Problem 4. «A sequence»

Two friends, Roman and Anton, are very interested in sequences and ciphers. Their new cryptosystem encrypts binary messages of length n, $X = (x_1, x_2, \ldots, x_n)$, where each x_i is either 0 or 1. A key K of the cipher is a set of n integers $a_1, a_2, \ldots, a_n$. The ciphertext C for the message X encrypted with the key K is the integer

$$Y = x_1 \cdot a_1 + x_2 \cdot a_2 + \ldots + x_n \cdot a_n.$$

Roman and Anton change their key regularly. Today, the key K is defined by

$$a_i = 2^i + (-1)^i \quad \text{for all } i = 1, \ldots, n.$$

The friends can easily decipher any message using the key defined by this sequence for any n!

1. Prove that the encryption is correct for this key K for any n: there are no two distinct input messages X^1 and X^2 such that their ciphertexts C^1 and C^2 are equal, i. e. $C^1 = C^2$.

2. Describe an algorithm which can be used to easily decipher any ciphertext C encrypted with today's key K. Here "easily" means that the algorithm should work much faster than checking all possible variants for an input message X.