256-bit AES key that is generated on the user's device. The record keys are protected by an additional key, called the Data Key.

**What's the license?**

There are three licenses which are as per user need:

Basic for end user or home user

Business for SME and tailored business users

Enterprise for advanced capabilities with added protection

**Where is the data stored?**

Keeper utilizes Amazon AWS hardened cloud infrastructure in multiple geographic locations to host and operate the Keeper Vault. Data at rest and in transit is fully isolated in a customer's preferred global data center.

**How is the data protected?**

Private Master Password, Multi-Factor Authentication, Strongest Encryption, FIPS 140-2 Validated, Deep-Level Encryption, Secure/Reliable Cloud Vault

All contents of the data vault are encrypted, including logins, file attachments, TOTP codes, payment information, URLs and custom fields.

**b) Demonstrate the use of a password manager**

A password manager is an app that stores your passwords, so you don't need to remember them. Once you've logged into the password manager using a 'master' password, it will generate and remember your passwords for all your online accounts.

A password manager is similar to a top-secret digital key system that protects our keys, simplifies our lives online, and increases security. Creating a Master Password is the first and most important step. The password manager does not keep a copy of this. Then The password manager assists in generating a secure and unique key each time we create a new online account. The password manager safely stores these unique keys. Thus, in order to open the password manager anytime we need to log in to a certain account, we must supply the Master key.

Password managers are safe to use, and that's a fact that not only the vast majority of cyber-security specialists agree with, but we do as well. After all, a password manager uses advanced encryption to protect your credentials, while without it, your passwords might be accessible.