2. Try to break the code whose enciphering key is $(n_A, e_A) = (536813567, 3602561)$. Use a computer to factor n_A by the stupidest known algorithm, i.e., dividing by all odd numbers 3, 5, 7,.... If you don't have a computer available, try to guess a prime factor of n_A by trying special classes of prime numbers. After factoring n_A, find the deciphering key. Then decipher the message BNBPPKZAVQZLBJ, under the assumption that the plaintext consists of 6-letter blocks in the usual 26-letter alphabet (converted to an integer between 0 and $26^6 - 1$ in the usual way) and the ciphertext consists of 7-letter blocks in the same alphabet. It should be clear from this exercise that even a 29-bit choice of n_A is far too small.
3. Suppose that both plaintexts and ciphertexts consist of trigraph message units, but while plaintexts are written in the 27-letter alphabet (consisting of A—Z and blank=26), ciphertexts are written in the 28-letter alphabet obtained by adding the symbol "/" (with numerical equivalent 27) to the 27-letter alphabet. We require that each user A choose n_A between $27^3 = 19683$ and $28^3 = 21952$, so that a plaintext trigraph in the 27-letter alphabet corresponds to a residue P modulo n_A, and then $C = P^{e_A} \ mod \ n_A$ corresponds to a ciphertext trigraph in the 28-letter alphabet.
(a) If your deciphering key is $K_D = (n, d) = (21583, 20787)$, decipher the message "YSNAUOZHXXH " (one blank at the end).
(b) If in part (a) you know that $\varphi(n) = 21280$, find (i) $e = d^{-1} mod \ \varphi(n)$, and (ii) the factorization of n.
4. Show why the 35-bit integer 23360947609 is a particularly bad choice for $n = pq$, because the two prime factors are too close to one another; that is, show that n can easily be factored by "Fermat factorization" as follows. Note that if $n = pq$ (say $p > q$), then $n = (\frac{p+q}{2})^2 - (\frac{p-q}{2})^2$. If p and q are close together, then $s = (p-q)/2$ is small and $t = (p+q)/2$ is an integer only slightly larger than $\sqrt{n}$ having the property that $t^2 - n$ is a perfect square. If you test the successive integers $t > \sqrt{n}$, you'll soon find one such that $n = t^2 - s^2$, at which point you have $p = t + s$, $q = t - s$. (See Exercise 3 of § I.2 and also §3 of Chapter V.)
5. Suppose that you have a quick algorithm (a probabilistic algorithm) for solving the equation $x^2 \equiv a \ mod \ p$ for any prime p and any quadratic residue a. For example, by trying random integers and computing the Legendre symbol, with high probability we can find a nonresidue; then we can apply the algorithm described in § II.2. Suppose, however, that there is no good algorithm for solving $x^2 \equiv a \ mod \ n$ for a a square modulo n and $n = pq$ a product of two large primes, unless one knows the factorization of n (in which case one can find a square root modulo p and modulo q and then use the Chinese Remainder Theorem to find a square root modulo n). Suppose that p and q are not both $\equiv 1 \ mod \ 4$. Let $K_E = n$, and let $K_D = \{p, q\}$ be its factorization. Let $\mathcal{P} = \mathcal{C} = (\mathbf{Z}/n\mathbf{Z})^*/\pm 1$, which is the set of pairs $(x, -x)$ of residues