



Problem 3. «Affine cipher»

Consider a 29-character alphabet $\{A, \dots, Z, \alpha, \beta, \gamma\}$. Letters A, \dots, Z have numerical equivalents $0, \dots, 25$, while numbers 26, 27 and 28 correspond to symbols α, β, γ .

We use a cryptosystem with plaintexts and ciphertexts being two-letter blocks, i. e. bigrams. For each bigram it is easy to find a numerical equivalent, it is an integer from 0 to $840 = 29^2 - 1$, determined by the rule $x \cdot 29 + y$, where x and y are the numerical equivalents of the letters of the bigram.

Encryption is implemented as an affine transformation $C = a \cdot P + b \pmod{841}$, where P is a plaintext, C is the corresponding ciphertext and the pair (a, b) is a secret key. Here a and b are integer numbers between 0 and 840. For example, if $a = 2$ and $b = 27$, then the bigram DP will be encrypted as $H\gamma$. In fact, for the bigram DP we put into the correspondence the number $3 \cdot 29 + 15 = 102$. Encrypting we get $2 \cdot 102 + 27 = 231$ that corresponds to the bigram $H\gamma$, since $231 = 7 \cdot 29 + 28$.

An analysis of the long ciphertext (for a fixed unknown key) showed that the bigrams “ $\beta \gamma$ ”, “UM” and “LC” are the most often found in this text. At the same time, we assume that the most frequent bigrams in English texts are “TH”, “HE” and “IN”.

Could you then decrypt the message “KEUDCR”? What about recovering of the key?

