Part 2

Historical Ciphers

In this part we discuss some historical ciphers; those who are interested in pressing on with modern cryptography should jump straight to Part 3. However, discussing the construction of historical ciphers and how they were broken enables one to get a view of how modern cryptosystems came to be designed as they are. For example, modern block ciphers are built out of two key primitives, substitution and permutation, both of which occur in the construction of historical ciphers.

Encryption of most data today is accomplished using fast block and stream ciphers. These are examples of symmetric encryption algorithms. In addition all historical, i.e. pre-1960, ciphers are symmetric in nature and share some design principles with modern ciphers. The main drawback of symmetric ciphers is that they give rise to the problem of how to distribute the secret keys, a problem which resulted in the Allied breaks of Enigma and Lorenz during World War II, which we discuss in this part.