Date: ۱۴۰۰/۶/۳۰ راشین احسانی ۹۷۵۲۱۰۱۸ Subject: یادداشت کلاسی

★ امنیت از دیدگاه NTST

← حفاظت از یک سامانه اطلاعاتی خودکار

↓

برای دست یابی به

↓ ↓ ↓

دسترس پذیری یکپارچگی محرمانگی

↓

availability integrity confidentiality

برای اینکه سیستم امن باشد ← باید در این چارچوب باشد

برای جلوگیری و پاسخ دادن به حملات سایبری به زیرساخت های شرکت

★ در گذشته ← امنیت ← فقط محرمانگی ← آشکار نبودن داده برای افراد غیرمجاز

← به مرور ← یکپارچگی و دسترس پذیری اضافه شدند

← فعالیت هایی که می نیستند ← یک سری الزامات دیگه نیاز داریم

★ منابع سامانه { سخت افزار / نرم افزار / اطلاعات / داده و مخابرات

★ Intel ← برداشتن داده بدون اجازه کاربر ← چین ← پرداز شکر

No-Intel

★ تفاوت داده و اطلاعات

↓

← از پردازش داده بدست می آید

تمام

★ مدل یک سیستم امنیت:

فرستنده → کانال → آسیب
دریافت کننده ← باب
کانال ↓ ایو ← شنود می‌کند

- اصل محرمانگی ← اطمینان از عدم در دسترس بودن داده‌های خصوصی برای افراد غیرمجاز.
  ← از موارد نقض ← شکسته شدن ماشین انیگما

★ امنیت ← مبتنی بر نداشتن کلید نه الگوریتم ← الگوریتم در نهایت لو خواهد رفت

★ یکپارچگی داده ← اطمینان از قابل تغییر بودن اطلاعات فقط توسط افراد مجاز
  ← سامانه ← انجام عملیات سامانه به صورت عادی
  ← کسی نتواند بدون اجازه تغییر دهد
  ← دعاری از دستکاری غیرمجاز

★ دسترس پذیری ← اطمینان از عملکرد بالا و بلادنگ برای کاربران مجاز
  ← real-time ← زود ✗
  دیر ✗
  ← به موقع انجام شود

Date: / /　　　　Subject:

* اولین هدف در امنیت ← رمزنگاری ← تنها ساز و کار امنیت ولی مهمترین است
← محرمانگی

* شانون از نوابغ حوزه رمزنگاری
قبل از شانون - بعد از شانون

* cryptography ← قدمت هزاران ساله
نوشتن محرمانه

* هیروگلیف ها ← جغد ← A
شاید ← هدف رمزنگاری نبوده
بیشتر جذابیت ← هدف

* Atabash ← A B C ..... Z
به جای A ← حرف آخر
" " B ← یکی مونده به آخر

* رمزنگاری آرشیلوس ← نوشتن پیام روی کاغذ ← پیچیدن دور یک استوانه با قطر معین ← تنها راه فهمیدن پیام ← داشتن استوانه

* نخستین الگوی مدون رمزنگاری ← سزار

Date: / / Subject:

* سزار ←

A B C D E
= ↑
↳ ۳ حرف جلوتر

* مدل یک سامانه رمزنگاری

ناامن
t
باب ⟷ کانال ⟷ آلیس
↓
ایو

متن اصلی
↑
- آلیس Plain text را برای باب می‌فرستد که رمزشده

- آلیس با استفاده از الگوریتم E و با قرار دادن ورودی M و کلید K
↳ خروجی → C → cypher text
متن رمزشده

$C = E_k(m) = (m+k) \bmod 26$ → سزار
↳ $E_3(T) = (20+3) = 23 \rightarrow W$

* رمزنگاری ← آلیس ← encryption
رمزگشایی ← باب ← decryption

← نباید خیلی پیچیده باشد
↳ کار ایو نباید سخت باشد ← ولی

Date: / /

Subject:

* cryptanalysis ← تحلیل رمز ← روش های رمزشکایی بدون داشتن کلید

* cryptology ← رمزنگاری + تحلیل رمز ← رمزشناسی