Date: ۱۴۰۰/۹/۱۴ یادداشت کلاسی - ۹۷۵۲۱۰۱۸ Subject: راستین احسانی

* شبکه همراه ← stream cipher ← احتیاج به تقسیم کلید

* call امنه ← یعنی چی؟ ← رمز شده است

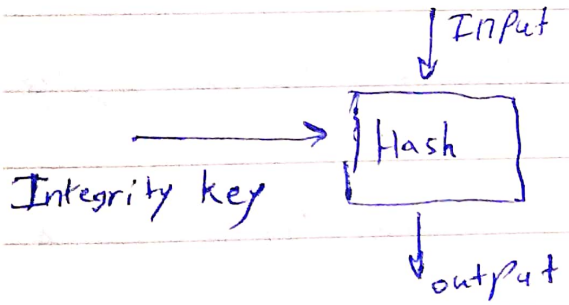
* رمز کردن با hash ← اگر hash همراه پیام باشد

← پیام را می‌توانه تغییر دهد

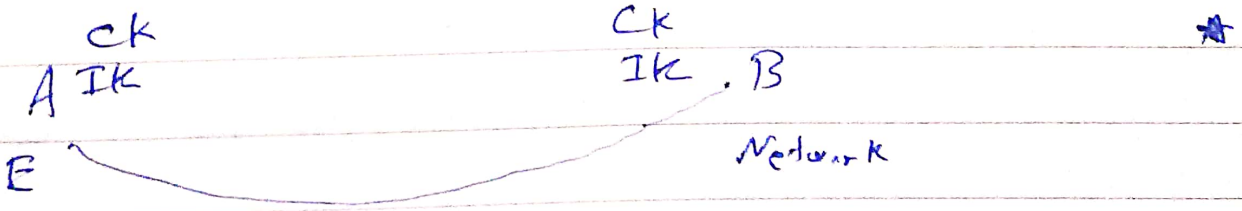
← بین ← hash را جداگانه در کانال

این نفرستیم

* در کانال ناامن چطور؟ ← استفاده از hash های کلید دار



کلید را نداشته باشه ← X outputX



* ارتباطات ← end-end ← این X

← از من تا شبکه ، از شبکه تا دریسلم

Date: / /

Subject:

* تلفن ← نیاز به ← { Ck, Ik } ← { encryption, integrity }

* اگر Ik, Ck لو برود ← تمام اطلاعات ←

forward
backward

لو می‌رود

* هر Session ← Ck, Ik خودش

* مشترکان ← 1) سیم‌کارت

UE ← گوشی + سیم‌کارت

2) گوشی ← جزا از سیم‌کارت

mobile equipment ← ME

AuC (۳

* هر سیم‌کارت ← شناسه unique

* مرکز ارزش اصالت ← AuC

* هر AuC = هر سیم‌کارت باید پشت این باشد.

* سیم‌کارت ← خلی high-tech

* RAN ← آنتن‌ها وجود دارند

* ارتباط از طریق هوا

Date: / / Subject:

* تا وقتی ارتباطات باسیم بود همه چی اوکی بود

* تا حدی Core خیلی کارا انجام می دهد

له تقسیم وظایف RAN با Core ارتباط با هسته رادیویی سرویس دهی

* کنش Core نسبت به درخواست سرویس ؟

له باید ارزش اضافه بیشتر شود