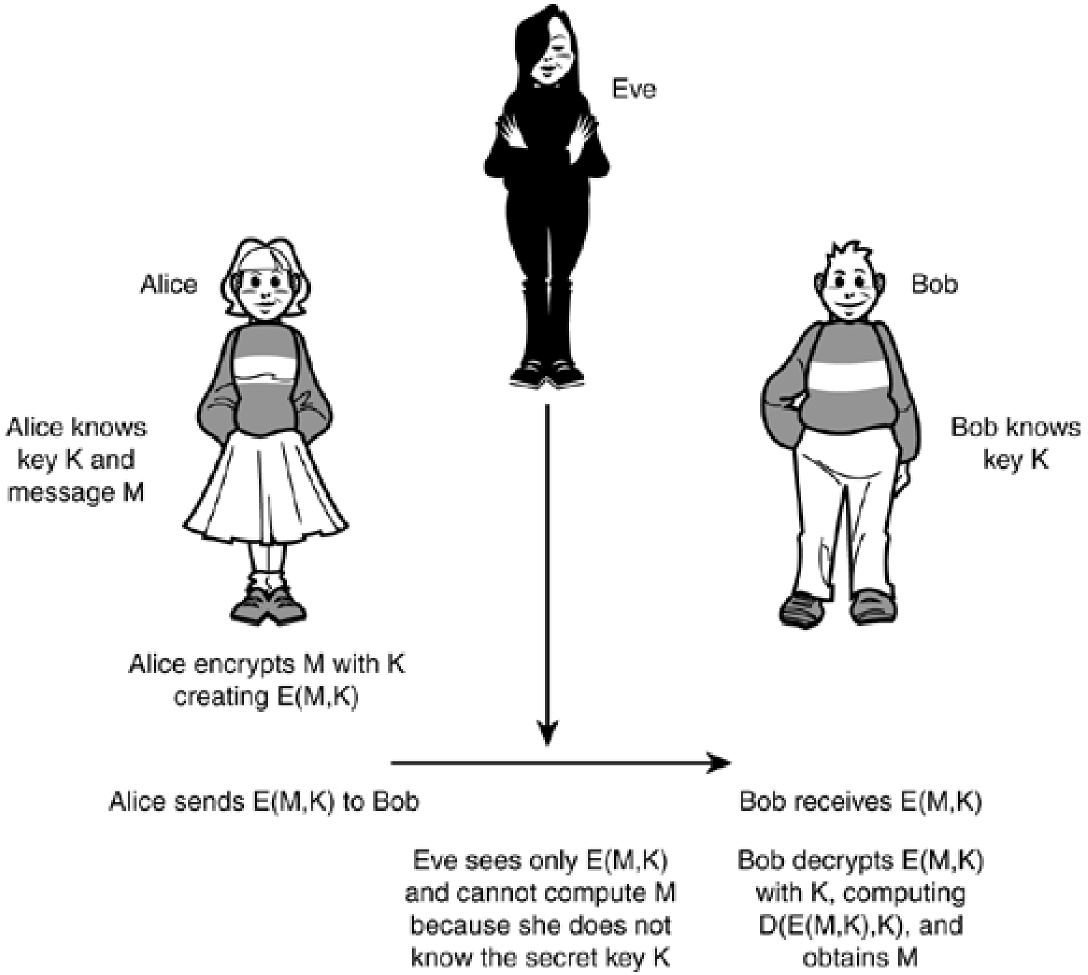
Basic Scenario of Cryptography

Basic Scenario of Cryptography

- Alice, who wants to say something privately to Bob
- Bob, who wants to hear from Alice
- Eve, the person who is trying to eavesdrop on their conversation. Eve's goal:
  - Read M
  - Get the Key Alice is using, and real all messages encrypted using that key
  - Modify the content of the message in such a way that Bob will think Alice sent the altered message.
  - Impersonate Alice and communicate with Bob who thinks he is communicating with Alice.

Passive

Active



Alice knows key K and message M

Bob knows key K

Alice encrypts M with K creating E(M,K)

Alice sends E(M,K) to Bob

Bob receives E(M,K)

Eve sees only E(M,K) and cannot compute M because she does not know the secret key K

Bob decrypts E(M,K) with K, computing D(E(M,K),K), and obtains M

(https://flylib.com/books/en/1.581.1.188/1/)

Terminologies of Cryptography

- **Cryptography: the art of secret writing**
  - The art of mangling information into apparent unintelligibility in a manner that allows a secret method of unmangling.
- **Related terminologies**
  - Cryptology: The study of communication over non-secure channels, and related problems
  - Cryptography: The process of designing systems that achieve secure communications.
  - Cryptanalysis: Breaking such systems. (The techniques used to recover the secret information hidden in cryptographic systems)
  - Plaintext: message to be sent, in readable form
  - Ciphertext: message in coded form, unreadable without special information such as a key
  - Encrypt: turn plaintext into ciphertext
  - Decrypt: turn ciphertext back into plaintext

Cryptosystem attacks

- Ciphertext-only attack
- Known-plaintext attack
- Chosen-plaintext attack
- Chosen-ciphertext attack