فهرست مطالب

- مفاهیم اولیه
- رمزگذاری پیام و کدهای تشخیص خطا
- کد های احراز اصالت پیام
- اصول توابع درهم ساز
- توابع درهم ساز مهم
- HMAC

مفهوم احراز اصالت پیام

- اطمینان از:
  - صحت پیام؛ یعنی پیام دریافتی دستکاری نشده است:
    - بدون تغییر،
    - بدون درج،
    - بدون حذف
    - بدون تکرار و تغییر توالی

Data Integrity

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

Data Origin Authentication

اهمیت اصالت پیام

در بسیاری از کاربرد ها 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

- رمزگذاری 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 احرازکننده پیام
- استفاده از توابع درهم‌ساز برای احراز صحت پیام
  - خروجی حاصل از نگاشت پیام به یک مقدار با طول ثابت (با استفاده از یک تابع درهم ساز) به عنوان احرازکننده پیام

فهرست مطالب

- مفاهیم اولیه
- رمزگذاری پیام و کدهای تشخیص خطا
- کد های احراز اصالت پیام
- اصول توابع درهم ساز
- توابع درهم ساز مهم
- HMAC

رمزگذاری پیام برای احراز اصالت پیام

- فرستنده پیام را رمز می‌کند.
- اگر متن رمز شده دستکاری شود با رمزگشایی به متن آشکار نامفهوم (درهم و برهم) می‌رسیم.
- گیرنده، بعد از رمزگشایی چک می‌کند که آیا پیام مفهوم است یا نه؟
- می توان از الگوریتم‌های رمز متقارن و یا نامتقارن برای این منظور استفاده کرد.

کاربرد رمزگذاری پیام

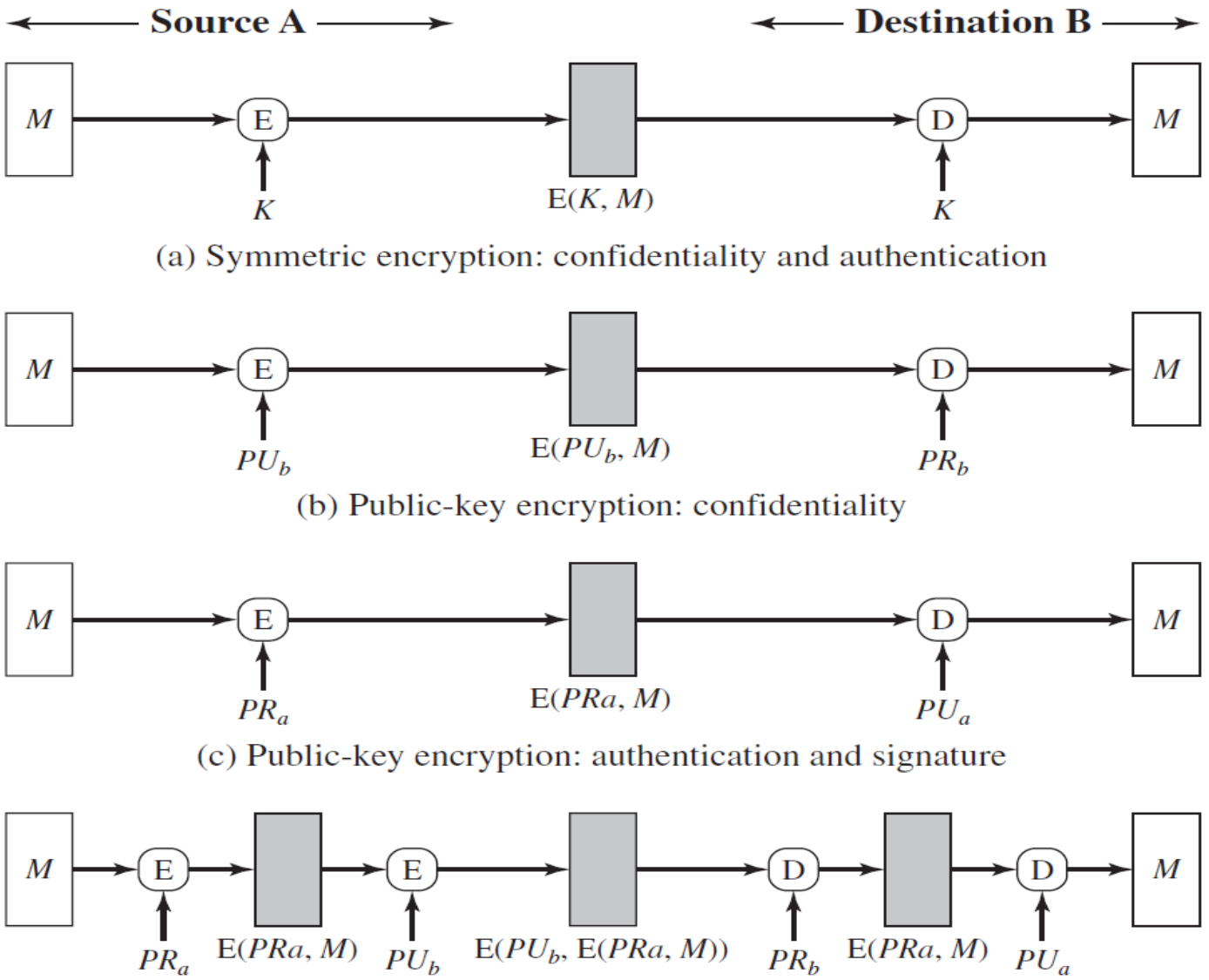


Figure 12.1 Basic Uses of Message Encryption

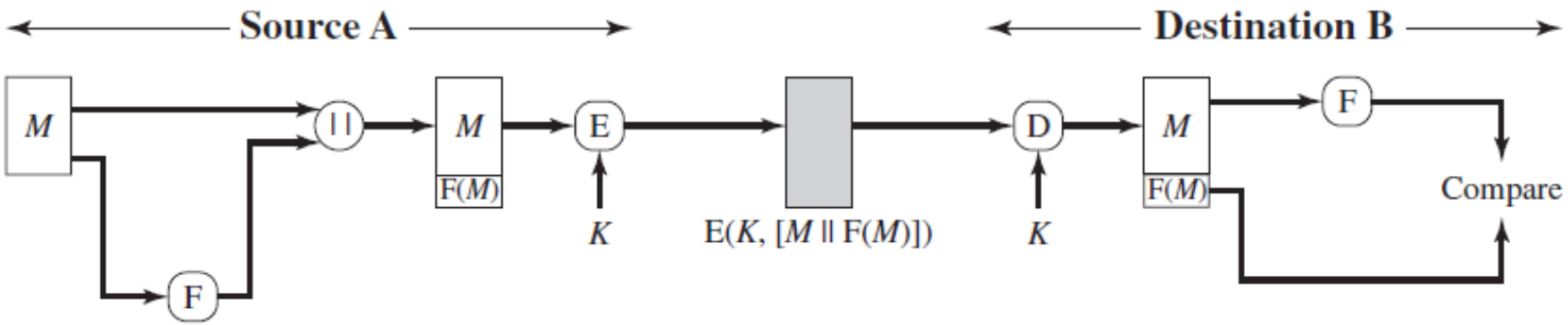
مشکلات رمزنگاری

- بررسی مفهوم بودن محتوا همواره آسان نیست.
  - در حالت کلی با نوعی افزونگی، ساختار درونی مورد انتظار را جستجو می‌کنند.
  - دشواری خودکارسازی فرآیند چک کردن ....
- هنگام ارسال داده
  - اگر داده ها خود تصادفی به نظر برسند، یعنی از ساختار درونی خاصی تبعیت ننمایند، بررسی محتوا تقریباً ناممکن است.
- **راه‌حل اولیه:** استفاده از کدهای تشخیص خطا
  - مثال: یک بیت به انتهای پیام اضافه نماییم، به گونه‌ای که تعداد بیتهای یک زوج شود.

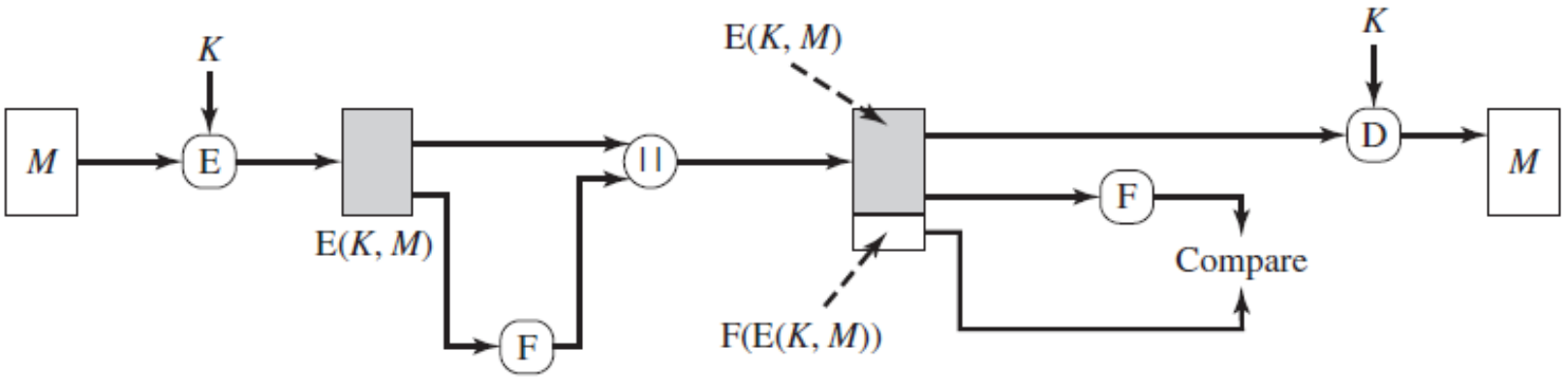
انواع کدهای تشخیص خطا

دو مدل اضافه کردن کد تشخیص خطا (اولی مناسب تر است)

تابع F کد تشخیص خطا



(a) Internal error control



(b) External error control

Figure 12.2 Internal and External Error Control

ناامن بودن کدهای تشخیص خطا

- کدهای تشخیص خطا مانند CRC برای تشخیص خطای حاصل از نویز در کاربردهای مخابراتی طراحی شده اند.
  - نویز:
    - تغییرات غیر هوشمندانه و غیر عمدی
  - دشمن:
    - تغییرات هوشمندانه و عمدی
- حملات موفقی به الگوریتمهایی که از کدهای تشخیص خطا استفاده میکردند، صورت پذیرفته است.
  - مثال: پروتکل ۸۰۲.۱۱

ناامن بودن کدهای تشخیص خطا

- کد تشخیص خطا نمی تواند در حالت کلی از دستکاری بسته ها جلوگیری کند
- راه حل : استفاده از کدهای احراز اصالت پیام

فهرست مطالب

- مفاهیم اولیه
- رویکردهای ممکن
- کد های احراز اصالت پیام
- اصول توابع درهم ساز
- توابع درهم ساز مهم
- HMAC

کد های احراز اصالت پیام

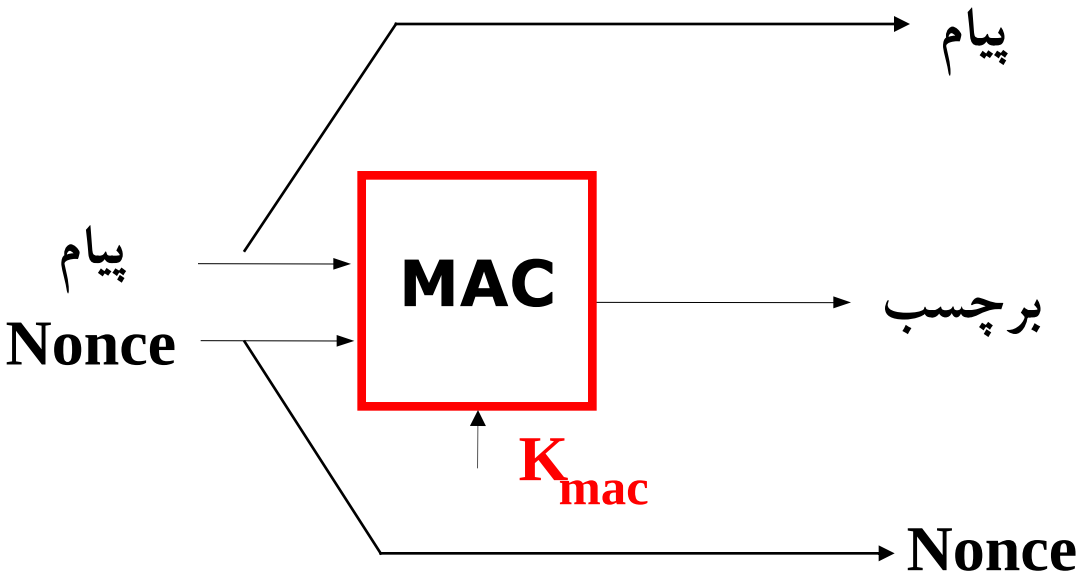
- تولید یک برچسب با طول ثابت:
  - وابسته به پیام
  - لزوماً برگشت پذیر نیست
  - نیازمند یک کلید مخفی مشترک بین طرفین
- آنرا به اختصار **MAC** مینامند. نام دیگر:

"Cryptographic Checksum"

- این برچسب را به پیام اضافه میکنند.
- گیرنده خود برچسب پیام را محاسبه نموده و با برچسب ارسالی مقایسه میکند.
- از اصالت پیام (یا اصالت فرستنده آن) اطمینان حاصل میشود.

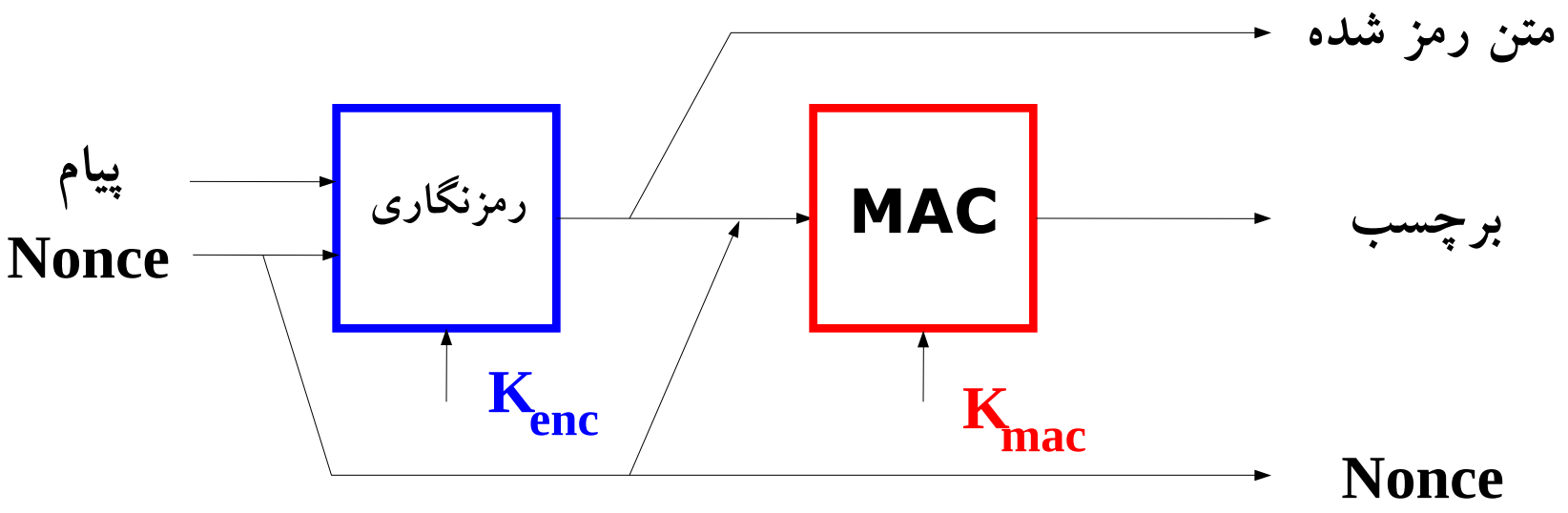
کد های احراز اصالت پیام

سرویس صحت:



کد های احراز اصالت پیام

سرویس محرمانگی و صحت:

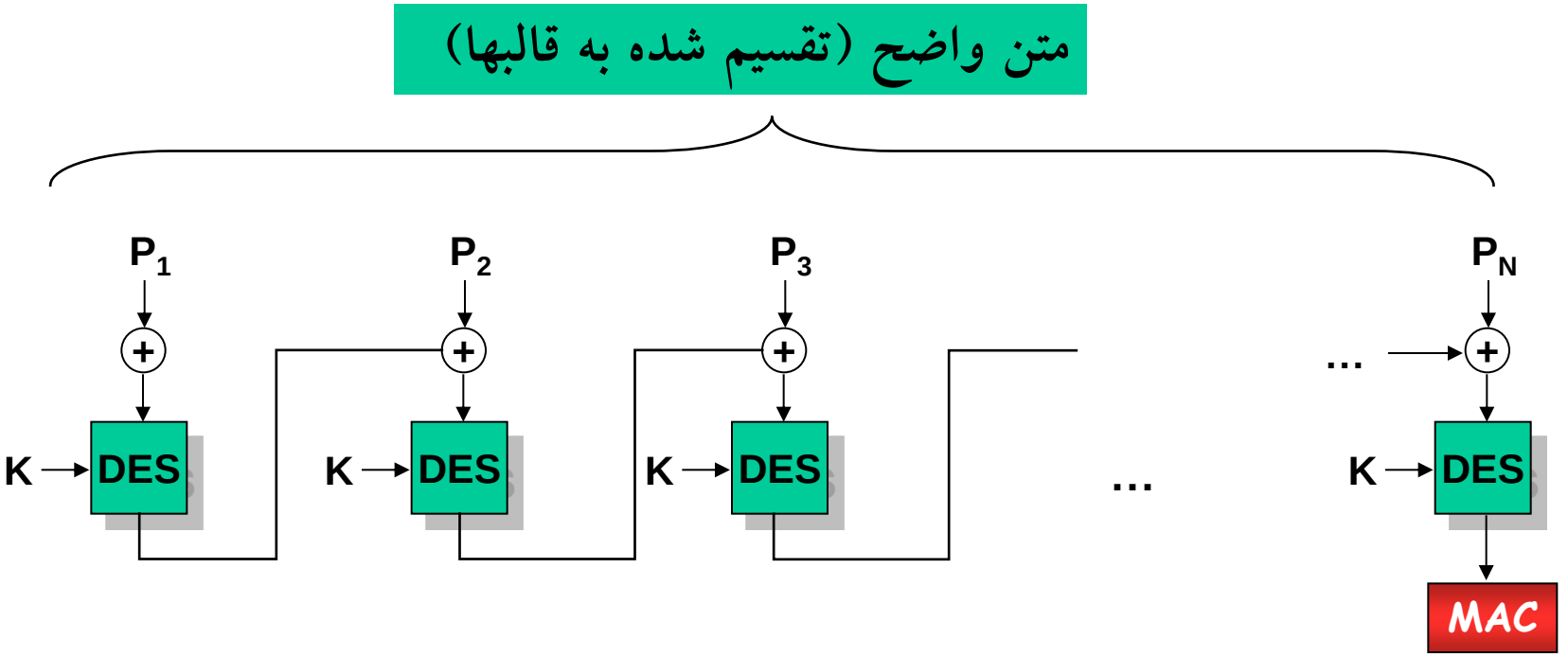


- ویژگیها:
  - هزینه کل « (هزینه رمز نگاری) + (هزینه تهیه MAC)
  - نیاز به دو کلید

کداحراز اصالت پیام DAA

- **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



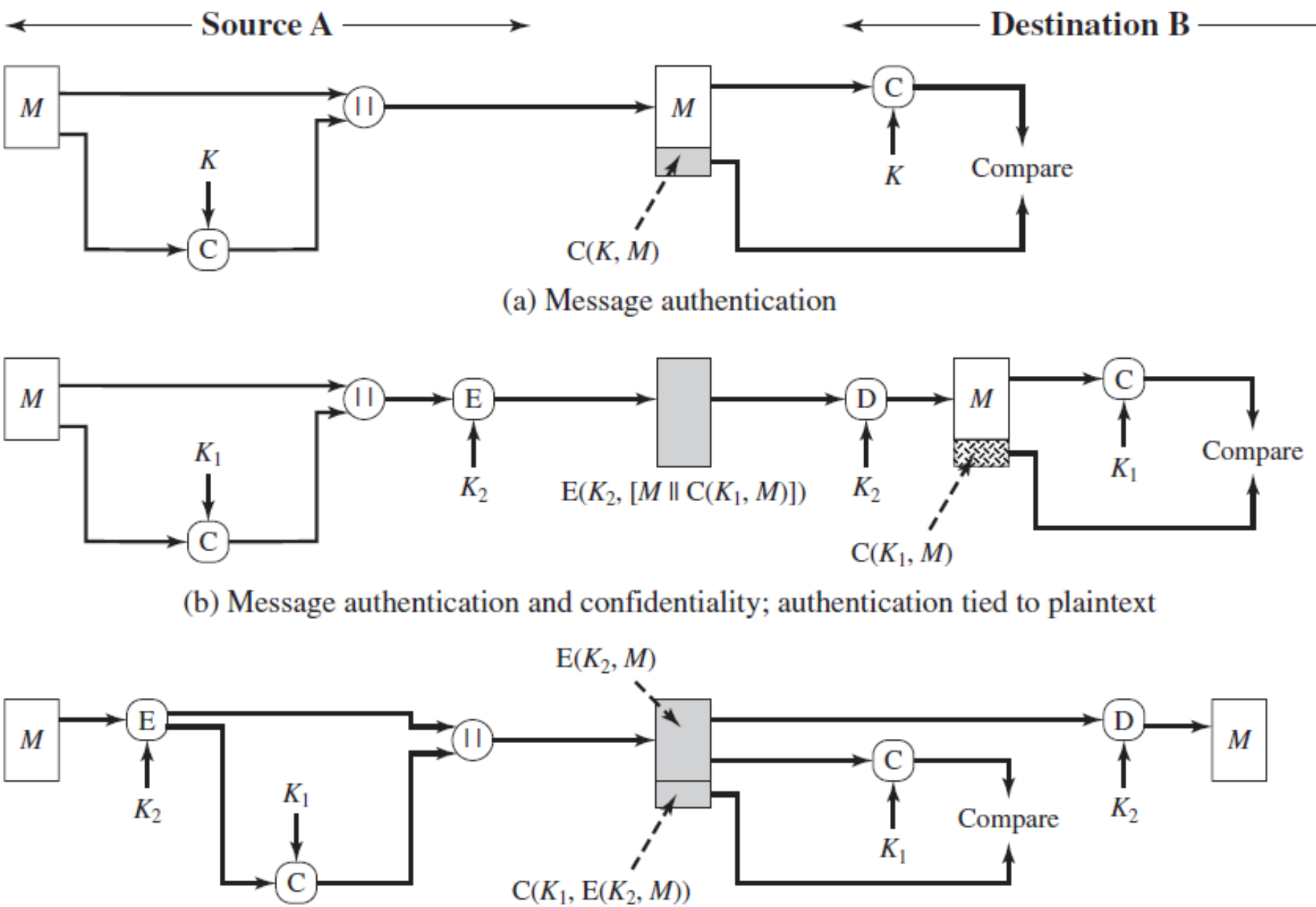


Figure 12.4 Basic Uses of Message Authentication code (MAC)

فهرست مطالب

- مفاهیم اولیه
- رویکردهای ممکن
- کد های احراز اصالت پیام
- اصول توابع درهم ساز
- توابع درهم ساز مهم
- HMAC

توابع درهم ساز

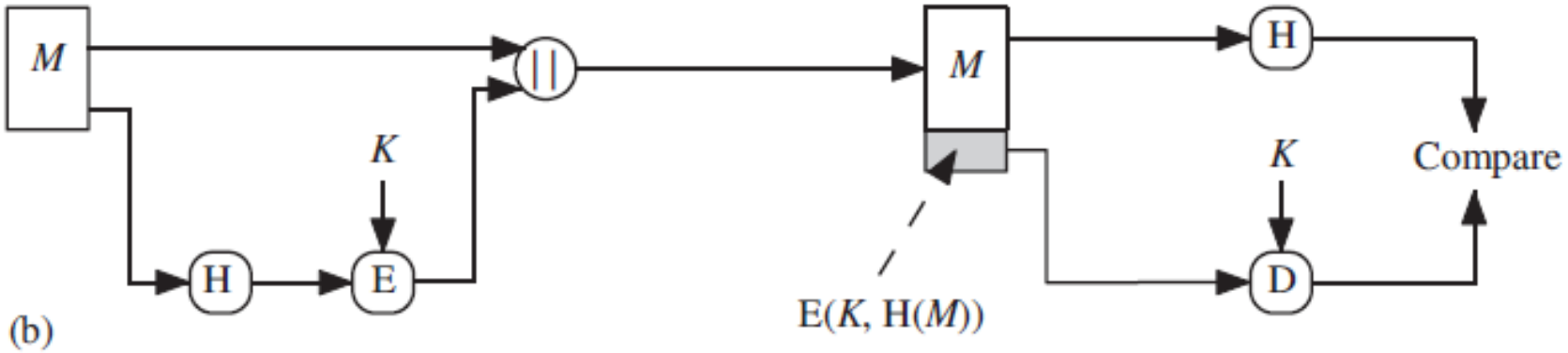
- تابع یک‌طرفه،
- طول ورودی متغیر
- طول خروجی ثابت (نگاشت از فضای بزرگتر به فضای کوچکتر) به گونه ای که:
  - یافتن پیامهای متفاوتی که به یک رشته یکسان نگاشته شوند دشوار باشد.
  - به این رشته عصاره یا چکیده پیام (Digest) میگوییم.
- در حالت کلی، کلیدی در کار نیست!

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 گونه‌ای که H(y) = H(x) از لحاظ محاسباتی ناممکن باشد.

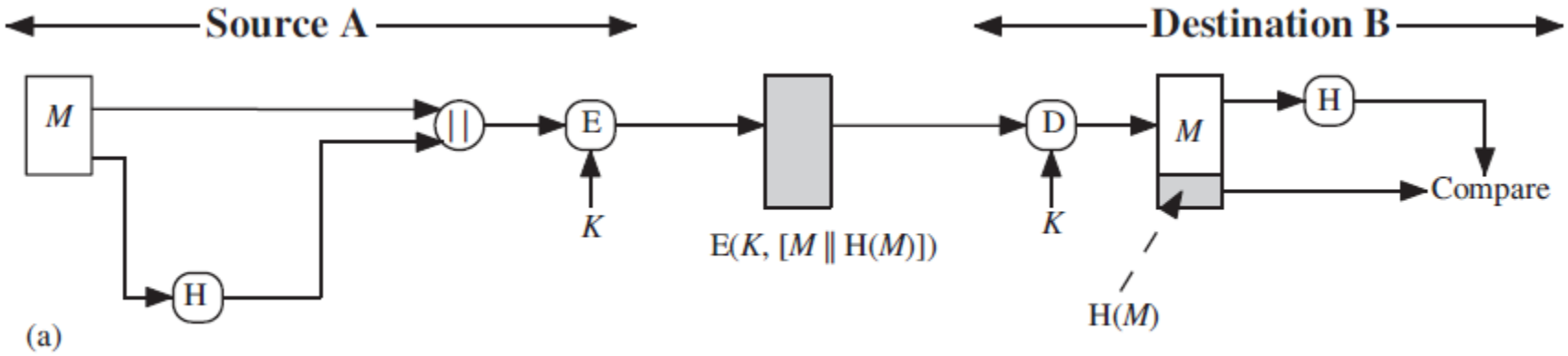
توابع درهم ساز و رمز نگاری متقارن

سرویس صحت:



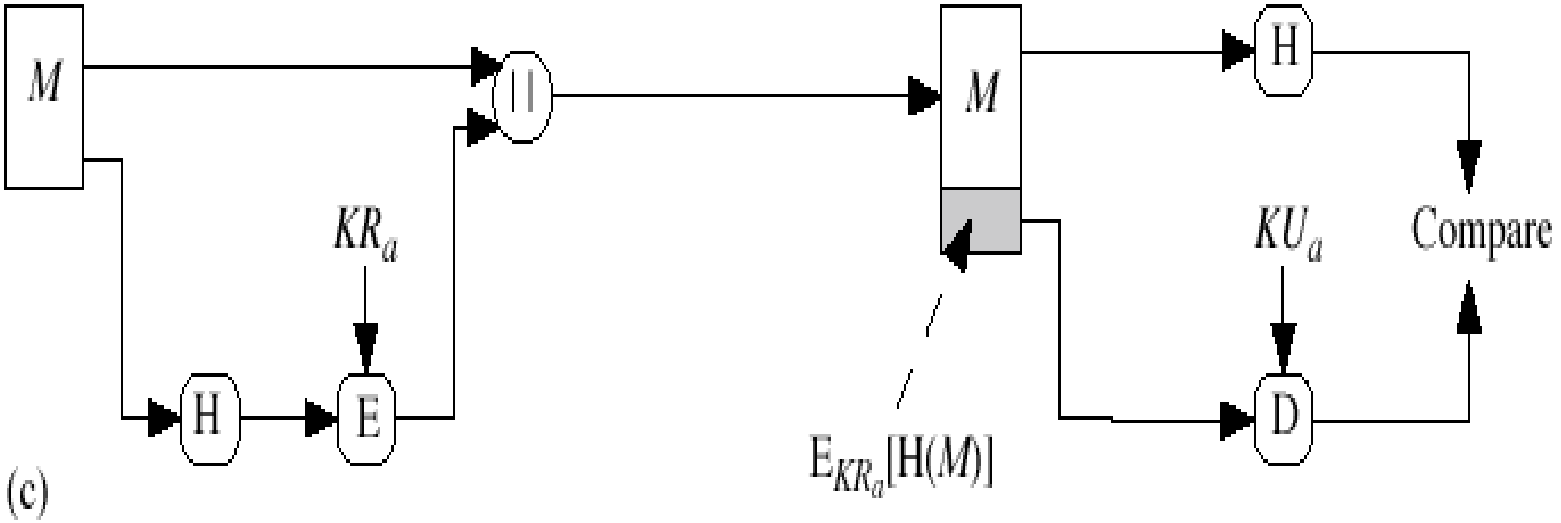
توابع درهم ساز و رمز نگاری متقارن

سرویس محرمانگی و صحت:



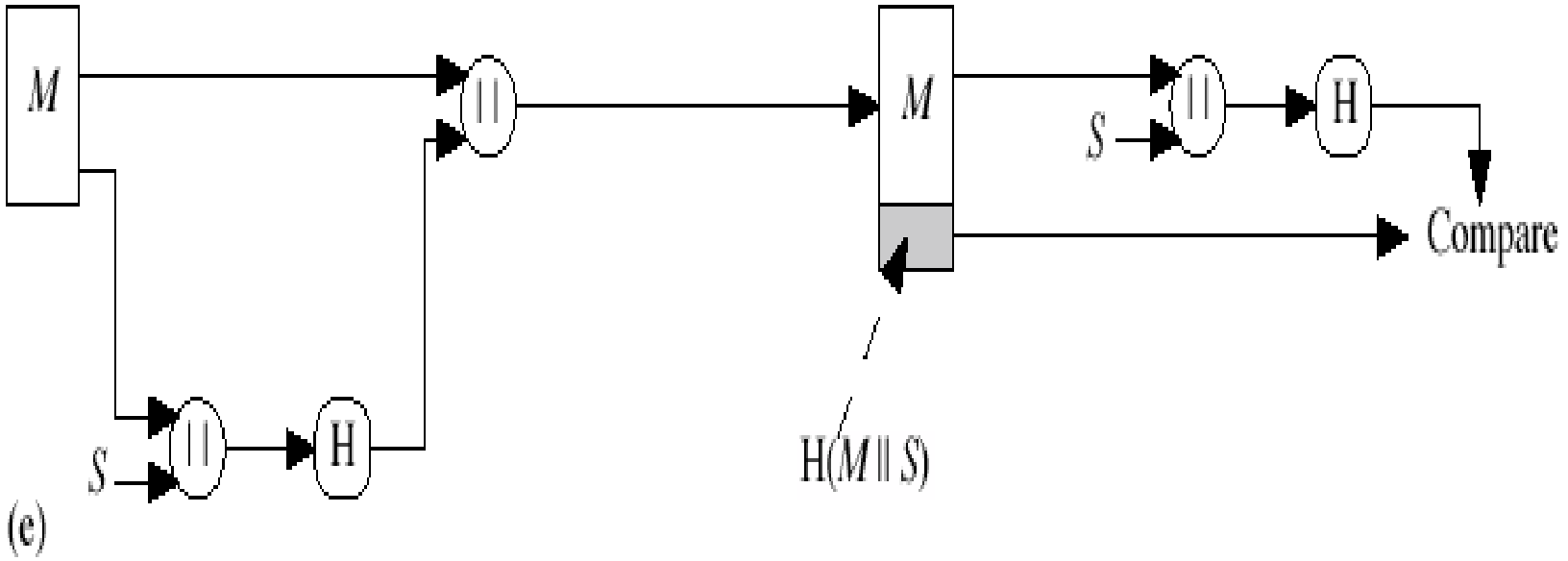
توابع درهم ساز و رمز نگاری نا متقارن

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:

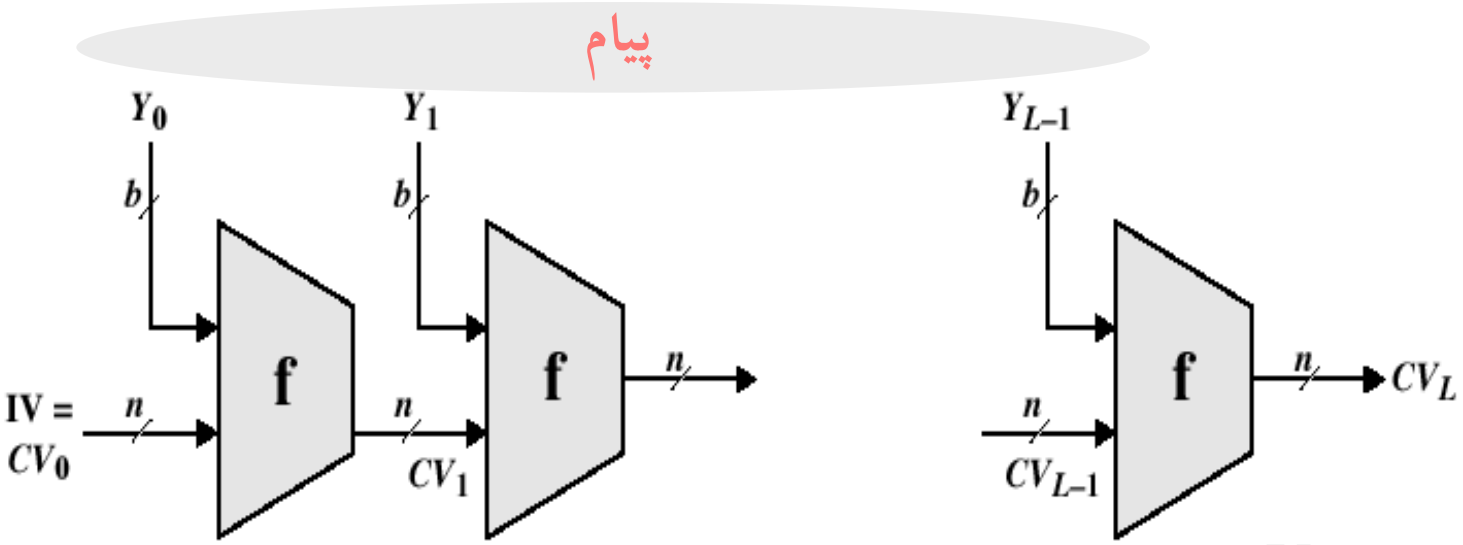
– پیاده سازی نرم افزاری توابع درهم ساز متداول سریعتر از رمزهای قالبی قابل اجرا است.

– دارای هزینه سخت افزاری بیشتر

– کارایی کمتر برای داده های حجیم

– دارای محدودیت‌های صادارتی (Export Control)

ساختار درونی تابع درهم ساز



- 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})

Hash = CV_L

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

فهرست مطالب

- مفاهیم اولیه
- رویکردهای ممکن
- کد های احراز اصالت پیام
- اصول توابع درهم ساز
- توابع درهم ساز مهم
- HMAC

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

- **SHA-1: Secure Hash Algorithm – 1**
  - 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

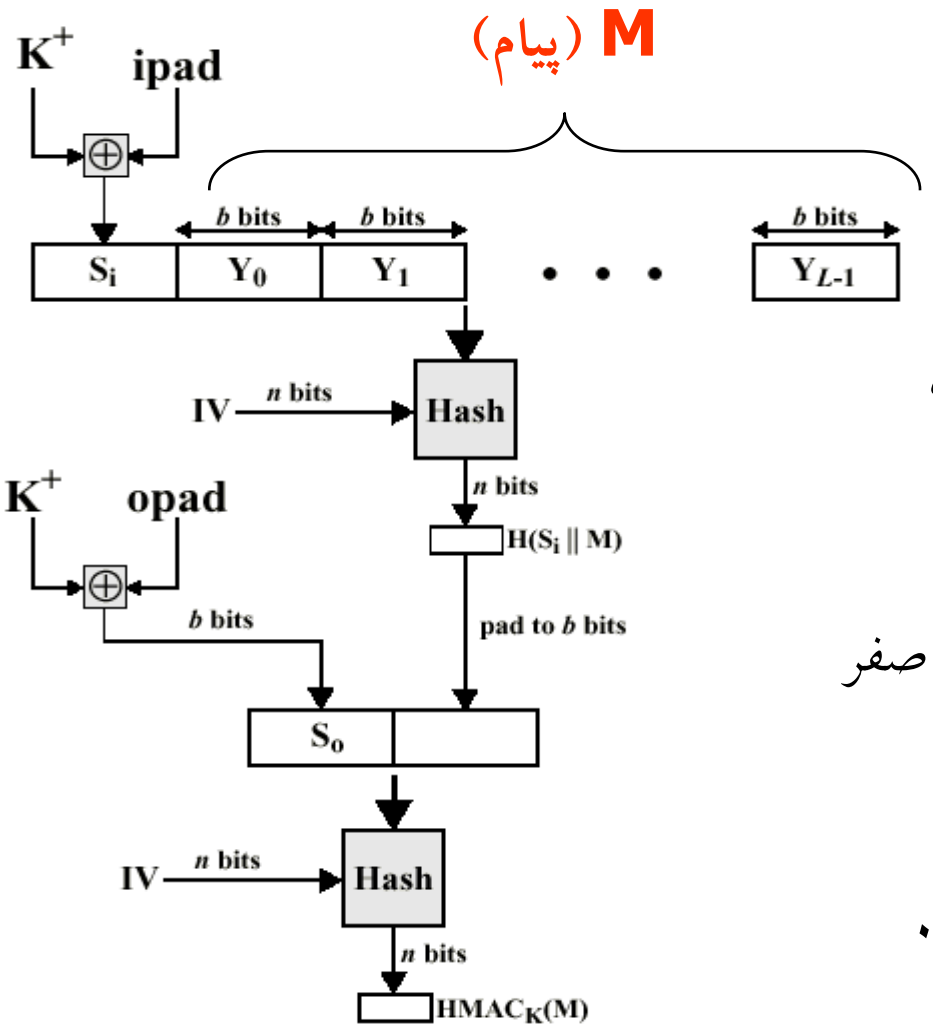
فهرست مطالب

- مفاهیم اولیه
- رویکردهای ممکن
- کد های احراز اصالت پیام
- اصول توابع درهم ساز
- توابع درهم ساز مهم
- HMAC

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

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

Figure 9.10 HMAC Structure

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

Exhaustive Search	آزمون جامع
Tag	برچسب
Packet	بسته
Compression	تابع فشرده ساز
One way Function	تابع یک‌طرفه
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