

algorithm always finds x and takes polynomial time in α , and estimate (using the O -notation) the number of bit operations required to find x :

- (i) Show that the discrete log problem is equivalent to the congruence with a moved to the left (i.e., $2^x a \equiv 1$). Next, show that without loss of generality we may assume that $a \equiv 1 \pmod{3}$ and x is even. Thus, we can replace our original congruence with the congruence $4^x a \equiv 1 \pmod{3^\alpha}$.
- (ii) Write $x = x_0 + 3x_1 + \cdots + 3^{\alpha-2}x_{\alpha-2}$, where the x_j are base-3 digits. Take $x_{-1} = 0$. Then the congruence

$$4^{x_0+3x_1+\cdots+3^{j-2}x_{j-2}}a \equiv 1 \pmod{3^j} \quad (*)_j$$

holds for $j = 1$. Set $g_1 = 4$. In the course of the algorithm as a by-product we will compute $g_j \stackrel{\text{def}}{=} 4^{3^{j-1}} \pmod{3^\alpha}$. Set $a_1 = a$, and for $j > 1$ define a_j to be the least positive residue mod 3^α of $4^{x_0+3x_1+\cdots+3^{j-2}x_{j-2}}a$; we will compute a_j below as we go along.

(iii) Suppose that $j > 1$ and we have found x_0, \dots, x_{j-3} such that the congruence $(*)_{j-1}$ holds (i.e., $(*)$ with $j-1$ in place of j). Further suppose that we have computed $g_{j-1} = 4^{3^{j-2}} \pmod{3^\alpha}$ and also a_{j-1} . First set x_{j-2} equal to $(1 - a_{j-1})/3^{j-1}$ modulo 3. (Notice that $a_{j-1} \equiv 1 \pmod{3^{j-1}}$ because of $(*)_{j-1}$.) Next, compute $a_j = g_{j-1}^{x_{j-2}} a_{j-1} \pmod{3^\alpha}$. Finally, if $j < \alpha$, compute g_j by raising g_{j-1} to the 3-rd power, working modulo 3^α .

(iv) When you reach $j = \alpha$, you're done.

3. You and your friend agree to communicate using affine enciphering transformations $C \equiv AP + B \pmod{N}$ (see Examples 3 and 4 in § III.1, where lowercase letters a and b were used for the coefficients of the transformation). Your message units are single letters in the 31-letter alphabet with A—Z corresponding to 0—25, blank=26, . = 27, ? = 28, ! = 29, ' = 30. You regard the key $K_E = (A, B)$ as an element $A + Bi$ in the field of 31^2 elements (where i denotes a square root of -1 in that field). You also agree to exchange keys using the Diffie–Hellman system, and to choose $g = 4 + i$. Then you randomly choose a secret integer $a = 209$. Your friend sends you her $g^b = 1 + 19i$.
 - (a) Find the enciphering key.
 - (b) What element of \mathbf{F}_{961} must you send your friend in order that she can also find the key?
 - (c) Find the deciphering transformation.
 - (d) Read the message “BUVCFIWOUJTZ!H.”
4. You receive the ciphertext “VHNHDOAM,” which was sent to you using a 2×2 enciphering matrix

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$