

* امنیت از دیدگاه NTIST

له حفاظت از یک سامانه اطلاعاتی خودکار

↓
پرای دست یابی به

↓
محرمانگی یکپارچگی دسترسی پذیری

↓
availability integrity confidentiality

برای اینکه سیستم امن باشد ← باید در این جا خوب باشد

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

* در گذشته امنیت فقط محرمانگی و کنترل ورودن دیتا برای افراد غیر مجاز

له به مرور به یکپارچگی، دسترسی پذیری اضافه کردند

له فعالین ها کامی نیستند به یک سری الیمان دیتا نیاز داریم

سخت افزار

نرم افزار

* منابع سامانه

اطلاعات / داده، مخابرات

No-Intel

↑

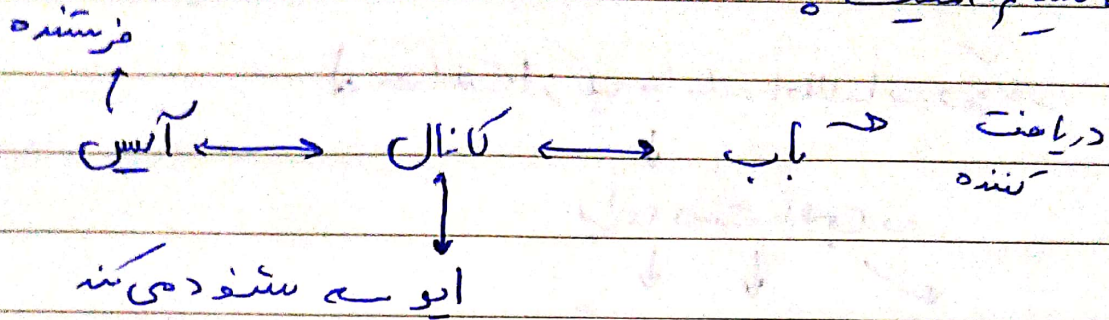
* Intel → داشتن دیتا بدون اجازه کاربر به چین → پردازشگر

* تفاوت دیتا و اطلاعات

↓
از پردازش دیتا بدست می آید

خام

• مدل یک سیستم امنیت :



• اصل محرمانگی : اطمینان از عدم دسترسی بودن داده های خصوصی

برای افراد غیر مجاز

لح از موارد نفوذ : سیستم امن ماسکین انلیس

• امنیت : مبتنی بر نداشتن کلید نه الگوریتم به الگوریتم در نهایت
لوحه اهرت

• یکبارگی : داده به اطمینان از قابل تغییر بودن اطلاعات فقط توسط
افراد مجاز

لح سامانه
انجام عملیات سامانه به صورت عمادی
دعاری از دستکاری غیر مجاز
کسی نتواند بدون اجازه تغییر دهد

• دسترسی پذیری : اطمینان از عملکرد بلادرنگ برای کاربران مجاز

زود x real-time

دیر x

لح به موقع انجام شود

* اولین هدف در امنیت رمزنگاری - تنها سازندگان و لی
 له مرمانی است
مدرستین است

* شانوں از نوابغ حوزه رمزنگاری
 قیل از شانوں - بعد از شانوں

* Cryptography - قدمت هزاران ساله
 نوشتن مرمیانه

* هیولایف ها - بعد از A
 سابه هدف رمزنگاری نبوده
 بستر جدایت هدف

* Atabash - A B C Z
 له ب جای A - حرف آخر
 " B - لکی موده به آخر

* رمزنگاری آرشیلووس - نوشتن پیام روی کاغذ ریچوندن دوریکه استوانه

با قطر معین - قضا راه مرمین پیام - داشتن استوانه

* نخستین الگوی مدون رمزنگاری - سزار

A B C D E
 =
 ۳ حرف جابجیا

* سزار ←

• مدل کد سامانه رمزنگاری

نام امن
 باب ← کمال ← آیس
 ↓
 اید

متن اصلی

↑
 - آیس Plain text، برای باب می فرستد به رمز شده

- آیس با استفاده از الگوریتم E، یا قرار دادن ورودی M و کلید K

cypher text → C → فرجهی
 متن رمز شده

سزار → $C = E_k(m) = (m+k) \text{ mod } 26$

↳ $E_3(T) = (20+3) = 23 \rightarrow W$

Encryption ← آیس

* رمزنگاری ←

Decryption ← باب

رمزگشایی ←

• بنابر ضمیمه صفحه

باب

کار ایو باب
 مستند باب

Date:

/ /

Subject:

* Cryptanalysis سے تھیل رمز سے روش های رمزنگاری بدون

داشتن کلید

* رمزنگاری + تھیل رمز سے رمزنگاری cryptology