

فهرست مطالب

- مفاهیم اولیه احراز اصالت پیام
- استفاده از توابع رمزنگاری در احراز اصالت پیام
- استفاده از تابع درهم ساز برای احراز اصالت پیام
- توابع درهم ساز مهم
- HMAC

مفهوم احراز اصالت پیام

- اطمینان از:

– صحت پیام؛ یعنی پیام دریافتی دستکاری نشده است:

- بدون تغییر،

- بدون درج،

Data Integrity

- بدون حذف

- بدون تکرار و تغییر توالی

– این که پیام از جانب فرستنده ادعا شده ارسال شده است

Data Origin Authentication

اهمیت اصالت پیام

در بسیاری از کاربردها مانند:

- تراکنشهای مالی

- ثبت احوال و اسناد

- بانکهای اطلاعاتی

ممکن است ارائه سرویس محرمانگی اهمیت زیادی نداشته باشد ولی اینکه محتوای اطلاعات قابل اعتماد باشند از اهمیت بسیار بالاتری برخوردار است.

راهکارهای احراز اصالت پیام

□ رمز گذاری پیام

- متن رمز کل پیام به عنوان احراز کننده اصالت پیام

□ کد احراز صحت پیام (MAC)

- تابعی از متن پیام و یک کلید سری (با خروجی با اندازه ثابت) به عنوان احراز کننده پیام

□ استفاده از توابع درهم ساز برای احراز صحت پیام

- خروجی حاصل از نگاشت پیام به یک مقدار با طول ثابت (با استفاده از یک تابع درهم ساز) به عنوان احراز کننده پیام

استفاده از رمزنگاری در احراز اصالت پیام

- رمزنگاری یک پیام و امکان بازگشایی آن می تواند به صورت مستقیم برای احراز اصالت پیام استفاده شود
- در صورت وجود کلید صحیح امکان رمزنگاری معتبر وجود دارد
- برای پی بردن به صحت داده ها نیاز به وجود الگوی قابل شناسایی در داده ها می باشد

کدهای احراز اصالت پیام

- تولید یک برجسب با طول ثابت:

- وابسته به پیام

- لزوماً برگشت پذیر نیست

- نیازمند یک کلید مخفی مشترک بین طرفین

- آنرا به اختصار MAC مینامند. نام دیگر:

“Cryptographic Checksum”

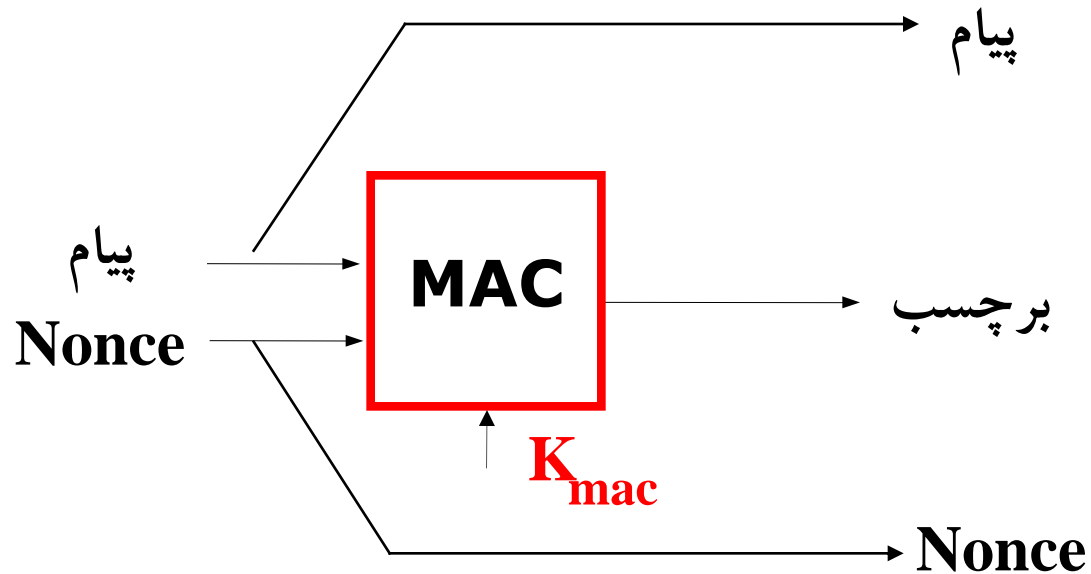
- این برجسب را به پیام اضافه میکنند.

- گیرنده خود برجسب پیام را محاسبه نموده و با برجسب ارسالی مقایسه میکند.

- از اصالت پیام (یا اصالت فرستنده آن) اطمینان حاصل میشود.

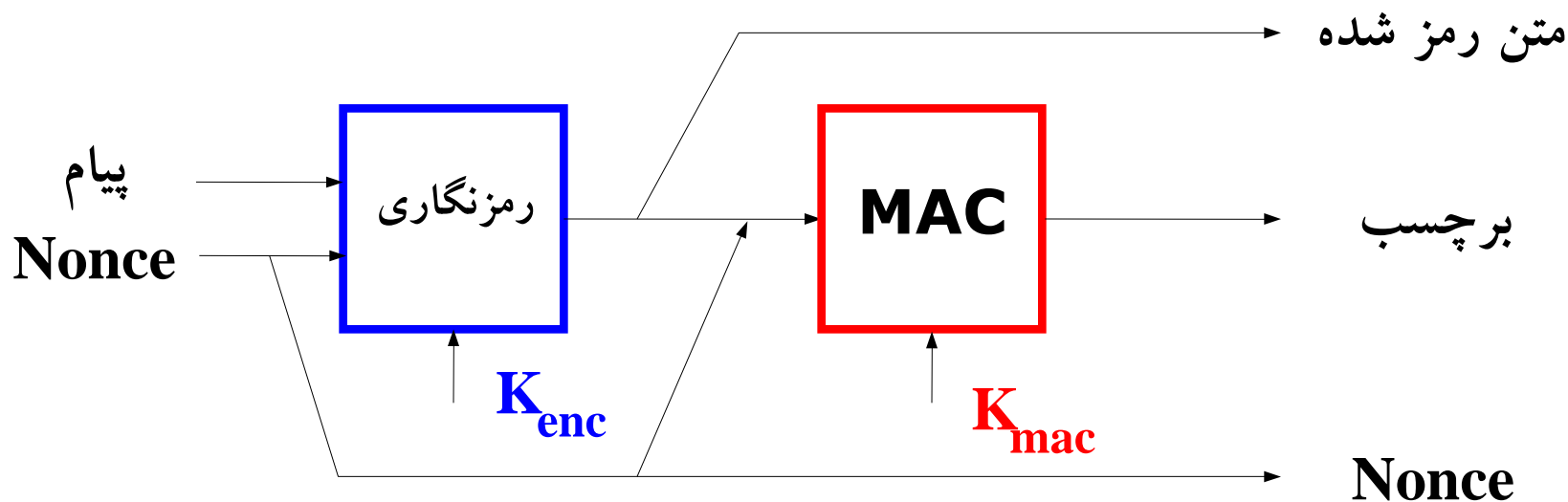
کدهای احراز اصالت پیام

سرویس صحت:



کدهای احراز اصالت پیام

سرویس محرمانگی و صحت:



• ویژگیها:

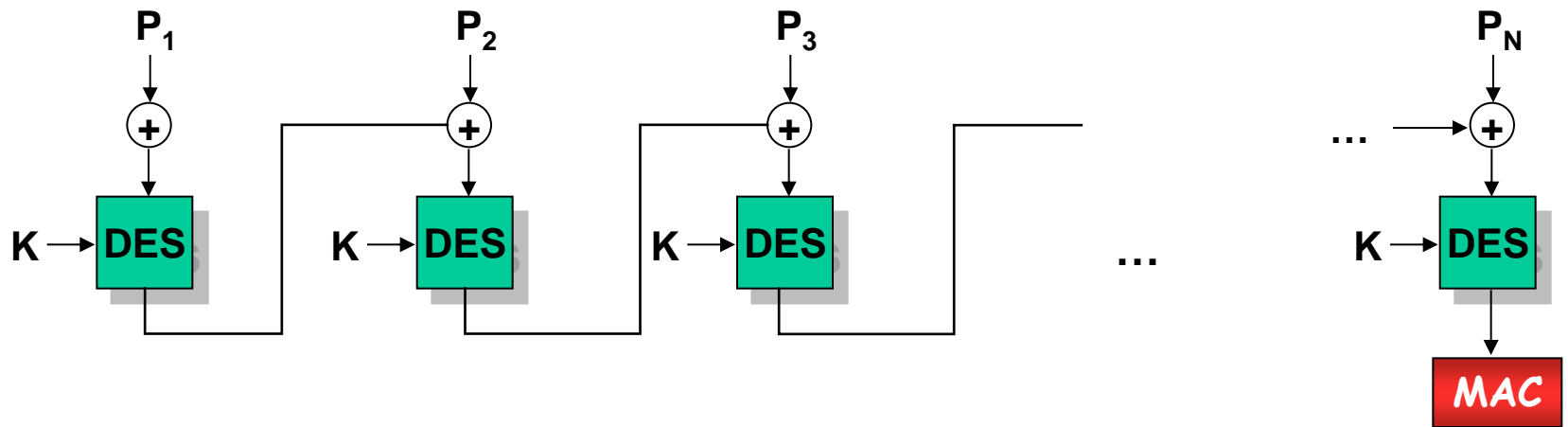
- هزینه کل » (هزینه رمز نگاری) + (هزینه تهیه MAC)
- نیاز به دو کلید

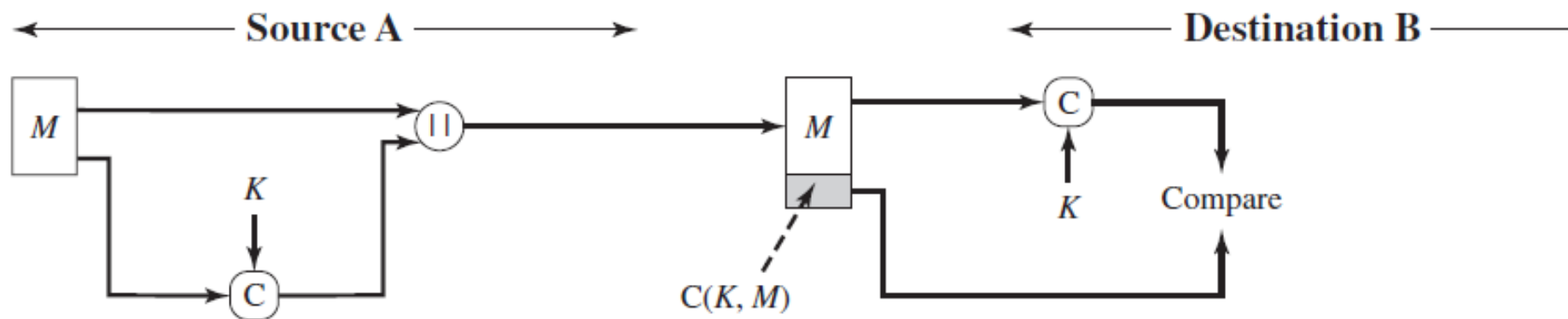
کدهای احراز اصالت پیام

- **DAA (Data Authentication Algorithm)**
 - استاندارد NIST و ANSI X9.17
 - بر اساس رمز قالبی DES و مد کاری CBC
 - همانند رمز نگاری CBC، پیام را پردازش کرده و تنها آخرین قالب را به عنوان برچسب استفاده میکنیم.

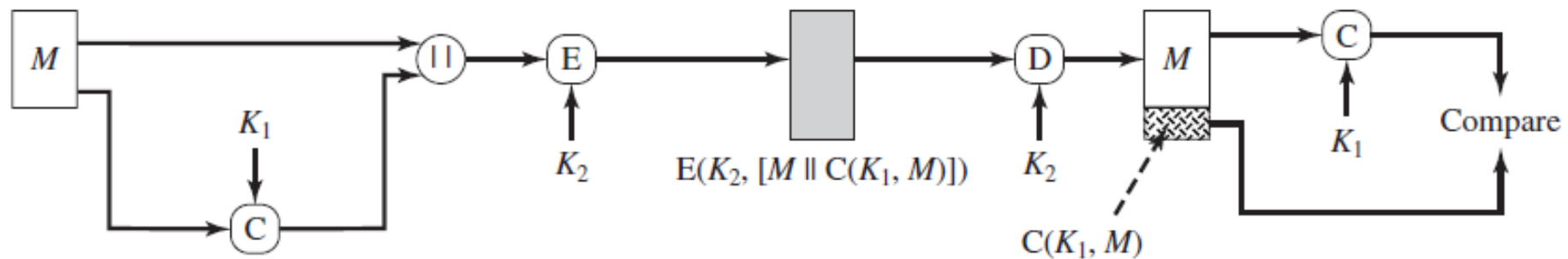
DAA

متن واضح (تقسیم شده به قالبها)

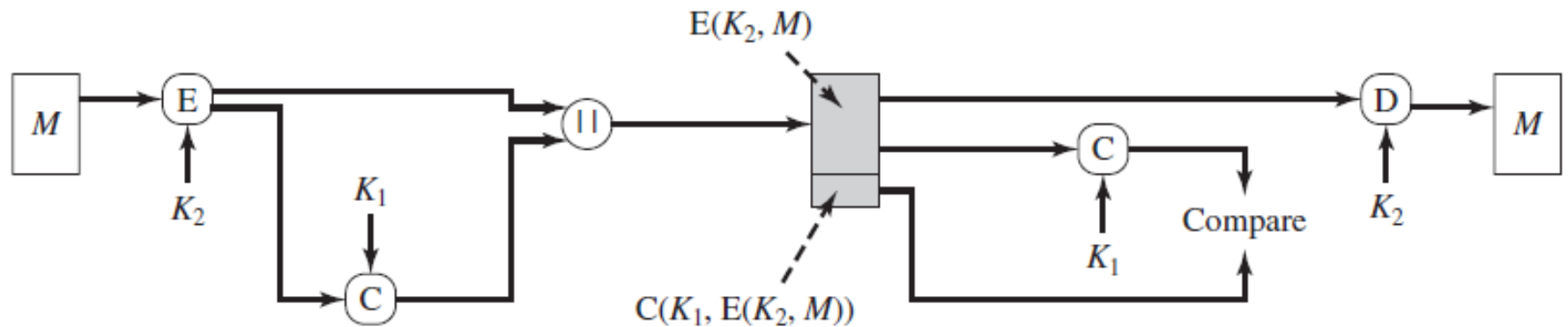




(a) Message authentication



(b) Message authentication and confidentiality; authentication tied to plaintext



(c) Message authentication and confidentiality; authentication tied to ciphertext

Figure 12.4 Basic Uses of Message Authentication code (MAC)

استفاده از توابع درهم ساز در احراز اصالت پیام

- تابع یک طرفه
- طول ورودی متغیر
- طول خروجی ثابت (نگاشت از فضای بزرگتر به فضای کوچکتر) به گونه ای که:
 - امکان نگاشت ورودی های متفاوت به یک خروجی
 - به این رشته عصاره یا چکیده پیام (Digest) میگوییم.
- در حالت کلی، کلیدی در کار نیست!

امنیت توابع درهم ساز

□ توابع درهم ساز باید یک طرفه (One-Way) باشند.

■ برای یک h داده شده، باید یافتن x به گونه ایی که $h = H(x)$ از لحاظ محاسباتی ناممکن باشد.

□ مقاومت در برابر تصادم ضعیف (Weak Collision)

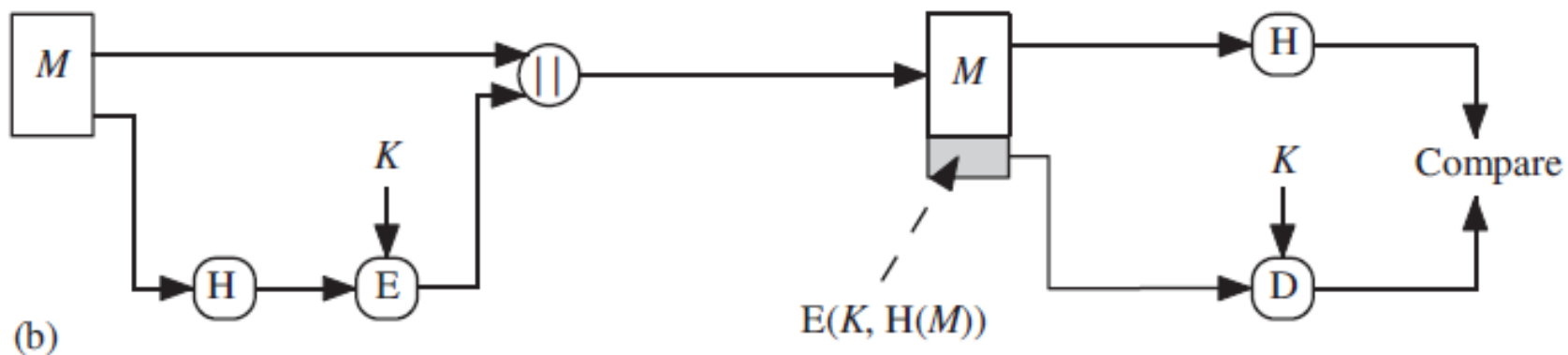
■ برای یک x داده شده، باید یافتن y به گونه ایی که $H(y) = H(x)$ از لحاظ محاسباتی ناممکن باشد.

□ مقاومت در برابر تصادم قوی (Strong Collision)

■ یافتن x و y به گونه ایی که $H(y) = H(x)$ از لحاظ محاسباتی ناممکن باشد.

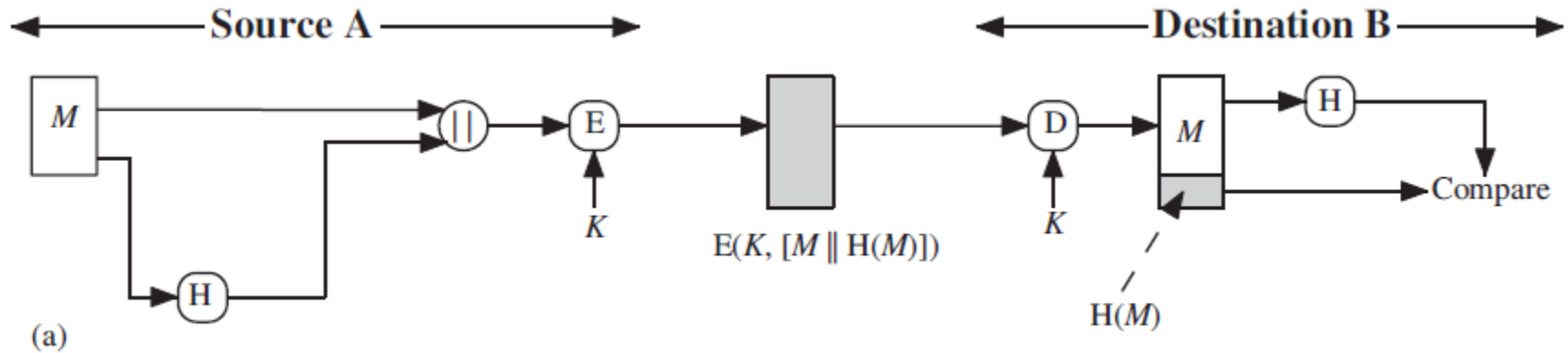
توابع درهم ساز و رمز نگاری متقارن

سرویس صحت:



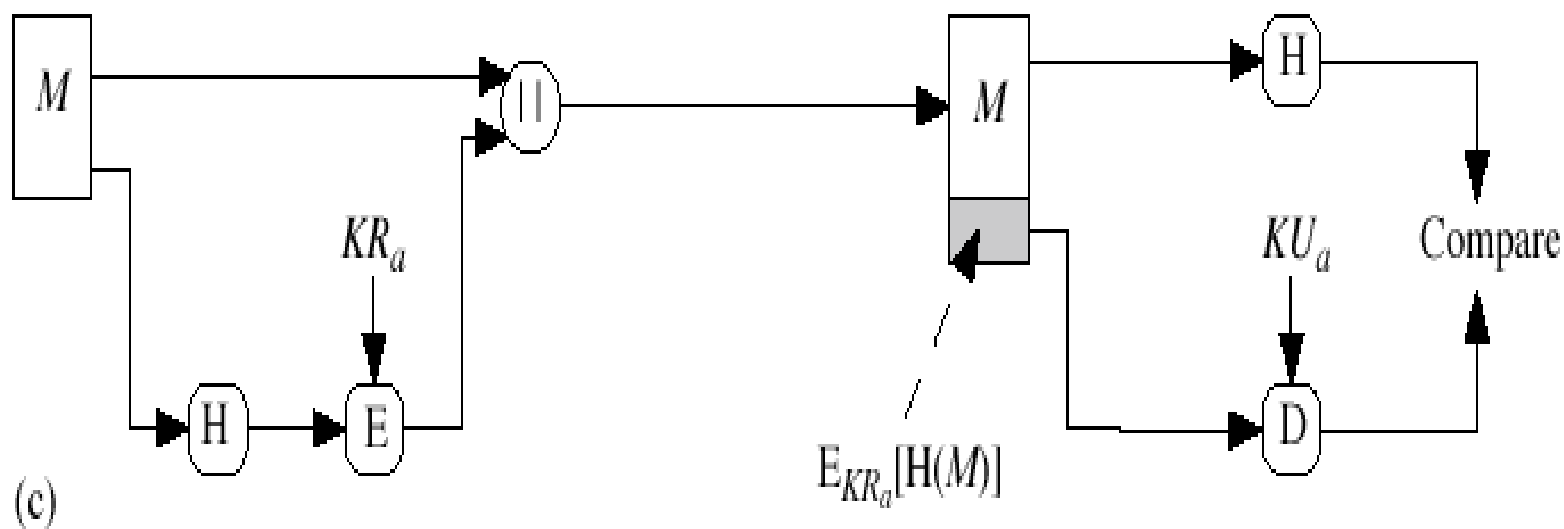
توابع درهم ساز و رمز نگاری متقارن

سرویس محرمانگی و صحت:



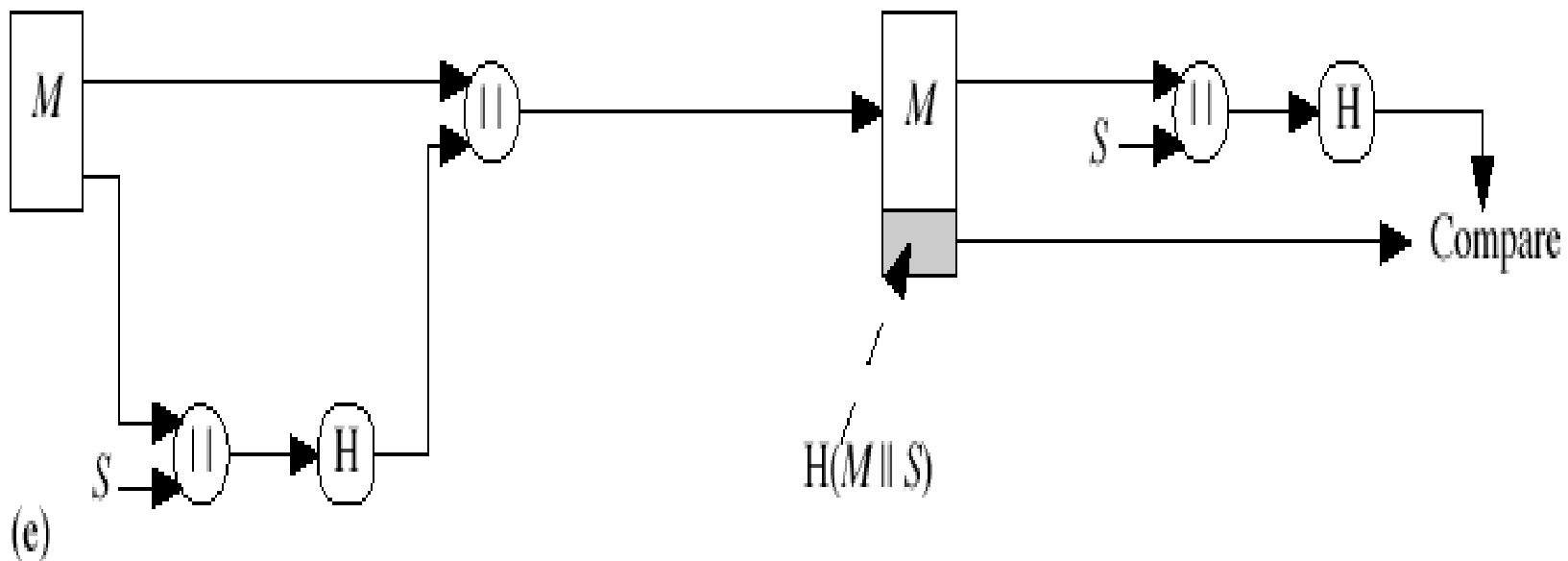
توابع درهم ساز و رمز نگاری نا متقارن

سرویس امضاء:



روشهای دیگر احراز اصالت پیام

- طرفین راز S را مخفیانه به اشتراک گذاشته اند.
- بدون استفاده از رمز
- کاربرد عملی زیاد



مقایسه رمزنگاری و توابع درهمساز

- رمزهای قالبی:

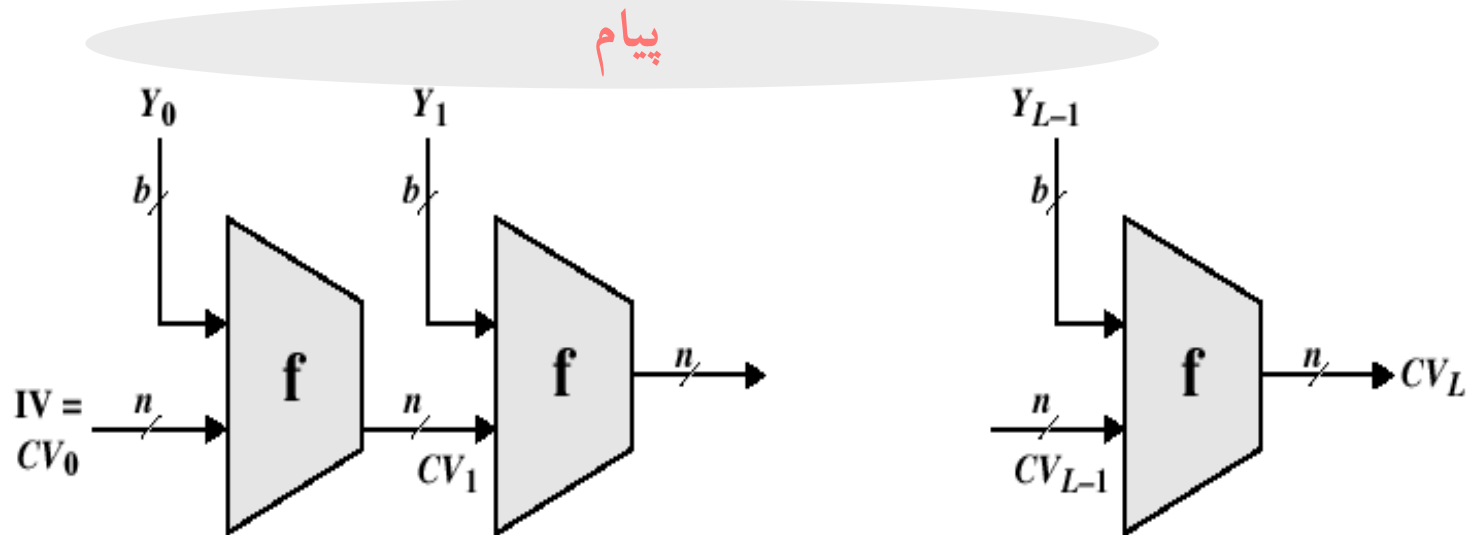
- پیاده سازی نرم افزاری توابع درهم ساز متداول سریعتر از رمزهای قالبی قابل اجرا است.

- دارای هزینه سخت افزاری بیشتر

- کارایی کمتر برای داده های حجیم

- دارای محدودیت های صادراتی (Export Control)

ساختار درونی تابع درهم ساز



IV = Initial value
 CV = chaining variable
 Y_i = i th input block
 f = compression algorithm
 L = number of input blocks
 n = length of hash code
 b = length of input block

- پیام به قطعات Y_i تقسیم شده است.
- IV یک رشته ثابت میباشد.

$$CV_0 = IV$$

$$CV_i = f(CV_{i-1}, Y_{i-1})$$

$$\text{Hash} = CV_L$$

توابع درهم ساز مهم: MD5

• MD5: Message Digest 5

- طراحی 1992 توسط Rivest، یکی از سه طراح RSA
- استفاده گسترده در گذشته، اما از کاربرد آن کاسته شده است.
- ویژگیها:

– پیام به قطعات ۵۱۲ بیتی تقسیم می شود

– خروجی ۱۲۸ بیتی

امنیت MD5

- حملات کارگر به این الگوریتم یافت شده اند:
 - Berson سال ۱۹۹۲: حمله تفاضلی به یک دور الگوریتم
 - Boer و Bosselaers سال ۹۳: یافتن تصادم های مجازی
 - Dobbertin سال ۹۶: تصادم در تابع فشرده ساز

توابع درهم ساز مهم: SHA-1

• 1 – SHA-1: Secure Hash Algorithm

- استاندارد NIST، ۱۹۹۵
- طول ورودی $> 2^{64}$ بیت
- طول خروجی ۱۶۰ بیت
- استفاده شده در استاندارد امضای دیجیتال DSS
- امنیت:
- در برابر حملات شناخته شده مقاومت بالایی دارد

گونه های SHA-1

□ نسخه‌های زیر نیز علاوه بر SHA-1 استاندارد شده اند:

■ SHA-256، SHA-384 و SHA-512

■ معروف به خانواده SHA-2 هستند.

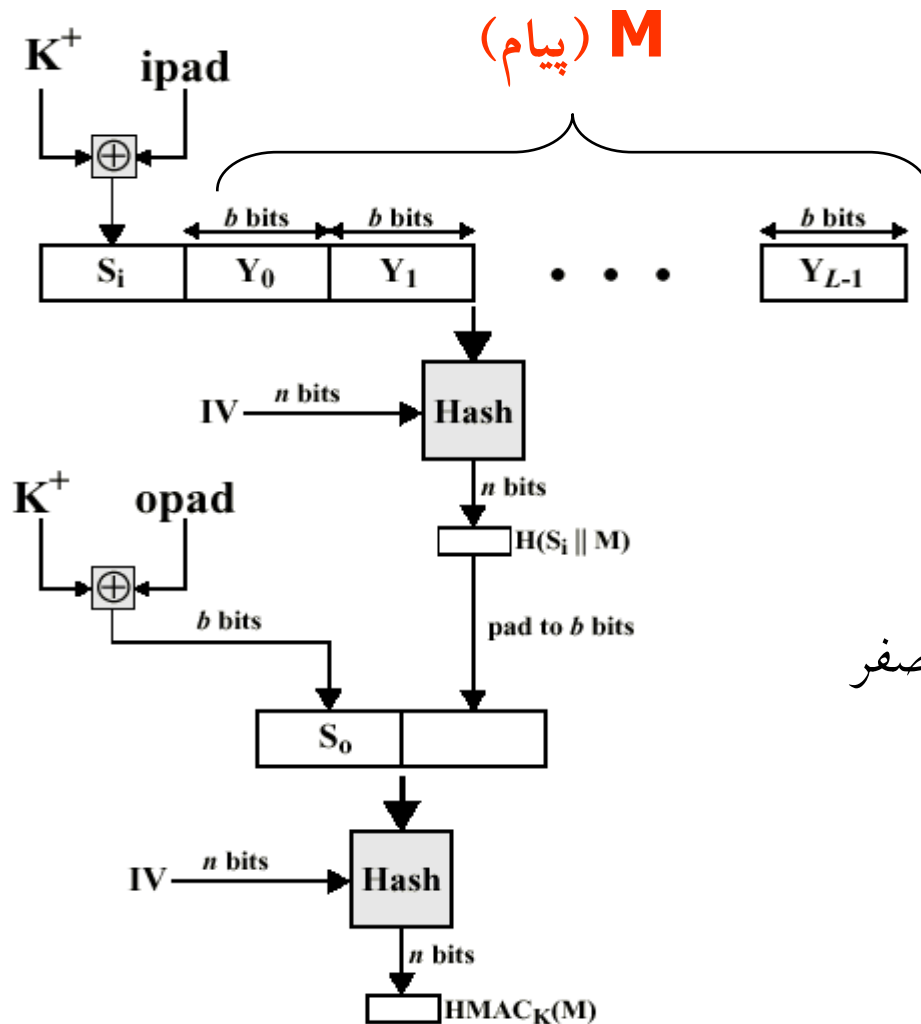
■ از لحاظ ساختار و جزئیات مشابه SHA-1 هستند.

Algorithm	Digest size	Block size	Message size	Security
SHA-1	160	512	$< 2^{64}$	80 bits
SHA-256	256	512	$< 2^{64}$	128 bits
SHA-384	384	1024	$< 2^{128}$	192 bits
SHA-512	512	1024	$< 2^{128}$	256 bits

HMAC

- **HMAC** یک الگوریتم احراز اصالت پیام است
- **HMAC** اساساً روشی برای ترکیب کردن کلید مخفی با الگوریتمهای درهم ساز فعلی می باشد.
- برای تولید چکیده پیغام، از توابع درهم استفاده شده است
 - در مقابل استفاده از رمزهای قطعه ای
 - بدلیل مزایای عملی توابع درهم ساز

HMAC



• H : تابع درهم ساز به کار گرفته شده

• M : پیام ورودی

• K : کلید مخفی

• K^+ : کلید مخفی که یک دنباله صفر

به آن اضافه شده است

• $ipad$: تکرار رشته ۰۰۱۱۰۱۱۰

• $opad$: تکرار رشته ۰۱۰۱۱۰۱۰

$$HMAC_K(M) = H[(K^+ \oplus opad) || H[(K^+ \oplus ipad) || M]]$$

Figure 9.10 HMAC Structure

Exhaustive Search	آزمون جامع
Tag	برچسب
Packet	بسته
Compression	تابع فشرده ساز
One way Function	تابع یک طرفه
Transaction	تراکنش
Collision	تصادم
Pseudo Collision	تصادم های مجازی
Modification	تغییر
Integrity	صحت (تمامیت)
Hash Function	تابع درهم ساز
Delete	حذف
Differential Attack	حمله تفاضلی
Birthday Attack	حمله روز تولد
Linear	خطی
Insert	درج
Frame Check Sequence	دنباله بررسی قالب

Round	دور
Block Cipher	رمز قالبی
Decryption	رمز گشایی
Conventional Encryption	رمزنگاری مرسوم
Collision Free	عاری از تصادم
Non-repudiation	انکارناپذیری
Unauthorized	غیر مجاز
Plain text	متن واضح
Confidentiality	محرمانگی
Operation Mode	نحوه بکارگیری
Valid	معتبر
Infeasible	ناممکن
MAC	کدهای احراز اصالت پیام
Error Detection Code	کدهای تشخیص خطا