Cryptology is the science of information security and privacy. Mathematical techniques are

investigated and developed to provide authenticity confidentiality, integrity and other security services

for information that is communicated, stored or processed in an information system. Also the strength

of cryptographic designs and protocols are evaluated from the point of view of mathematics, systems

theory and complexity theory.

The design part of the science is called cryptography, while the security investigations and analysis is

known as cryptanalysis. The naming convention reflects the two sides of the science of cryptology.

This division is also apparent in the practical cryptographic development work, where the best practise

has become to split the development resources into two teams. The team of cryptographers make

proposals for cryptographic designs, which the team of cryptanalysts try to break.

A cryptographic system in its basic form is often depicted as a communication system involving three

entities. Two of the entities are exchanging messages over an insecure communication channel. It has

become customary to call these entities Alice and Bob. The third entity has access to the

communication channel. She is called Carol, as the third letter to the alphabet, or Eve, as the

eavesdropper. But Eve is allowed to perform all kind of malicious actions on the communicated

messages, not just passive eavesdropping. All parties are also assumed to have certain computation

resources. Different theoretical models vary a lot with respect to the amount computation resources the

entities have and what kind of tampering Eve is performing on the communication channel.