Date: ۱۴۰۰/۱۰/۵ راستین احسانی ۹۷۵۲۱۰۱۸ Subject: یادداشت کلاسی

* شناسه ای که کاربر برای شبکه می فرستد؟ ← IMSI

↓

فرستادن به AuC

چرا AuC؟

به همه است بستی بر کلید

یک کپی در کارت ما

یک کپی در AuC

* مستقیم به ما نمی دهد X ← غیر ناک است

استفاده از پارامترهای واسطه

* AuC هر اپراتور از هم جداست

* توابع F_1 تا F_5 ← توابع Milenage

* f_1 تا f_5 ← ورودی K , RAND

عدد رندوم

* تولید Ak , Ik , Ck , XRES , MAC و ارسال به Core

↑

AuC

Date: / /

Subject:

$AUTN = SQN \oplus Ak \| AMF \| MAC$ *

* ارسال RAND, AUTN به کاربر

* چگونه بفهمیم AUTN اصل است؟ ← MAC را چک کنیم.

↳ verify MAC = XMAC

* بعد از آن کاربر جواب RES را برای شبکه می‌فرستد

* در سنل ۲ ← احراز هویت یک طرفه بود

مقایسه با RES تولید شده توسط خودش

که فقط کاربر احراز می‌شد

* از سنل ۲ به بعد ← ۲ طرفه

* کپی از سیمکارت؟ ← خللی ایجاد نمی‌کند.

که مثل کارت شناسایی است

که بعد از سنل ۲ این اتفاق خللی کم رنگ شده است

Date: / / Subject:

* در تلفن همراه سه تأمین امنیت با رمز

integrity و

Ik , Ck ← متناظر به ۲ کلید

* عملیات رمزنگاری و integrity

در گوشی انجام می شود

پس Ck , Ik از سیمکارت به گوشی

می رود

integrity ندارد

* مثل ۲ ← encryption ← بین گوشی و RAN

* مثل E و D ← encryption / integrity ← بین گوشی و RAN / بین گوشی و شبکه

* با کدام انتخاب الگوریتم می توانه رمز بشود؟ ← چیز چون هنوز کاربر

الگوریتم را نمی داند

integrity چی؟ ← می شود