



Task 8. «A pseudo-random generator»

Alice and Bob communicate in Russia through the Internet using some protocol. In the process of communication Bob sends random numbers to Alice. It is known, that Bob's pseudo-random generator works in the following way:

1. it generates the binary sequence u_0, u_1, u_2, \dots , where $u_i \in \mathbb{F}_2 = \{0, 1\}$, such that for some secret $c_0, \dots, c_{15} \in \mathbb{F}_2$ it holds

$$u_{i+16} = c_{15}u_{i+15} \oplus c_{14}u_{i+14} \oplus \dots \oplus c_0u_i \text{ for all integer } i \geq 0;$$

2. i -th random number r_i , $i \geq 1$, is calculated as

$$r_i = u_{16i} + u_{16i+1}2 + u_{16i+2}2^2 + \dots + u_{16i+15}2^{15};$$

3. Bob initializes u_0, u_1, \dots, u_{15} using some integer number IV (initial value), where $0 < IV < 2^{16}$, by the same way, i. e.

$$IV = u_0 + u_12 + u_22^2 + \dots + u_{15}2^{15};$$

4. it is known that as IV Bob uses the number of seconds from January 1, 1970, 00:00 (in his time zone) to his current time (in his time zone too) modulo 2^{16} .

Eva has intercepted the third and the fourth random numbers ($r_3 = 9731$ and $r_4 = 57586$). She lives in Novosibirsk and knows that Bob has initialized the generator at November 17, 2014, at about 12:05 UTC+6 up to several minutes. The number of seconds from January 1, 1970, 00:00 UTC+6 to November 17, 2014, 12:05 UTC+6 is equal to 1 416 225 900.

Help Eva to detect Bob's time zone.