III
Cryptography

1 Some simple cryptosystems

Basic notions. Cryptography is the study of methods of sending messages in disguised form so that only the intended recipients can remove the disguise and read the message. The message we want to send is called the *plaintext* and the disguised message is called the *ciphertext*. The plaintext and ciphertext are written in some *alphabet* (usually, but not always, they are written in the same alphabet) consisting of a certain number N of *letters*. The term "letter" (or "character") can refer not only to the familiar A—Z, but also to numerals, blanks, punctuation marks, or any other symbols that we allow ourselves to use when writing the messages. (If we don't include a blank, for example, then all of the words are run together, and the messages are harder to read.) The process of converting a plaintext to a ciphertext is called *enciphering* or *encryption*, and the reverse process is called *deciphering* or *decryption*.

The plaintext and ciphertext are broken up into *message units*. A message unit might be a single letter, a pair of letters (*digraph*), a triple of letters (*trigraph*), or a block of 50 letters. An *enciphering transformation* is a function that takes any plaintext message unit and gives us a ciphertext message unit. In other words, it is a map f from the set $\mathcal{P}$ of all possible plaintext message units to the set $\mathcal{C}$ of all possible ciphertext message units. We shall always assume that f is a 1-to-1 correspondence. That is, given a ciphertext message unit, there is one and only one plaintext message unit for which it is the encryption. The *deciphering transformation* is the map f^{-1} which goes back and recovers the plaintext from the ciphertext. We