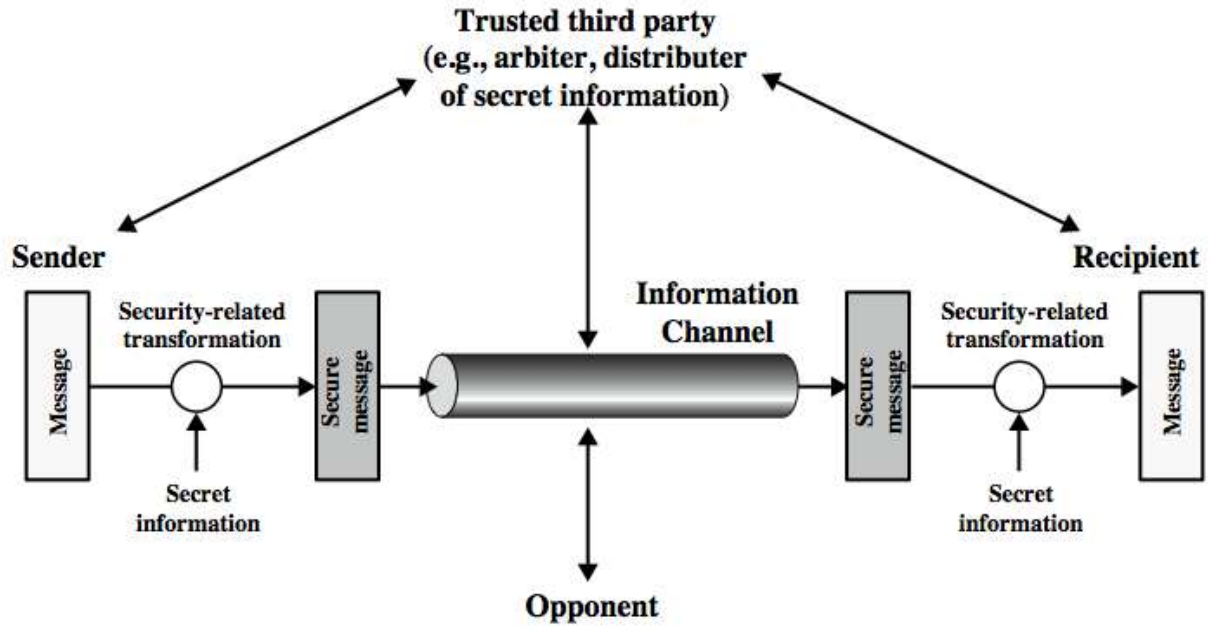
## Model for Network Security

The two parties, who are the principals in this transaction, must cooperate for the exchange to take place. They can use an appropriate security transform (encryption algorithm), with suitable keys, possibly negotiated using the presence of a trusted third party.




All the techniques for providing security have two components:

- A security-related transformation: An example includes the encryption of the message, which scrambles the message so that it is unreadable by the opponent.
- Some secret information: An example is an encryption key used in conjunction with the transformation to scramble the message before transmission and unscramble it on reception.

A trusted third party may be needed to achieve secure transmission. For example, a third party may be responsible for distributing the secret information to the two principals while keeping it from any opponent. Or a third party may be needed to arbitrate disputes between the two principals concerning the authenticity of a message transmission.