Clarification to the Skipjack Algorithm Specification

May 9, 2002

The document titled “SKIPJACK and KEA Algorithm Specifications Version 2.0” and dated 29 May 1998 provides the specification for the Skipjack algorithm. The specification is incomplete in that the order of bytes is not made clear.

Input to that algorithm can be thought of as a set of 8 bytes. If these bytes are numbered from 7 to 0, the input sequence is $B_7\ B_6\ B_5\ B_4\ B_3\ B_2\ B_1\ B_0$. These values are then placed in the w_i word array. The byte sequence is placed in to the word array in the following way:

$w_1 <= B_0\ B_1$
$w_2 <= B_2\ B_3$
$w_3 <= B_4\ B_5$
$w_4 <= B_6\ B_7$

Output from the algorithm works in a similar fashion:

$w_1 => B_0\ B_1$
$w_2 => B_2\ B_3$
$w_3 => B_4\ B_5$
$w_4 => B_6\ B_7$

Additionally, the cryptovariable is a sequence of 10 bytes. These bytes should be labeled as follows:

$cv_9\ cv_8\ cv_7\ cv_6\ cv_5\ cv_4\ cv_3\ cv_2\ cv_1\ cv_0$

Using the sample found in Annex III.A, step 0 has the data loaded into the w_i word array. In order to get w_i loaded correctly - and to be consistent with the notation above - the data supplied to the algorithm should actually read as follows:

Plaintext input:	aabbccdd00112233
Cryptovariable:	11223344556677889900

And results in the following:

Ciphertext output:	00d3127ae2ca8725