THIS SHEET HAS BEEN REPLACED

Summary

In access control systems, e.g. pay TV systems, square, or more general, d-th roots modulo X are used where X is a composite number having at least two large prime factors. If a sender, e.g. a smart-card, communicates with a receiver only few data are transmitted in order to save time. But this results in an increased number of computation operations in the sender and/or receiver.
The invention is applicable when a first cryptographic device (28) communicates with a second cryptographic device (27), especially when the devices use a modulo-based protocol. Thereby the required number of modular operations is reduced or even eliminated. It can be avoided to do modular operations by the first device.
This is particularily advantageous when said first device has a weaker computional power (e.g. less RAM and/or ROM capacity, slower clock rate) than said second device.

Fig. 2

This Sheet Has Been Replaced

