

substitution cipher CBC

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2003-10/2985.html>

From: Michael Scott (mike_at_computing.dcu.ie)

Date: 10/29/03

Date: 29 Oct 2003 05:24:51 -0800

Since a block cipher is simply a substitution cipher with a much larger block size, I was idly wondering what advantage if any would arise from using CBC mode with a simple letter-for-letter substitution cipher. For the XOR operation in CBC, simple addition/subtraction mod 26 could be used. Also was such a scheme ever used or suggested in pre-computer times...

Mike Scott