

Date: ۱۴۰۰/۹/۷

Subject: یادداشت کلاسی رایتین احسانی ۹۷۵۳۱۰۱۸

* شرط گلویتیم های کدی ناستقارن به حل مشکل صدر دستانی

له نیاز به اهراز هویت کدی عمومی

* راه حل به راجع صدر گواهی نامه

دارند

له شخص ثالث به هم آکس هم باب قبولش

PKI *

Public Key Infrastructure

له مجبور ای از سخت افزار، نرم افزار، سیاست و دستور العمل

له برای مدیریت کدی های عمومی

له جهت رمزنگاری کدی عمومی و توزیع گواهی نامه و ...

* ابطال گواهی نامه به تارک زمانی اعتبار دارد.

* ایده دیگر برای جابیزینی CA به Web of trust

له وب اعتماد

له غیر متمرکز

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

له اولین بار استفاده در PGP

Date: / /

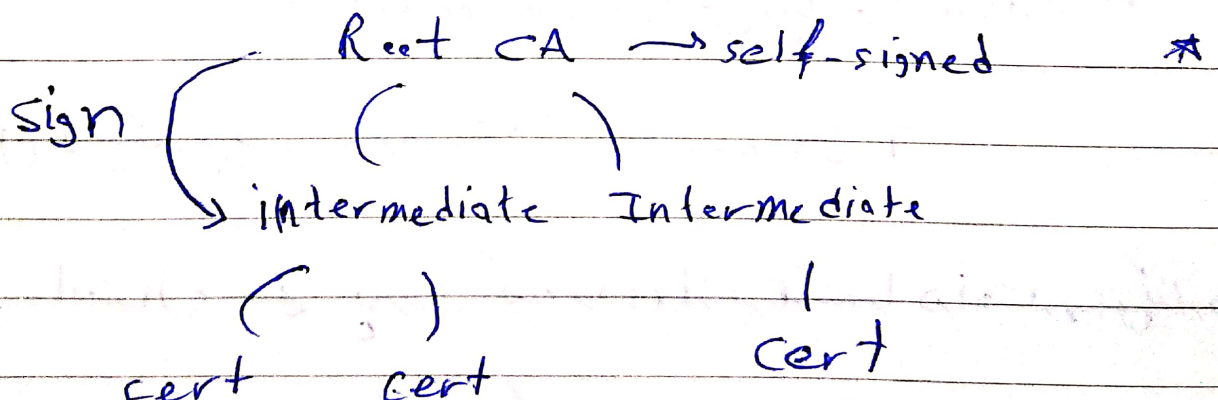
Subject: _____

* اجزای PKI و کلمه عمومی
کلمه خصوصی
CA
فروستگاه گواهی نامه
سیاست ابطال گواهی نامه
ساختار امنیت سخت افزار

* CA به عمومی یا خصوصی

* فقط یک CA به X به نام مشکل می شود

به واسطه رابطة چند سطحی اعتماد
به نفع غیره گواهی نامه



* تفاوت Privacy, Security ?

له پنجره داریم . میله هم میگذاریم چه در دزد نمی تواند وارد شود

✓ security

له دزدی نمی تواند دید داشته باشد

privacy نه داریم

✓ privacy

* تاهمت ها به امنیت CIA

له با گذشت زمان به مفاهیم جدیدی

حریم خصوصی، گمنامی، انکار پذیری، Freshness

data oriented به محتوا دیتا

context oriented به حواسی دیتا به کی، کجا، توسط

* دیتا داخل لایه کاربرد به رمز شده است TLS

* در لایه انتقال به پورت یک ردی از برنامه را در اختیار همای ندارد

له برای اینکه تضمین به انتخاب پورت نامبر تصادفی

* در ارتباطی یک ^{اثر} منحصر به فردی در هر لایه انتقال می گذارد

له قابل فهمیدن با سیستم های هوش مصنوعی

Date:

/ /

Subject:

* SPI, DPI به لایه انتقال به برای طبقه بندی ترافیک

A