Part X

Protocols to do seemingly impossible and zero-knowledge protocols

PROTOCOLS to do SEEMINGLY IMPOSSIBLE

A **protocol** is an algorithm two (or more) parties have to follow to perform a communication/cooperation.

A cryptographical protocol is a protocol to achieve secure communication during some goal oriented cooperation.

In this chapter we first present several cryptographic protocols for such basic cryptographic primitives as coin tossing, bit commitment and oblivious transfer.

After that we deal with a variety of cryptographical protocols that allow to solve easily seemingly unsolvable problems.

Of special importance among them are so called zero-knowledge protocols we will deaal with afterwards. They are counterintuitive, though powerful and useful.

PRIMITIVES for CRYPTOGRAPHIC PROTOCOLS

Cryptographic protocols are specifications how two parties, Alice and Bob, should prepare themselves for a communication and how they should behave during a communication in order to achieve their goal and be protected against an adversary.

In **coin-flipping protocols** Alice and Bob can flip a coin over a distance in such a way that neither of them can determine the outcome of the flip, but both can agree on the outcome in spite of the fact that they do not trust each other.

In **bit commitment protocols** Alice can choose a bit and get committed to it in the following sense: Bob has no way of learning Alice's commitment and Alice has no way of changing her commitment. Alice commits herself to a bit x using a *commit*(x) procedure, and reveals her commitment, if needed, using *open*(x) procedure.

In 1-out-2 **oblivious transfer protocols** Alice transmits two messages m_1 and m_2 to Bob who can chose whether to receive m_1 or m_2, but cannot learn both, and Alice has no idea which of them Bob has received.