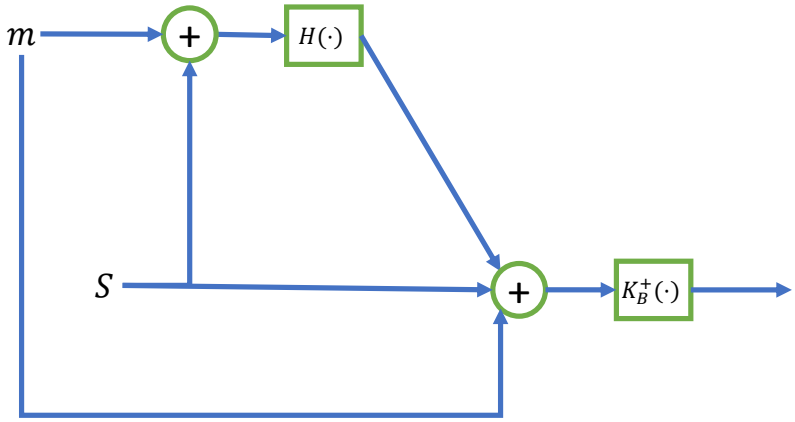
سوال ۶) در مراحل رمزنگاری زیر، فرض کنید بلوک دایره، اتصال دو رشته به هم را نمایش می دهد. هم چنین K_A^+ ، K_A^- ، K_B^+ و K_B^- به ترتیب کلیدهای عمومی و خصوصی آلیس و کلیدهای عمومی و خصوصی باب باشند. همچنین بلوک تابع چکیده ساز (Hash) در شکل نشان داده شده است:



فرض کنید آلیس جهت ارسال پیام m به باب، یک کلید تصادفی S تولید و از آن هم در تابع چکیده ساز و هم در اتصال دو رشته (مطابق شکل) استفاده می کند.

الف) بلوک دیاگرام لازم را برای رمزگشایی کردن پیام ارسالی ترسیم کنید.

ب) در این شکل، کدام یک از موارد محرمانگی، اصالت پیام و تمامیت پیام (Message Integrity) حفظ می شوند؟

پ) تغییری (حداقلی) در بلوک دیاگرام ایجاد کنید به گونه ای که مواردی که در ب) حفظ نشده اند، رعایت شوند (پاسخ ممکن است یکتا نباشد؛ ولی تلاش کنید با کمترین اصلاحات ممکن به پاسخ برسید!)