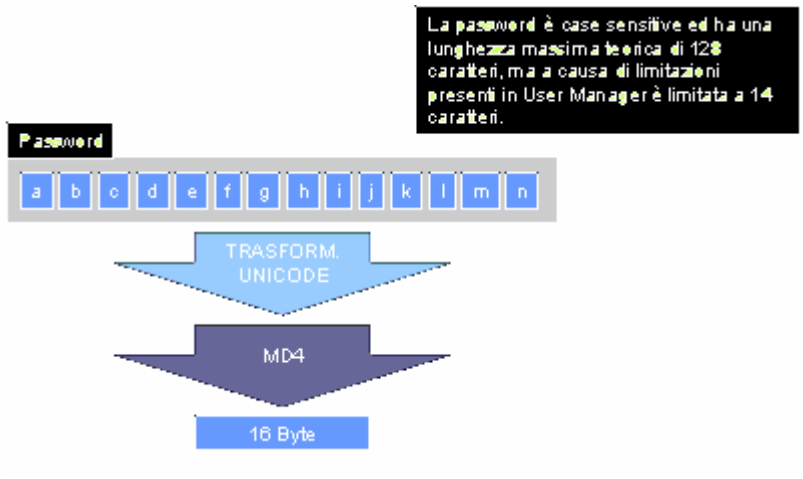
NTLM sfrutta la conversione Unicode dei caratteri. Ogni carattere Unicode è composto da 16 bit. Teoricamente, visto che il set di caratteri ASCII richiede esclusivamente l'utilizzo del primo carattere Unicode, la conversione fra i due si otterrebbe semplicemente aggiungendo un byte nullo e 0x00 nel byte più alto.

Microsoft, stando all'analisi del codice di l0phtcrack, programma ora noto con il nome di LC, ha preferito procedere diversamente. In pratica, prendendo come esempio il carattere 'A', l'algoritmo utilizzato lo converte in 0x41 0x00 e non in 0x41 0x00 0x00 0x00. Viene a mancare cioè, l'ultimo byte nullo previsto secondo le specifiche.

Dopo di che il risultato ottenuto, viene sottoposto all'algoritmo di hash MD4 per produrre infine i 16 byte finali.

A fattor comune, mi preme aggiungere che, nei sistemi MS Windows NT, per limitazioni proprie dell'interfaccia, la password viene limitata a 14 caratteri.

Semplificando, tutto il procedimento potrebbe essere così riassunto:



Lo schema NTLM utilizzato su HTTP è il seguente: