Confidentiality using conventional encryption-

Confidentiality can be achieved using conventional encryption, also known as symmetric-key encryption, which involves using the same key for both encryption and decryption. Here's how conventional encryption can be used to ensure confidentiality:

1. Encryption Process: a. Select an encryption algorithm: Choose a secure encryption algorithm, such as the Advanced Encryption Standard (AES), which is widely regarded as robust. b. Generate a secret key: Generate a strong and random encryption key. The key should be kept confidential and known only to authorized parties. c. Encrypt the data: Use the encryption algorithm and the secret key to encrypt the data. The plaintext (original data) is transformed into ciphertext (encrypted data) using the encryption algorithm and the secret key. 

1. Decryption Process: a. Obtain the secret key: To decrypt the ciphertext and recover the original plaintext, the recipient must possess the same secret key used for encryption. b. Decrypt the data: Use the decryption algorithm (which is typically the reverse of the encryption algorithm) and the secret key to decrypt the ciphertext. Applying the decryption process to the ciphertext using the secret key results in the recovery of the original plaintext.
2. Key Management:

 

* + Key Distribution: Securely distribute the secret key to the intended recipient(s). This can be done through secure channels, such as in-person exchange, secure messaging, or using secure key distribution protocols.
	+ Key Protection: Safeguard the secret key from unauthorized access or disclosure. Employ secure key storage techniques, such as using hardware security modules or secure key management systems, to protect the key from being compromised.

By using conventional encryption, the confidentiality of the data is ensured as only authorized parties possessing the secret key can decrypt the ciphertext and access the original plaintext. This protects the data from unauthorized access or disclosure during storage, transmission, or processing.

It's important to note that conventional encryption relies on the secrecy and integrity of the encryption key. Thus, key management practices, including key generation, distribution, protection, and rotation, are critical for maintaining the security of the encryption scheme. Additionally, conventional encryption does not address other aspects of security, such as data integrity or authentication, which may require additional measures or cryptographic techniques.