Definition. If G is a finite group, b is an element of G, and y is an element of G which is a power of b, then the *discrete logarithm* of y to the base b is any integer x such that $b^x = y$.

Example 1. If we take $G = \mathbf{F}_{19}^* = (\mathbf{Z}/19\mathbf{Z})^*$ and let b be the generator 2 (see Example 1 of § II.1), then the discrete logarithm of 7 to the base 2 is 6.

Example 2. In $\mathbf{F}_9^*$ with α a root of $X^2 - X - 1$ (see Example 2 of § II.1), the discrete logarithm of -1 to the base α is 4.

At the end of this section we shall briefly discuss the present state of algorithms to solve the discrete logarithm problem in finite fields. First we describe several public key cryptosystems or special purpose public key arrangements that are based on the computational difficulty of solving the discrete logarithm problem in finite fields.

The Diffie–Hellman key exchange system. Because public key cryptosystems are relatively slow compared to classical cryptosystems (at least at our present stage of technology and theoretical knowledge), it is often more realistic to use them in a limited role in conjunction with a classical cryptosystem in which the actual messages are transmitted. In particular, the process of agreeing on a key for a classical cryptosystem can be accomplished fairly efficiently using a public key system. The first detailed proposal for doing this, due to W. Diffie and M. E. Hellman, was based on the discrete logarithm problem.

We suppose that the key for the classical cryptosystem is a large randomly chosen positive integer (or a collection of such integers). For example, suppose we want to use an affine matrix transformation of pairs of digraphs (see § III.2)

$$C \equiv \begin{pmatrix} a & b \\ c & d \end{pmatrix} P + \begin{pmatrix} e \\ f \end{pmatrix} \; mod \; N^2,$$

where $0 \leq a,\ b,\ c,\ d,\ e,\ f < N^2$ and P is a column vector consisting of the numerical equivalents of two successive plaintext digraphs (i.e., altogether a four-letter block) in an N-letter alphabet. Once we have a randomly selected integer k between 0 and N^{12}; we can take a, b, c, d, e, f to be the six digits in k written to the base N^2. (We must check that $ad - bc$ is invertible modulo N^2; i.e., that it has no common factor with N; otherwise we choose another random integer k.)

We observe that choosing a random integer in some interval is equivalent to choosing a random element of a large finite field of roughly the same size. Let us suppose, for example, that we want to choose a random positive $k < N^{12}$. If our finite field is a prime field of p elements, we simply let an element of $\mathbf{F}_p$ correspond to an integer from 0 to $p - 1$ in the usual way; if the resulting integer is larger than N^{12}; we reduce it modulo N^{12}.