because $2^{\text{odd}} \equiv 2 \ mod\ 3$. (iii) To show that $(*)_j$ holds after choosing $x_{j-2} = (1-a_{j-1})/3^{j-1}$, you compute the left side of $(*)_j$ modulo 3^j as follows: it equals $a_{j-1}g_{j-1}^{x_{j-2}} \equiv (1-3^{j-1}x_{j-2})g_{j-1}^{x_{j-2}}$, and then show that $(1+3)^{3^{j-2}x_{j-2}} \equiv 1+3^{j-1}x_{j-2} \ mod\ 3^j$ (use the binomial expansion). Thus, the left side of $(*)_j$ is $\equiv (1-x_{j-2}^2 3^{2(j-1)}) \equiv 1 \ mod\ 3^j$. Finally, to estimate the number of bit operations, note that each time step (iii) is performed one does a couple of multiplications and reductions (divisions) with integers having $O(\alpha)$ bits, i.e., each step takes $O(\alpha^2)$ bit operations; thus, the whole thing takes $O(\alpha^3)$ bit operations.

3. (a) To make your computation of $(g^b)^a$ in $\mathbf{F}_{31^2}$ easier, use the fact that $(c+di)^{32} = c^2+d^2$; you find that $A+Bi = 26+28i$; (b) $20+13i$; (c) $P \equiv 6C+18 \ mod\ 31$; (d) YOU'RE JOKING!
4. (a) $K_E = 1951280$, its least nonnegative residue modulo 26^4 is $7\cdot 26^3 + 0\cdot 26^2 + 13\cdot 26 + 6$; but you have to add 1 to this in order to get an invertible enciphering matrix $\begin{pmatrix} 7 & 0 \\ 13 & 7 \end{pmatrix}$; (b) $\begin{pmatrix} 15 & 0 \\ 13 & 15 \end{pmatrix}$, DONOTPAY.
5. The f_A's must commute, i.e., $f_A f_B = f_B f_A$ for all pairs of users A and B; you need to use it with a good signature scheme (as explained in the text); and it must not be feasible to determine the key for f_A from the knowledge of pairs $(P,\ f_A(P))$. For example, a translation map $f_A(P) \equiv P+b$ or a linear map $f_A(P) \equiv aP$ has the first property but not the last one, since knowing any pair $(P,\ P+b)$ (or $(P,\ aP)$) immediately enables anyone to find b (or a). The example in the text satisfies this property because of our assumption that the discrete log problem cannot be solved in a reasonable length of time.
6. $P = 6229 =$"GO!"
7. (a) First replace x by $p-1-x$ so as to reduce to the equivalent congruence $g^x a \equiv 1 \ mod\, p$. Set $l = 2^k$, and $x = x_0 + 2x_1 + \cdots + 2^{l-1}x_{l-1}$. Define $g_j = g^{2^j} \ mod\ p$ and $a_j = g^{x_0+2x_1+\cdots+2^{j-1}x_{j-1}}a \ mod\ p$ (with a_0 taken to be a). At the j-th step, compute $a_{j-1}^{2^{k-j}} = \pm 1$, and set $x_{j-1} = 0$ if it is $+1$ and $x_{j-1} = 1$ if it is -1; also compute $g_j = g_{j-1}^2$, and $a_j = g_{j-1}^{x_{j-1}}$. When $j = l$, you're done. (b) $O(log^4 p)$. (c) $k = 7912$.
8. THEYREFUSEOURTERMS.
9. To find x, Alice converts the congruence $g^S \equiv y^r r^x \equiv g^{ar+kx}$ to the congruence $S \equiv ar + kx \ mod\ p-1$, which has solution $x = k^{-1}(S - ar) \ mod\ p-1$. Bob knows p, g, and $y = y_A$, and so can verify that $g^S \equiv y^r r^x \ mod\ p$ once he is sent the pair $(r,\ x)$ along with S. Finally, someone who can solve the discrete log problem can determine a from g and y, and hence forge the signature by finding x.
10. 107.
11. (a) $9/128 = 7.03\%$, $160/1023 = 15.64\%$; (b) $70/2187 = 3.20\%$, $1805/29524 = 6.11\%$. (See the corollary to Proposition II.1.8.)
12. (a) Neglect terms beyond the leading power of p. Then the number of monic polynomials is $(p^{n+1}-1)/(p-1) \approx p^n$. The number of products of degree $< n$ can be neglected. The number n_f of irreducible monic