“Conditional access” (in the following referred to as CA) is a technique used to protect a programme or a number of programmes from unauthorised viewing. Its implementation requires a variety of technical and commercial system components, which serve the purpose of making the programmes available only to those viewers authorised to receive them (pay TV). Viewers are usually required to pay a monthly or annual fee to gain access to a particular programme channel (pay-per-channel) or, alternatively, a fee for an individual programme (pay-per-view). CA is a technique which originated, and is widely used, in English-language countries, which is why the English expressions are internationally accepted. An overview of a complete CA system is shown in figure 8.1.

The programme signal is processed in a scrambler before transmission. Within the framework of the DVB Project it has been possible to develop a so-called common scrambling system, which is supported by all CA providers. The specification describing this system is not published so that possible “pirates” will have difficulty acquiring the knowledge needed for the construction of illegal descramblers. Although the members of the DVB Project are aware that an absolutely secure scrambling system cannot be found, they are satisfied that the common scrambling system adopted is as secure as possible. As long as the instructions for deciphering are missing in a receiver, it will be impossible to view a scrambled programme.

The DVB Project has taken the initiative to propose anti-piracy laws for Europe and for each individual country. These laws will complement the development of the common scrambling system.

The concept of the common scrambling system is based on the cascading of two ciphering procedures. In the first system, data blocks of 8 bytes, each consisting of 8 bits, are scrambled, and in the second, the resulting data are re-scrambled bit by bit [ETR 289].

The procedure used for scrambling is illustrated in figure 8.2. First of all a decision is taken as to which data are to be scrambled. If, for example, scrambling is performed at the level of the transport stream the header cannot be included, because the header is necessary to synchronise the receiver. Furthermore it must be possible for the content provider to scramble only part of the services.
Fig. 8.1. System overview of a conditional-access system