

Part 4, §2.15.1.28, page 1,158, line 15:

First, the password string shall be converted to UTF-16LE if it is not already encoded as such, and the result hashed using the following algorithm. If there is a leading BOM character (U+FEFF) in the encoded password it is removed before hash calculation. The following steps assume that all words are unsigned, the word size is two bytes, and that bit-level SHL/SHR operations shift in the direction of the highest-order and lowest-order bit, respectively. [*Example: 0x61 SHR 1 is 0xC2, as 01100001 shifted one position in the direction of its highest-order bit is 11000010. end example*]: