# امنیت شبکه

محمدمهدی فرح بخش

۱۷ خرداد ۱۴۰۳

به نام خداوند بخشنده مهربان

## ۱.۰ فصل ۶: کد های تصدیق صحت پیام

- بعضی وقتا(در برخی کاربردها) صحت اهمیتش بالاتر از محرمانگی
- عملکرد ها برای تصدیق صحت پیام:
  - یک تابع تولید کننده ← عامل تصدیق پیام
  - یک تابع وارسی ← 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 وارسی
- هدف رمزنگاری ← 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 ← برای تشخیص نویز ( غیر عمدی و غیر هوشمند) ه حمله دشمن (عمدی و هوشمند)
- بعضی وقتا(در برخی کاربردها) صحت اهمیتش بالاتر از محرمانگی
- بعضی وقتا(در برخی کاربردها) صحت اهمیتش بالاتر از محرمانگی
- بعضی وقتا(در برخی کاربردها) صحت اهمیتش بالاتر از محرمانگی
- بعضی وقتا(در برخی کاربردها) صحت اهمیتش بالاتر از محرمانگی
- بعضی وقتا(در برخی کاربردها) صحت اهمیتش بالاتر از محرمانگی
- بعضی وقتا(در برخی کاربردها) صحت اهمیتش بالاتر از محرمانگی

### ۱.۱.۰ سوال

۱. آیا همیشه محرمانگی مهم است؟

۲. عملکرد های تصدیق صحت پیام کدوما هستن؟

۳. از الگوریتم های رمزنگاری میشه استفاده کرد برای تصدیق صحت پیام؟

۴. هدف رمزنگاری چیست؟

۵. کدهای تشخیص خطا چیا هستن؟

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. عملکرد های تصدیق صحت پیام کدوما هستن؟
۱۲. عملکرد های تصدیق صحت پیام کدوما هستن؟
۱۳. عملکرد های تصدیق صحت پیام کدوما هستن؟