12

Abstract

Method for securing communications using an initialization vector the time not being known

The invention relates to a method for securing communications in a network comprising at least one emitter terminal A and one receiver terminal B, characterized in that it comprises in combination at least the following steps:

1) defining a measurable quantity that can be measured at the emitter A and the receiver B;

2) normalizing and quantifying said defined quantity;

3) initializing an initialization vector with said normalized and quantified quantity;

4) using said initialization vector with a cryptographic key to randomly generate a set of consecutive frequencies to use for securing said communications between the emitter A and the receiver B; and

5) incrementing the initialization vector by a given value after each pseudo-random generation time interval ltpa in order to generate a set of consecutive frequency values.

Figure 2 to be published.

162162

G00002