over word for word to any finite field $\mathbf{F}_q$. In order to use it we must have a nonsquare g in the field, which can easily be found by a probabilistic algorithm.) If we find a y such that $y^2 = f(x)$, we take $P_m = (x, y)$. If it turns out that $f(x)$ is a nonsquare, then we increment j by 1 and try again with the corresponding x. Provided we find an x for which $f(x)$ is a square before j gets bigger than κ, we can recover m from the point (x, y) by the formula $m = \big[(\tilde{x} - 1)/\kappa\big]$, where $\tilde{x}$ is the integer corresponding to x under the 1-to-1 correspondence between integers and elements of $\mathbf{F}_q$. Since $f(x)$ is a square for approximately 50% of all x, there is only about a $2^{-\kappa}$ probability that this method will fail to produce a point P_m whose x-coordinate corresponds to an integer $\tilde{x}$ between $m\kappa+1$ and $m\kappa+\kappa$. (More precisely, the probability that $f(x)$ is a square is essentially equal to $N/2q$; but $N/2q$ is very close to $1/2$.)

Discrete log on E. In § IV.3 we discussed public key cryptosystems based on the discrete logarithm problem in the multiplicative group of a finite field. Now we do the same in the group (under addition of points) of an elliptic curve E defined over a finite field $\mathbf{F}_q$.

Definition. If E is an elliptic curve over $\mathbf{F}_q$ and B is a point of E, then the *discrete log problem* on E (to the base B) is the problem, given a point $P \in E$, of finding an integer $x \in \mathbf{Z}$ such that $xB = P$ if such an integer x exists.

It is likely that the discrete log problem on elliptic curves will prove to be more intractible than the discrete log problem in finite fields. The strongest techniques developed for use in finite fields do not seem to work on elliptic curves. This is especially true in the case of characteristic 2. As explained in Odlyzko's survey article cited in the references, special methods for solving the discrete log problem in $\mathbf{F}_{2^r}^*$ make it relatively easy to compute discrete logs, and hence break the cryptosystems discussed in § IV.3, unless r is chosen to be rather large. It seems that the analogous systems using elliptic curves defined over $\mathbf{F}_{2^r}$ (see below) will be secure with significantly smaller values of r. Since there are practical reasons (relating to both computer hardware and software) for preferring to do arithmetic over the fields $\mathbf{F}_{2^r}$, the public key cryptosystems discussed below may turn out to be more convenient in applications than the systems based on the discrete log problem in $\mathbf{F}_q^*$.

Until 1990, the only discrete log algorithms known for an elliptic curve were the ones that work in any group, irrespective of any particular structure. These are exponential time algorithms, provided that the order of the group is divisible by a large prime factor. But then Menezes, Okamoto, and Vanstone found a new approach to the discrete log problem on an elliptic curve E defined over $\mathbf{F}_q$. Namely, they used the Weil pairing (see §III.8 of Silverman's textbook cited in the references to §1) to imbed the group E into the multiplicative group of some extension field $\mathbf{F}_{q^k}$. This imbedding reduces the discrete log problem on E to the discrete log problem in $\mathbf{F}_{q^k}^*$.

However, in order for the Weil pairing reduction to help, it is essential