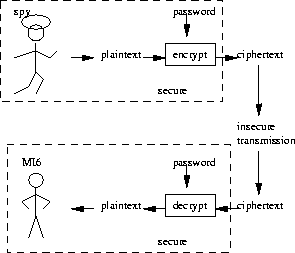
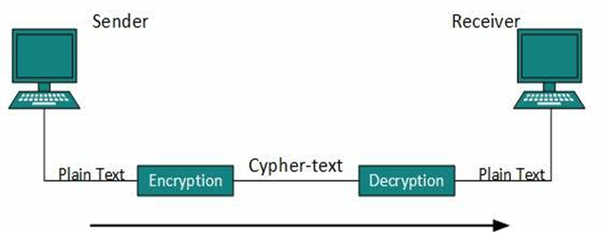
**(1) What is Cryptography ?**

* Cryptographyis the practice and study of techniques for secure communication in the presence of third parties called adversaries.
* cryptography is about constructing and analyzing protocols that prevent third parties or the public from reading private messages;
* Applications of cryptography include electronic commerce, chip-based payment cards, digital currencies, computer passwords, and military communications.
* Modern cryptography is heavily based on mathematical theory and computer science practice; cryptographic algorithms are designed around computational hardness assumptions, making such algorithms hard to break in practice by any adversary.
* encryption is the process of converting  plaintext into cipher text .
* Decryption is the process of converting cipher text to original message.
* A cipher  is a pair of algorithms that create the encryption and the reversing decryption.
* The detailed operation of a cipher is controlled both by the algorithm and in each instance by a "key". The key is a secret (ideally known only to the communicants), usually a short string of characters, which is needed to decrypt the cipher text.

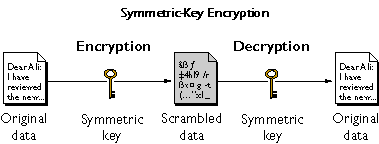




**2)What is Symmetric and Asymatric key Cryptography** **?**

**(i) Symmetric Key Cryptography**

* Symmetric-key algorithms are algorithms for cryptography that use the same cryptographic keys for both encryption of plaintext and decryption of cipher text.
* The keys may be identical or there may be a simple transformation to go between the two keys.
* Symmetric-key encryption can use either stream ciphers or block ciphers.
* Stream cipher: encrypts data one bit or one byte at a time.
* Block cipher: encrypts a block of plaintext at a time.(typically 64 or 128 bits).
* This requirement that both parties have access to the secret key is one of the main drawbacks of symmetric key encryption, in comparison to public-key encryption .



**(ii) Asymmetric Key Cryptography**

* Public-key cryptography, or asymmetric cryptography, is a cryptographic system that uses pairs of keys: public keys which may be disseminated widely, and private keys which are known only to the owner.
* In such a system, any person can encrypt a message using the receiver's public key, but that encrypted message can only be decrypted with the receiver's private key.
* The most obvious application of a public key encryption system is in encrypting communication to provide confidentiality – a message that a sender encrypts using the recipient's public key can be decrypted only by the recipient's paired private key.
* Advantage is no need to send key with message to receiver.
* if encryption key is stolen than also attacker can not decrypt the message as decryption key is only available with receiver.
* Asymmetric encryption algorithms are :RSA,Diffie-helman.
* Disadvantage is encryption is more complex and encryption and decryption is time consuming.

