Date: ۱۴۰۰/ ۹/ ۷ Subject: یادداشت کلاسی راشین احسانی ۹۷۵۲۱۰۱۸

* شرط الگوریتم های کلید نامتقارن ← حل مشکل حمله مرد میانی

له نیاز به احراز هویت کلید عمومی

* راه حل ← مراجع صدور گواهینامه

له شخص ثالث ← هم آلیس هم باب قبولش دارند

* PKI

له public key Infrastructure

له مجموعه ای از سخت افزار، نرم افزار، سیاست و دستورالعمل

له برای مدیریت کلید های عمومی

له جهت رمزنگاری کلید عمومی، توزیع گواهینامه و...

* ابطال گواهینامه ← تا یک زمانی اعتبار دارد.

* ایده دیگر برای جایگزینی CA ← Web of trust

له وب اعتماد

له غیرمتمرکز

انجمنی از کاربرها اعتبار چیزی را تأیید یا تکذیب می کنند.

له اولین بار استفاده در PGP

Date: / /

Subject:

* اجزای PKI ← کلید عمومی
کلید محرمانه
CA
فروشنده گواهی نامه
لیست ابطال گواهی نامه
ماژول امنیت سخت افزار

* CA ← عمومی یا خصوصی

* فقط یک CA ← X ← باید ساخته شود

له سلسله مراتب چند سطحی اعتماد

له از نصیره گواهی نامه

* Root CA → self-signed

Sign → intermediate Intermediate

cert cert cert

Date: / /

Subject:

* تفاوت Privacy و security؟

← پنجره داریم. میله هم می‌گذاریم ← دزد نمی‌تواند وارد شود

← security ✓

← ولی همچنان دید دارند ← privacy نداریم

← پرده می‌کشیم ← privacy ✓

* تا مدت‌ها امنیت ← CIA

← با گذشت زمان ← مفاهیم جدیدی

حریم خصوصی، گمنامی، انکارناپذیری، freshness و ...

← data oriented ← محتوا دیتا ?

context oriented ← حواشی دیتا ← کی، کجا، توسط

* دیتا داخل لایه کاربرد ← رمز شده است ← TLS

* در لایه انتقال ← پورت یک ردی از برنامه را در اختیار ما می‌گذارد

← برای اینکه نفهمیم ← انتخاب پورت‌ها بر تصادفی

* در اپلیکیشن یک ~~...~~ اثر منحصر به فردی در هدر لایه انتقال می‌گذارد

← قابل فهمیدن با سیستم‌های هوش مصنوعی

iman NOTEBOOK

Date: / /

Subject:

* DPI , SPI ← لایه انتقال ← برای طبقه‌بندی ترافیک

A