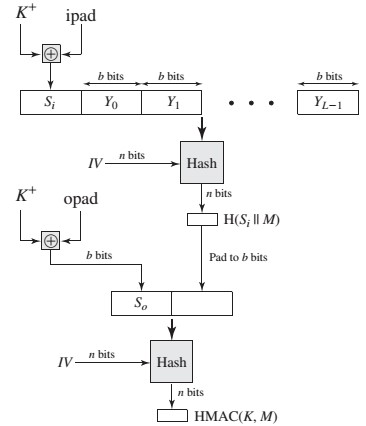
•



*:*

**31**

HMAC:از دو بخش درهمساز داخلی ودرهم‌ساز خارجی تشکیل شده است.

+K: کليد مخفي که يک دنباله صفربه آن اضافه شده است.

ipad : تکرار رشته 00110110

IV:برای مقداردهی اولیهstate

opad : تکرار رشته 01011010

HMACK =

H[(K+ opad) || H[(K+ ipad) || M ]]