

It's getting there, but not good enough yet - see comments

Project Proposal

One of the major concerns, in the field of security, is how to communicate without fear of being overheard. When people communicate over long distances, for example, by telephone, it is difficult to make sure that no one is listening to what they say. Someone might have tapped the telephone line, and be listening to every word spoken. If the telephone line were very long, it would be difficult to protect all of it. It is simpler to encrypt any message that is to be sent. If someone is listening, then all that they will hear is garbage. Unless they know how to decrypt the message that was sent, they will not know what was being said.

Usually, when two people, (or two computers), wish to communicate securely, they agree on some form of encryption beforehand. Perhaps they will agree on a simple substitution method, and both will know which letters are to be substituted for which other letters. They can communicate securely because only they know what method they are using. Secure communications are made possible because of knowledge, known to both people, which is not known to anyone else. Usually, both people know this knowledge because they were able to hold a private conversation with each other before they began to send encrypted messages over an unsecure channel. This prior conversation can be regarded as communications, and they were therefore able to establish a secure communications channel only because they were previously able to exchange information over an already existing secure communications channel.

*add
but*

start here

It might seem intuitively obvious that if two people have never

had the opportunity to prearrange an encryption method, then they will be unable to communicate securely over an insecure channel. While this might seem intuitively obvious, I believe it is false. I believe that it is possible for two people to communicate securely without having made any prior arrangements that are not completely public. My quarter project would be to investigate any method by which this could be accomplished, and what advantages and disadvantages these methods might have over other ways of establishing secure communications.

give
2 more P's
on ideas +
then stop