any case, after Shamir's breakthrough, most experts lost confidence in the security of a public key cryptosystem of this type.

An as yet unbroken knapsack. We now describe a method of message transmission based on a knapsack-type one-way function that uses polynomials over a finite field. The cryptosystem is due to Chor and Rivest; we shall describe a slightly simplified (and less efficient) version of their construction.

Again suppose that Alice wants to be able to receive messages that are k-tuples of bits $\epsilon_0, \ldots, \epsilon_{k-1}$. (The number k is selected by Alice, as described below.) Her public key, as before, is a sequence of positive integers $v_0, \ldots, v_{k-1}$, constructed in the way described below. This time Bob must send her not only the integer $c = \sum \epsilon_j v_j$ but also the sum of the bits $c' = \sum \epsilon_j$.

Alice constructs the sequence v_j as follows. All of the choices described in this paragraph can be kept secret, since it is only the final k-tuple $v_0, \ldots, v_{k-1}$ that Bob needs to know in order to send a message. First, Alice chooses a prime power $q = p^f$ such that $q - 1$ has no large prime factors (in which case discrete logs can feasibly be computed in $\mathbf{F}_q^*$, see §3) and such that both p and f are of intermediate size (e.g., 2 or 3 digits). In the 1988 paper by Chor and Rivest the value $q = 197^{24}$ was suggested. Next, Alice chooses a monic irreducible polynomial $F(X) \in \mathbf{F}_p[X]$ of degree f, so that $\mathbf{F}_q$ may be regarded as $\mathbf{F}_p[X]/F(X)$. She also chooses a generator g of $\mathbf{F}_q^*$, and an integer z. Alice makes these choices of F, g, and z in some random way.

Let $t \in \mathbf{F}_q = \mathbf{F}_p[X]/F(X)$ denote the residue class of X. Alice chooses k to be any integer less than both p and f. For $j = 0, \ldots, k-1$, she computes the nonnegative integer $b_j < q - 1$ such that $g^{b_j} = t + j$. (By assumption, Alice can easily find discrete logarithms in $\mathbf{F}_q^*$.) Finally, Alice chooses at random a permutation π of $\{0, \ldots, k-1\}$, and sets v_j equal to the least nonnegative residue of $b_{\pi(j)} + z$ modulo $q - 1$. She publishes the k-tuple $(v_0, \ldots, v_{k-1})$ as her public key.

Deciphering works as follows. After receiving c and c' from Bob, she first computes $g^{c-zc'}$, which is represented as a unique polynomial $G(X) \in \mathbf{F}_p[X]$ of degree $< f$. But she knows that this element must also be equal to $\prod g^{\epsilon_j b_{\pi(j)}} = \prod (t + \pi(j))^{\epsilon_j}$, which is represented by the polynomial $\prod (X + \pi(j))^{\epsilon_j}$. Since both $G(X)$ and $\prod (X + \pi(j))^{\epsilon_j}$ have degree $< f$ and represent the same element modulo $F(X)$, she must have

$$G(X) = \prod (X + \pi(j))^{\epsilon_j},$$

from which she can determine the ϵ_j by factoring $G(X)$ (for which efficient algorithms are available, see Vol. 2 of Knuth).