



## Problem 2. «AntCipher»

Sam studies microelectronics, while his hobbies are biology and cryptography. He decided to unite all these areas in a research project aimed at constructing a tiny GPS tracker for an ant to monitor its movements.



The tracker consists of 3 modules: GPS, encryption, transmission. Once a minute, coordinates are determined, encrypted, and transmitted to a Sam's computer, where they are automatically decrypted. Due to the size limitation, the encryption module takes only a 2-bit plaintext and produces a 2-bit ciphertext, so the coordinates are divided into 2-bit blocks which are given to the encryption module. Sam has just developed a symmetric cipher called **AntCipher** for this purpose.

The cipher must be represented by the equation  $CNF = True$ , where CNF is a conjunction of disjunctions of literals, yet literal is a Boolean variable or its negation. In the Sam's CNF,  $x_1$  and  $x_2$  correspond to the plaintext,  $x_9$  and  $x_{10}$  correspond to the ciphertext, while the remaining 6 variables are auxiliary. The equation is as follows:

$$\begin{aligned} & (x_1 \vee x_2 \vee x_9) \wedge (\neg x_1 \vee \neg x_2 \vee \neg x_9) \wedge (\neg x_1 \vee x_2 \vee \neg x_9) \wedge (x_1 \vee \neg x_2 \vee x_9) \wedge \\ & (x_1 \vee x_2 \vee x_3) \wedge (\neg x_9 \vee \neg x_{10} \vee \neg x_3) \wedge (x_1 \vee \neg x_2 \vee x_4) \wedge (\neg x_9 \vee x_{10} \vee \neg x_4) \wedge \\ & (\neg x_1 \vee x_2 \vee x_5) \wedge (x_9 \vee \neg x_{10} \vee \neg x_5) \wedge (\neg x_1 \vee \neg x_2 \vee x_6) \wedge (x_9 \vee x_{10} \vee \neg x_6) \wedge \\ & (x_1 \vee x_2 \vee x_3 \vee x_4 \vee \neg x_7) \wedge (x_2 \vee x_3 \vee x_4 \vee \neg x_7 \vee \neg x_8) = True \end{aligned}$$

The problem is that, due to the limitations, the CNF must consist of at most 20 literals and at most 16 variables, while the presented one consists of 46 literals and 10 variables. Please, help Sam to construct an equivalent CNF that fits the limits. By equivalent it is meant that for each pair of plaintext-variables' values, the same pair of ciphertext-variables' values is derived in the equation.