6.2. MAC на основе алгоритма симметричного шифрования

Для вычисления *MAC* может использоваться алгоритм симметричного шифрования (например, DES) в режиме CBC и нулевой инициализационный вектор. В этом случае сообщение представляется в виде последовательности блоков, длина которых равна длине блока алгоритма шифрования. При необходимости последний блок дополняется справа нулями, чтобы получился блок нужной длины. Вычисление *MAC* происходит по следующей схеме:

$MAC_1 = E_K [P_1]$

$MAC_2 = E_K [P_2 \oplus MAC_1]$

. . .

$MAC_N = E_K [P_N \oplus MAC_{N-1}]$

$MAC = MAC_N$