

امنیت شبکه

محمد مهدی فرح بخش

۱۸ خرداد ۱۴۰۳

به نام خداوند بخشنده مهربان

۱.۰ فصل ۶: کدهای تصدیق صحت پیام

- بعضی وقتا (در برخی کاربردها) صحت اهمیتش بالاتر از محرمانگی
- عملکردها برای تصدیق صحت پیام:
 - یک تابع تولید کننده \leftarrow عامل تصدیق پیام
 - یک تابع واریسی \leftarrow چک کردن عامل تصدیق پیام
- از الگوریتم های رمزنگاری برای تصدیق صحت پیام می شه استفاده کرد اما:
 - کارایی پایین
 - بررسی مفهوم بودن محتوی همواره آسان نیست
 - * نیاز به قالب استاندارد
 - * نیاز به افزونگی
 - * دوشواری خودکار سازی فرآیند تولید و واریسی
- هدف رمزنگاری \leftarrow محرمانگیست نه صحت
- کدهای تشخیص خطا:
 - Parity (CRC-1 bit)
 - * تعداد ۱ ها فرد بود یک دونه ۱ اضافه می کنه
 - CRC-32 bit
 - * قطعات ۳۲ بیتی رو جمع می کنه
- کد تشخیص کلید ندارد \leftarrow برای تشخیص نویز (غیر عمدی و غیر هوشمند) ه حمله دشمن (عمدی و هوشمند) برخلاف امضاء دو طرف قادر به ایجاد MAC هستند.
- ایراد اصلی MAC \leftarrow کارایی پایین
- ویژگی توابع درهم ساز:
 ۱. تابع یکطرفه
 ۲. طول ورودی دلخواه
 ۳. طول خروجی ثابتی
 ۴. کلید در کار نیست \leftarrow برخلاف رمزنگاری و MAC
- یافتن پیام متفاوتی که به یک رشته یکسان نگاشته می شود دوشوار باشد.
 - OW
 - ۲PR
 - CR
- با تست

$$1.25 \times 2^{\frac{n}{2}}$$

\leftarrow احتمال 50% یک تصادم پیدا می شود.

- n : طول خروجی

• تابع f حتما CR باشد.

- با داشتن $H(x)$ برای x های نا معلوم به طول L

$$H(x||pad(x)||L||y)$$

– y : دلخواه

– راه حل:

* طول پیام قطعه اول ؟؟؟؟

* قطعه آخر با تابع H متفاوت

- یافتن پیام متفاوتی که به یک رشته یکسان نگاشته می شود دوشوار باشد.
- یافتن پیام متفاوتی که به یک رشته یکسان نگاشته می شود دوشوار باشد.
- یافتن پیام متفاوتی که به یک رشته یکسان نگاشته می شود دوشوار باشد.
- یافتن پیام متفاوتی که به یک رشته یکسان نگاشته می شود دوشوار باشد.
- یافتن پیام متفاوتی که به یک رشته یکسان نگاشته می شود دوشوار باشد.
- یافتن پیام متفاوتی که به یک رشته یکسان نگاشته می شود دوشوار باشد.

۱.۱.۰ سوال

۱. آیا همیشه محرمانگی مهم است؟
۲. عملکرد های تصدیق صحت پیام کدوما هستند؟
۳. از الگوریتم های رمزنگاری میشه استفاده کرد برای تصدیق صحت پیام؟
۴. هدف رمزنگاری چیست؟
۵. کدهای تشخیص خطا چیا هستند؟
۶. خطای بیرونی و خطای درونی؟؟
۷. کد تشخیص خطا امنه؟ چرا؟ مثال؟
۸. کد های تصدیق صحت پیام
۹. توضیح MAC؟
۱۰. توضیح CBC-MAC؟ حمله؟ راه حل؟ حمله؟ راه حل؟
۱۱. تفاوت MAC با رمزنگاری؟
۱۲. آیا MAC غیرقابل امضا است؟
۱۳. روش های ترکیب MAC با رمزنگاری؟
۱۴. ایراد اصلی MAC؟
۱۵. ویژگی توابع درهم ساز؟
۱۶. امنیت توابع درهم ساز چگونه تامین میشود؟
۱۷. حمله آزمون جامع به Hash؟
۱۸. مرکل دمگارد؟ MD؟
۱۹. عملکرد های تصدیق صحت پیام کدوما هستند؟
۲۰. عملکرد های تصدیق صحت پیام کدوما هستند؟