



## Problem 8. «Algebraic cryptanalysis»

Bob decided to construct a new stream cipher **BOB-0.1**.

He used the binary key of length 8, say  $K = (k_1, \dots, k_8)$ . Then he generated the binary sequence  $\beta$  such that  $\beta_n = k_n$  for all  $n = 1, \dots, 8$  and for  $n > 8$  it is defined as  $\beta_n = \beta_{n-1} \oplus \beta_{n-8}$ . Then Bob constructed the secret sequence  $\gamma$  for XORing it with a binary plaintext. The sequence  $\gamma$  is generated by the following rule:  $\gamma_n = \beta_n \cdot \beta_{n+2} \oplus \beta_{n+7}$  for  $n \geq 1$ .

Alice intercepted the eight secret bits of  $\gamma$  after the first 1200 missed bits. These bits are 00100001. Is she able to recover the original key  $K$ ?

