

هدف از به کارگیری این کد آن است که مهاجم نتواند پیام ارسالی را بدون اینکه طرفین مکالمه متوجه شوند تغییر دهد. مهاجم نتواند پیام ارسالی را بدون اینکه طرفین مکالمه.

(از کتاب رمزنگاری)