**How cryptography can be used to secure data in transit, data at use, data at rest**

**Cryptography**

The study of secure communication methods, such as encryption, that are only accessible to the message's sender and intended recipient is known as cryptography. The word is derived from the hidden word Kryptos in Greek.

Explanation

Digital data is now protected by encryption. The goal of this branch of computer science is to convert data into forms that are inaccessible to unauthorised users. An encrypted message that has had the letters changed with other characters serves as an example of basic cryptography.

Step 2 of 5

**Data-in-transit**

Any data transmitted from one system to another is considered to be in transit. This covers both communications within your workload between the resources and communication between other services and your end users.

All information shared or transferred over any network, including the internet, is considered to be in transit or in motion. Data provided to business partners, data uploaded to cloud apps, and files exchanged with coworkers are a few examples.

Step 3 of 5

**Data at rest**

Data that has reached its destination but is not being accessed or used is said to be in a state of rest. Data that is currently traveling across a network or waiting to be read or updated temporarily in computer memory aren't normally included in the term because they aren't typically saved.

Data that is at rest is, as the term suggests, not actively moving. Data that has been archived to a storage device or kept on a hard drive. For instance, files kept on your laptop and emails stored in email clients like Outlook are both examples of data at rest.

Step 4 of 5

**Data in use**

Data that is currently being updated, processed, deleted, accessed, or read by a system is referred to as data that is in use. This kind of data is actively travelling across various components of an IT infrastructure rather than being passively stored.

Data that is currently being updated, processed, accessed, and read by a system is known as data that is in use. This is the condition at which data is most susceptible to assaults and when encryption is most necessary since data in use is immediately accessible by one or more users.

Step 5 of 5

**Securing data using cryptography**

Enterprises are vulnerable to attack when there is unprotected data, whether it is in transit or at rest. However, there are effective security techniques that provide strong data protection across endpoints and networks to safeguard data in both stages. Data encryption is one of the best ways to safeguard data, both when it's in use and when it's at rest.

Put in place strong network security measures to secure data while it is being transmitted. Networks used to transfer data will be more secure against malware assaults and intrusions with the help of network security solutions like firewalls and network access control.

Don't depend on reactive security to safeguard your important corporate data. Use preventative security measures that recognize data that is in danger and put in place strong data protection for data both in transit and at rest.

To order to secure sensitive data while it is in transit, such as when files are attached to emails, moved to cloud storage, portable devices, or transferred elsewhere, choose data protection solutions with rules that provide user prompting, blocking, or automatic encryption.

To guarantee that the proper data protection measures are applied while data is at rest and triggered when data classified as at-risk is accessed, used, or transferred, policies should be created for systematically categorizing and classifying all company data, regardless of where it resides.

Advanced mathematics, computer science, communication, and engineering techniques have been combined to create modern cryptography. Computers and operating systems encrypt messages using sophisticated techniques so that only authorized parties can access them. With the use of an encryption algorithm that creates an encryption key, the message, or plaintext, is transformed into ciphertext. The recipient must employ a decryption key to convert the ciphertext back into plaintext to read the communication.

Last but not least, if you use a public, private, or hybrid cloud provider to store data or apps, carefully assess cloud providers based on the security measures they offer, but don't rely on the cloud service to secure your data. It is crucial to find out who has access to your data, how it is secured, and how frequently it is backed up.

**Final Answer**

**Conclusion:**

Data security is the practice of guarding against unauthorized access to, corruption of, or theft of digital data at any stage of its lifetime. Some claim that because of the knowledge and insight that can be gained from data, it is now more valuable than oil. Additionally, it is quite easy for fraudsters to steal your accounts and undermine your business once they have this information. Security in cyberspace is essential for all of these connected devices.