polynomials of degree f is $\frac{1}{f}(p^f - \sum_{d<f,\ d|f} dn_d) \approx \frac{p^f}{f}$. The number of products of degree n is then the following sum taken over all partitions $n = \sum_{d=1}^{m} i_d d \ \ (i_d \geq 0)$:

$$\sum \binom{n_1 + i_1 - 1}{i_1} \cdots \binom{n_m + i_m - 1}{i_m}$$
$$\approx p^n \sum \frac{1}{2^{i_2} 3^{i_3} \cdots m^{i_m} i_1! i_2! \cdots i_m!}.$$

Thus,

$$P(n,m) = \sum \Bigl(\prod_{d=1}^{m} d^{i_d} i_d! \Bigr)^{-1}.$$

This is obviously > 0; to see that $P(n,m) < 1$, notice that there are approximately p^n/n monic irreducible polynomials of degree n, and so the probability that a monic polynomial fails to factor as desired is at least $1/n$. (b) $\sum_{i+2j=n,\ 0\leq i,j} (2^j i! j!)^{-1}$. (c) $P(3,2) = 2/3$, $P(4,2) = 5/12$, $P(5,2) = 13/60$, $P(6,2) = 19/180$, $P(7,2) = 29/630$.

§ IV.4.

1. (a) yes, 1; (b) yes, 0; (c) no, 2; (d) no, 0; (e) yes, 1; (f) no, 1.
2. (a) Use induction on k. (b) To show the second part, let v_i be strictly greater than $1 + v_{i-1} + \cdots + v_0$, and set $V = v_i - 1$.
3. Use induction.
4. (a) INTERCEPTCONVOY; (b) 89, 3, 25, 11, 41, 60, 65.
5. FORMULA STOLEN!
6. BRIBE HIM!

§ IV.5.

1. 2^T to 1.
2. (a) The numbers e and $x + e$ modulo N that Vivales receives in steps (2) and (3) are in the range from 0 to $N - 1$; so after a large number of trials Vivales will get a good idea of the magnitude of N. (b) Let N' be a very large multiple of N, and replace N by N' in steps (1) and (3).
3. The values Vivales receives in step (3) are upper bounds for x. The values Clyde sends in step (3) are not bounded from below, unlike the values $x + e$ that Pícara sends.
4. Pícara would have y as her public key; signing a document would consist of convincing the recipient that she knows its discrete log x.
5. Knowing the factorization enables one to take square roots, using the method at the end of §II.2 along with the Chinese Remainder Theorem (see also Exercise 5 of §IV.2). Conversely, suppose you have an algorithm to take square roots. Then choose a random number x, and apply the algorithm to the least nonnegative residue of x^2 *mod* n. The result will be x' such that $x'^2 \equiv x^2 \pmod{n}$. There is a 50% chance