

Addenda for

STATUS REPORT
ON THE FIRST ROUND OF THE
DEVELOPMENT OF THE
ADVANCED ENCRYPTION STANDARD

August 18, 1999

It has been brought to NIST's attention by Dr. Masayuki Kanda of NTT that the "lesser attacks" on E2 listed in Sec. 2.3.2 (d) of NIST's Round 1 Report were, in fact, attacks on a *modified* version of E2 (and not the submitted version of the algorithm). Since those lesser attacks assumed a modification of part of the round function, E2 should not have been listed as having "lesser attacks".

However, NIST's overall assessment of E2 remains unchanged. The original mischaracterization of E2 as having a minor security gap (Sec. 2.6.5) did not prevent that algorithm from gaining admission to Round 2; the overall profiles of E2 and the other candidates were considered together (Sec. 2.6) in NIST's selection of the finalists.

October 1, 1999

Page 46, "Table 6. Operations Used": The reference "Source [4]" is incorrect. It should read "Source [12]".