جلسه ۷ -

۱۴ ذی القعده ۱۴۴۱ | 6 Jul 2020 | ۱۶ | دوشنبه | تیر | ۱۳۹۹

پیام‌های پرداخت الکترونیکی این :

رمزنگاری : روشی برای حفاظت در برابر انواع حملاتی است که ممکن است بررسی ارتباطات بین دو نقطه روی دهد.

(در رمزنگاری هدف شنود حملات و محافظت در مقابل آن است)

* در حوضه رمزنگاری اصطلاحاتی هستند که باید به آن پرداخته شود.

رمزنگاری در رمزنگاری : (plaintext , cleartext)
متن اولیه — متن شفاف

(متنی که راحت قابل دیدن است و قرارات با رمزنگاری برای هرکسی قابل plaintext _ cleartext مشاهده نباشد)

* پیغامی که توسط انسان قابل خواندن باشد

رمزنگاری :

* فرایند تغییر یک پیغام به گونه‌ای که اجزای تشکیل دهنده آن مخفی بماند را

توسط انسان قابل خواندن نیست ولی با استفاده از رمزنگاری و پیغام حاصل از این کار را ciphetext می نامند. الگوریتم ها قابل خواندن می شود

* رمزنگاری متن cipher را به عنوان ورودی دریافت می کند و متن رمزنده

قابل خواندن برای انسان

plain text اصلی را بازیابی می کند.

P = plaintext

C = ciphertext

الگوریتم رمزگذاری

C = E(P) → تابع رمزنگاری E روی P عمل می کند تا C تولید شود

P = D(C) → تابع رمزگشایی D عمل می کند تا P تولید شود.

(۷۴)

* الگوریتم رمزنگاری (یا همان رمز نگاری): یک تابع ریاضی که برای رمزنگاری و رمزگشایی استفاده می‌شود.

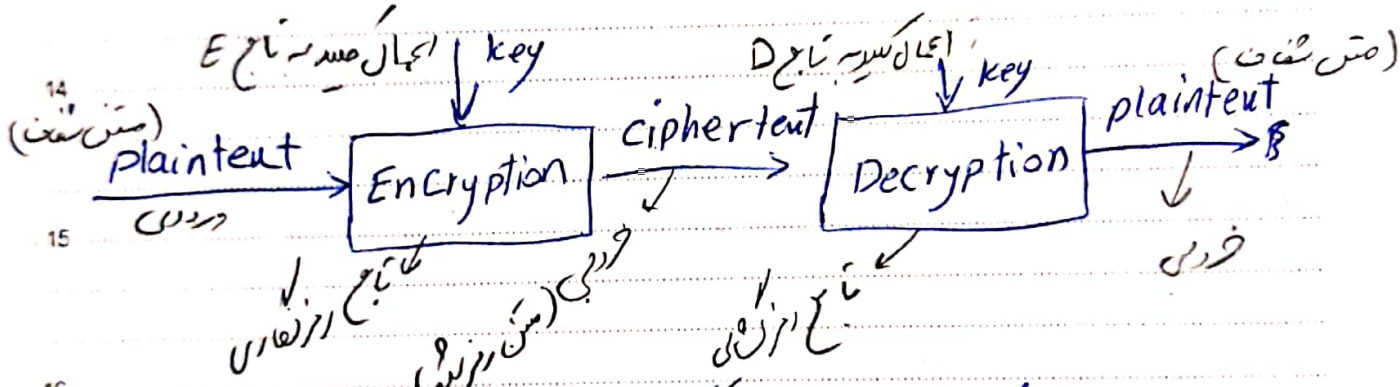
* تمامی الگوریتم های رمزنگاری جدید از یک کلید استفاده می‌کنند که با K نشان داده می‌شود.

* مقدار این کلید توابع رمزنگاری و رمزگشایی را تحت تاثیر قرار می‌دهد.

$$E(k,p) = C \qquad \begin{pmatrix} C = E(P) \\ P = D(C) \end{pmatrix}$$

$$D(k,C) = P$$

اگر از کلید استفاده نکنیم توابع مقابل به صورت روبرو تغییر می‌کند و کلید K در آن موثر خواهد بود.



* هدف اصلی رمزنویسی (یا همان نگاری) این است که متن اصلی از افراد متخاصم پنهان بماند (امنیت متن حفظ شود)

* کشف رمز (cryptanalysis) علم بازیابی متن اصلی بدون داشتن (کشف رمز بدون کلید اضافی) می‌شود

هیچ دانشی در مورد کلید نباید داشته باشد.

کلید رمزنگاری

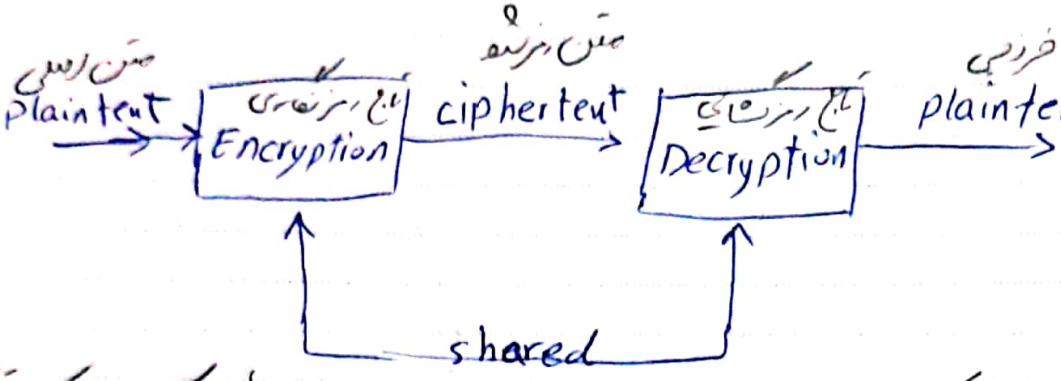
* الگوریتم رمزنگاری باید به گونه‌ای باشد که با کشف رمز و جود داشته باشد

بازیابی برای کشف رمز طولانی باشد

رمزنگاری ← متقارن ← رشته و کلید هر دو مشترک استفاده می‌شود
نامتقارن ← رشته و کلید یکی عمومی و خصوصی

۱۸ چهارشنبه تیر ۱۳۹۹ — 8 Jul 2020 — ۱۶ ذی القعده ۱۴۴۱

* رمزنگاری متقارن: رمزنگاری متقارن بدان
می گفته هر دو طرف شرکت کننده در یک ارتباط باید
در ابتدا یک کلید محرمانه در اختیار داشته باشند.



کلید مشترک متقارن) Semmetric key ← عملکرد سیستم رمزنگاری متقارن

* رمزنگاری متقارن شیوه‌ای برای درهم سازی اطلاعاتی است که ارسال می‌شود به
گونه‌ای که افرادی که قصد مشخص دارند نتوانند این اطلاعات را درک و دیباریابی کنند.

* همیشه هدف این نیست بلکه حتی سوابق هدف ارسال در پشت اطلاعات روی (پیغام)
شبکه مورد تایید قرار گیرد که یک راه برای ارسال صحیح پیغام روش خلاصه
سازی است که از توابع هش استفاده می‌شود یک پیغام طولانی را خلاصه می‌کند.

روی شبکه قرار داده و می‌توان کلید محرمانه را روی هش اعمال کرد
و نتیجه را روی شبکه اعمال کرد.

روز ادبیات کودکان و نوجوانان

تفاوت hash در رمزنگاری : hash یک طرفه است و بعد از hash می‌توان به حالت اولیه برگرداند ولی در رمزنگاری متن رمزشده می‌تواند به حالت قبل (اول) برگردد.

۱۹ پنجشنبه تیر ۱۳۹۹ — 9 Jul 2020 — ۱۷ ذی القعده ۱۴۴۱

* خلاصه سازی پیغام با هش کردن :

* در بسیاری از موارد هیچ کدام از درستی پیغام مورد نیاز می‌باشد.

* یک راه برای تضمین درستی پیغام بدون نیاز به رمزنگاری استفاده از تکنیکی است که به عنوان خلاصه سازی پیغام شناخته می‌شود

* این کار شامل اعمال تابع هش یا خلاصه سازی روی یک پیغام طولانی و تولید یک پیغام خلاصه شده (کوتاه) می‌باشد.

* گیرنده می‌تواند بررسی این هش را اعمال کرد و نتیجه را به همراه پیغام بررسی شده تحلیل کرد.

۲۰ جمعه تیر ۱۳۹۹ — 10 Jul 2020 — ۱۸ ذی القعده ۱۴۴۱

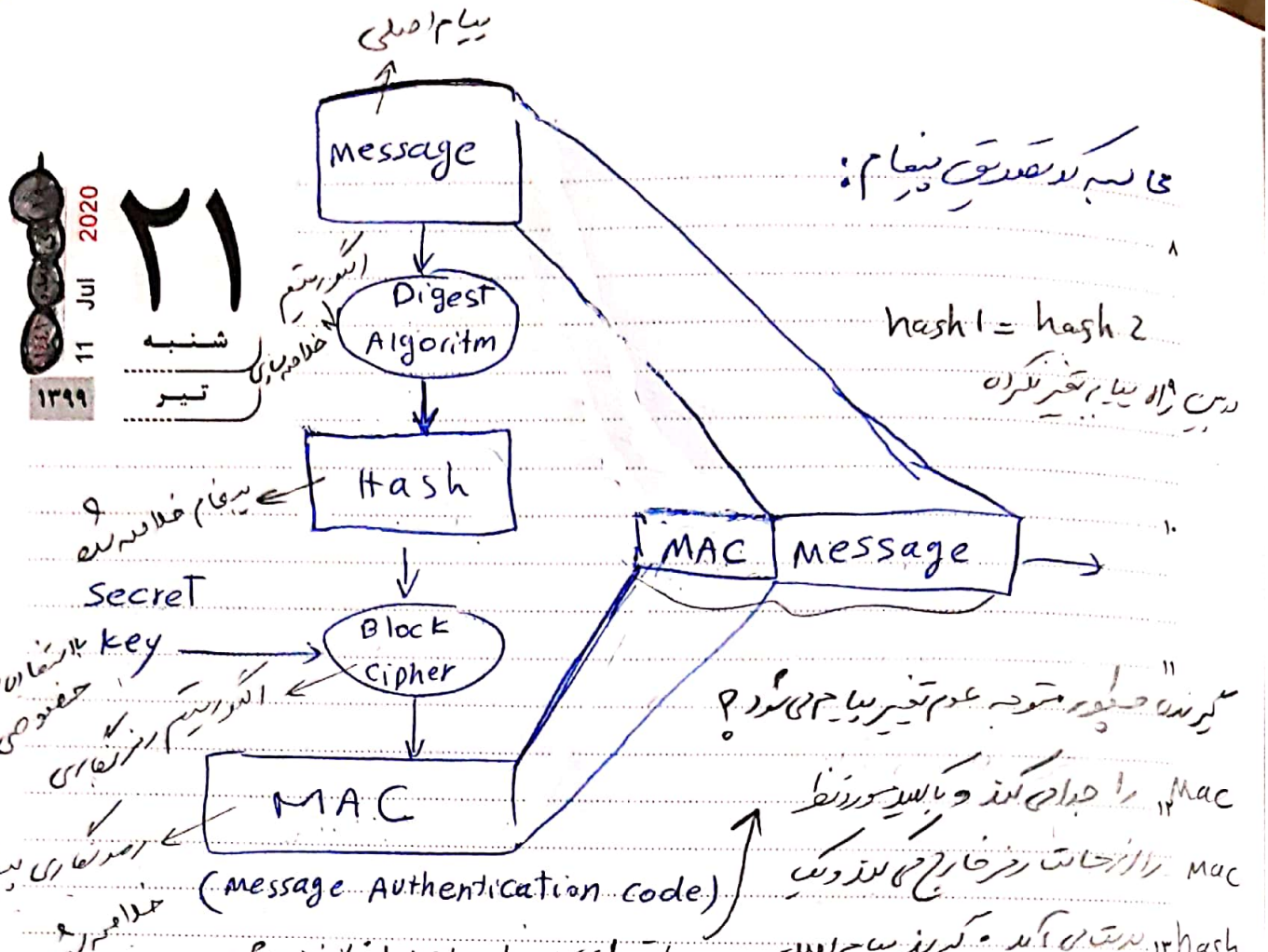
* سپس هش رمزنگاری می‌شود تا تبدیل به یک کد تصدیق پیغام (MAC) گردد که قابل انتقال به پیغام ضمیمه است.

→ به فایل اصلی ضمیمه می‌شود

* وقتی پیغام رسید دریافت کننده هش پیغام را با استفاده از الگوریتم رمزنگاری محاسبه می‌کند.

* اگر مقدار دریافت آمده با MAC رمزگشایی شده که به همراه پیغام رسیده است انطباق داشته باشد بدین صورت مطمئن خواهیم شد که پیغام در راه تغییر نکرده است.

۲۱ Jul 2020 — ۱۱ تیر ۱۳۹۹ — شنبه



نحوه کد تصدیق پیام:

۸ hash 1 = hash 2

دریافت پیام تغییر نکرده

۹ گیرنده حدس متوجه عدم تغییر پیام می‌شود؟

۱۰ MAC را جدا می‌کند و با کلید مورد توافق

۱۱ MAC را از حالت رمز خارج می‌کند و یک

۱۲ hash بدست می‌آید. گیرنده پیام اصلی

۱۳ ① hash هم گیرنده یک hash بدست می‌آید

② دو hash را با هم مقایسه می‌کند

۱۴* رمزنگاری نامتقارن یا کلید عمومی:

---

۱۵ * مشکل سیستم های رمزنگاری متقارن این است که قبل از این که هر ارتباطی

۱۶ رخ دهد؛ هر دو عضو شرکت کننده باید یک کلید مشترک را به دست آورند،

مشکل معرفی کلید بین هر دو طرف گیرنده و فرستنده است.

۱۷ * در رمزنگاری کلید عمومی (نامتقارن) هر فرد یک جفت کلید را در اختیار

۱۸ دارد که کلید عمومی و خصوصی نامیده می‌شود.

۱۹* کلید عمومی به طور گسترده منتشر می‌شود و همه می‌توانند آن را در اختیار داشته

باشند اما کلید خصوصی محرمانه است و هرگز آشکار نمی‌شود.

روز غفاف و حجاب

۲۲ یکشنبه تیر ۱۳۹۹ — ۲۰ ذی القعده ۱۴۴۱ — 12 Jul 2020

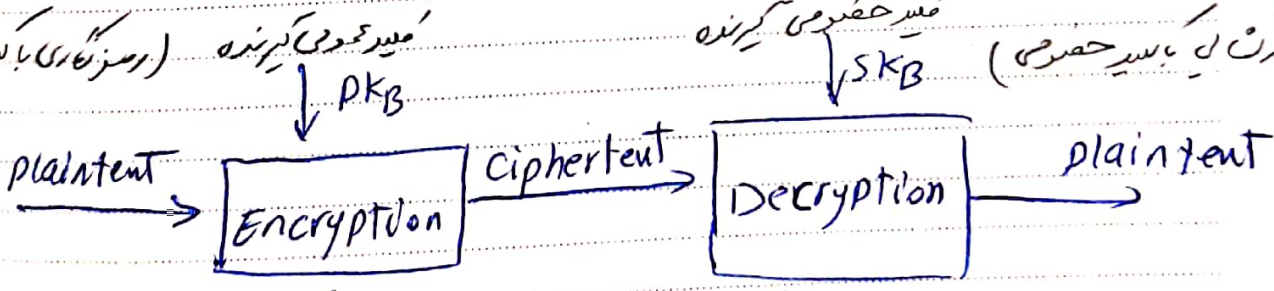
* فرستنده از کلید عمومی گیرنده استفاده می‌کند تا پیام را رمزنگاری کند.

* سپس گیرنده از کلید خصوصی خود (SKB) استفاده می‌کند تا پیام را رمزگشایی کند.

* هرکس که به کلید عمومی گیرنده دسترسی داشته باشد می‌تواند کلید پیام رمزشده را برای او ارسال کند اما هیچ کس بجز دریافت کننده نمی‌تواند آن را رمزگشایی کند.

* در این شیوه اگر از روی پیام M اعمال کنیم و سپس از روی Publickey از روی Secret Keey نتیجه حاصل اعمال کنیم نتیجه‌ای همان M یا پیام اصلی است بنابراین با داشتن PK عمومی و SK خصوصی می‌توانیم رمزگشایی و رمزنگاری را انجام دهیم.

* کلید خصوصی نباید به هیچ وجه آشکار باشد و قابل پیدا کردن نباشد.



* سیستم رمزنگاری نامتقارن (کلید عمومی)

(۸۱)

۲۱ ذی القعده ۱۴۴۱
۲۳ Jul 2020
دوشنبه
13 تیر
۱۳۹۹

مکانیزم دیگری که برای ترکیب این دو توضیح می دهیم:

* امضای دیجیتال و پوشش پیام

- تصدیق پیام مورد توجه می باشد (از نرم مورد تأیید ارسال شده است)

- راه حل: یک خلاصه پیام را با استفاده از الگوریتم های مانند MD5 و SHA را محاسبه کند و سپس کلید خصوصی فرستنده را روی آن اعمال کند.

- مقدار حاصل را می توان به عنوان امضای دیجیتال در نظر گرفت و قبل از انتقال به پیام ضمیمه می شود (این امضا اعتبار فرستنده را تأیید می کند)

- در مقصد گیرنده از الگوریتم های یکسانی برای تولید خلاصه پیام استفاده می کند و با استفاده از کلید عمومی فرستنده تأیید می کند که خلاصه پیام ما به شده با امضای رمزگشایی شده یکسان است.

انطباق داده و از فرستاده معتبر ارسال شده

- در صورت انطباق گیرنده می تواند مطمئن شود که پیام از فرستنده صحیح تأیید نشده است و در طول انتقال تغییر نکرده است.

روز گفت و گو و تعامل سازنده با جهان

۸۲

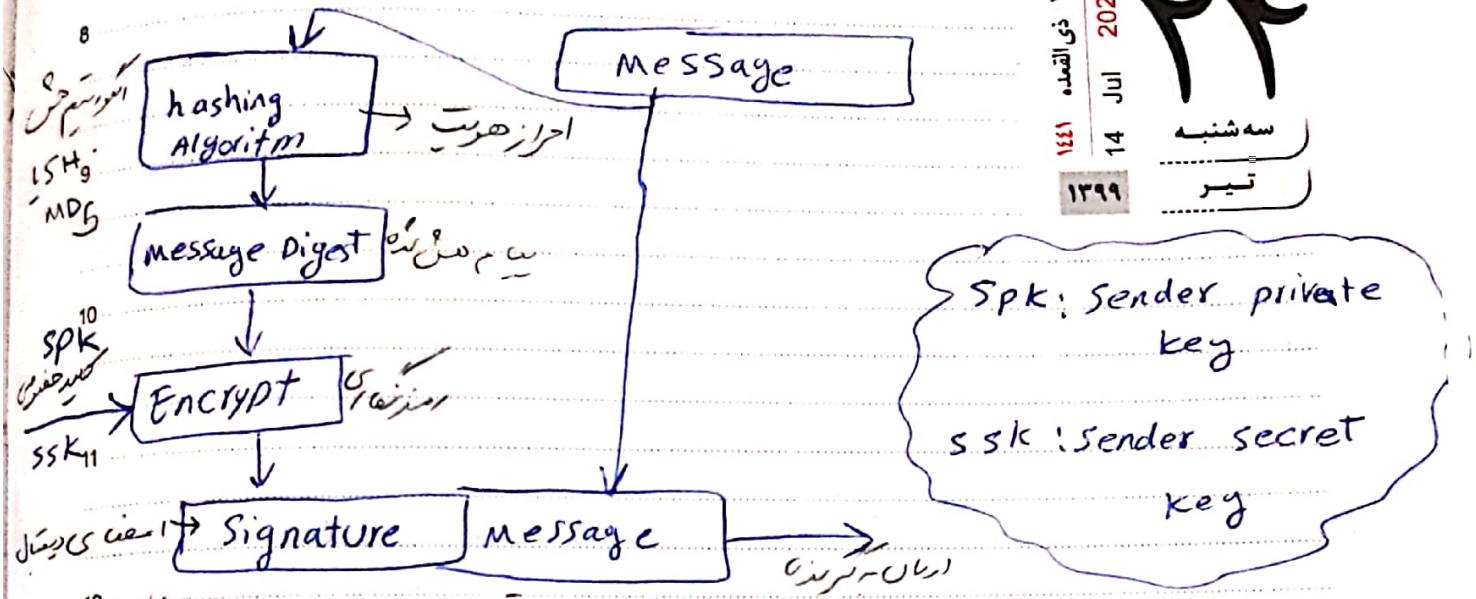
۲۴ سه‌شنبه تیر ۱۳۹۹ | ۲۳ ذی‌القعده ۱۴۴۱ | 14 Jul 2020

— اطمینان از اینکه فرستنده همان شخص هست که منتظرش بوده ایم؟

* امضا را از حاصل رمزخارج می‌کند با استفاده از کلید عمومی فرستنده و سپس hash بدست آمده از طرف

پیام اصلی را هم hash می‌کنیم اگر این دو hash برابر شد فرستنده احراز هویت و تأیید میشود

* امضا نه تنها امضای دیجیتال به پیام متن را انتقال



امضای دیجیتال به ابتدای پیام اصلی اضافه می‌شود

* اگر نیاز به محرمانگی پیغام داشته باشیم باید پیغام پوشانده شود.

* برای رسیدن به هدف، فرستنده می‌تواند یک کلید را به طور تصادفی تولید کند و می‌تواند از این کلید پیغام به همراه یک الگوریتم رمزنگاری سریع برای رمزنگاری پیغام استفاده کند.

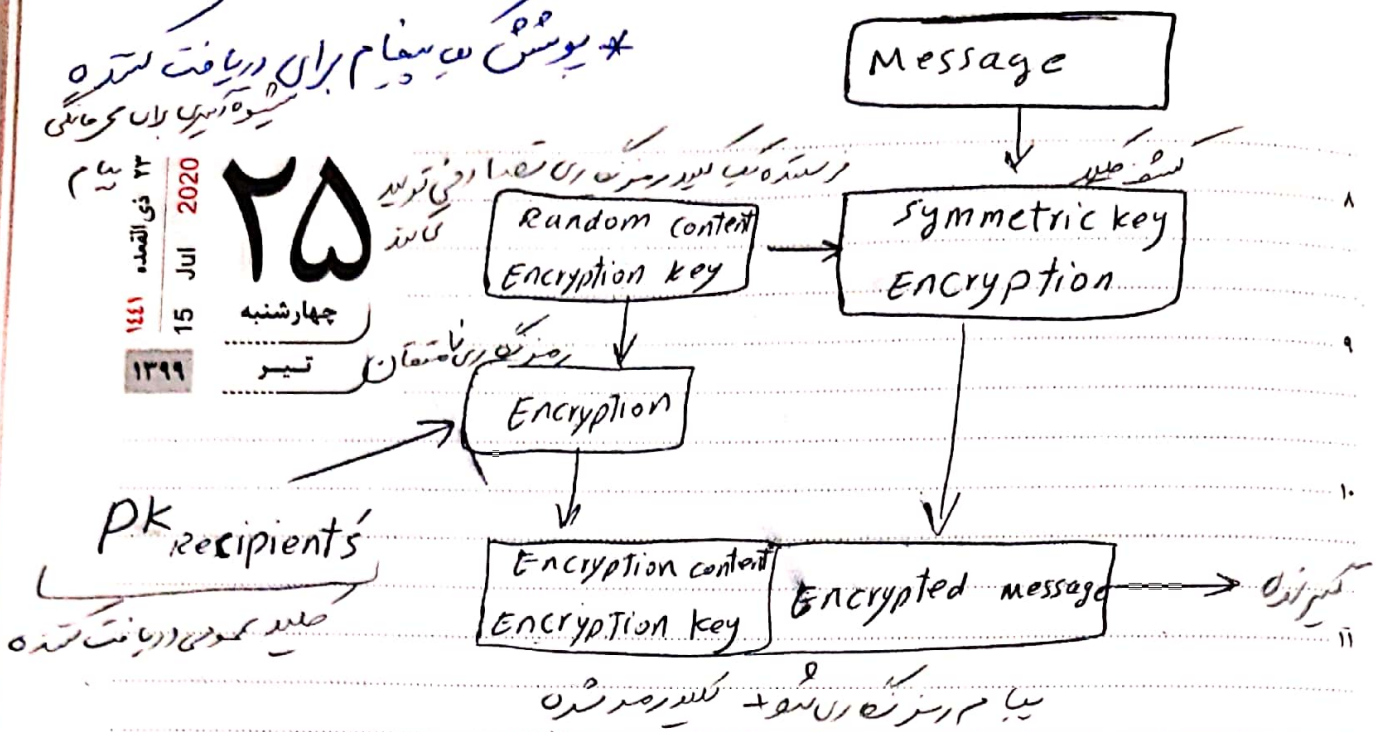
* برای ارسال کد پیغام به دریافت کننده این کلید با استفاده از کلید عمومی (کلید تصادفی) دریافت کننده رمز می‌شود و به پیغام ارسالی ضمیمه می‌شود.

* وقتی پیغام رسید دریافت کننده از کلید خصوصی اش استفاده می‌کند تا کلید رمزنگاری را بدست آورد در این صورت وی این امکان را به دست می‌آورد تا متن دریافت شده را به صورت خوانا تبدیل کند.

۸۳

* پوشش یک پیام برای دریافت کننده

۲۳ ذی القعده ۱۴۴۱ | 15 Jul 2020 | چهارشنبه ۲۵ تیر ۱۳۹۹



کلید عمومی دریافت کننده

پیام رمزنگاری شده + کلید رمز شده

* پروتکل های پرداخت الکترونیکی:

پروتکل SET : الکترونیکی پرداخت کارت اعتباری ۴ چهار عضو اصلی در مزاندکارت اعتباری وجود دارد.

عضو اول: مالکی که عضو انجمن کارت ممکن است به عنوان صادر کننده کارت ابزار پرداخت

با کسب درآمد یا مشتریانشان عمل کند.

- این کار شامل ارائه یک کارت یا نگهداری حساب کارت اعتباری برای افراد می باشد که به وسیله آن بتوانند تراکنش های ارسال شده از سوی آن ها را مدیریت کند.

۲۶ پنجشنبه تیر ۱۳۹۹ | ۲۴ ذی القعده ۱۴۴۱ | 16 Jul 2020

عضو دوم: بانک دریافت کننده به عنوان دریافت کننده برای مشتریان پایانه‌ای که می‌خواهند پرداخت های کارت اعتباری را دریافت کنند عمل می‌کند.

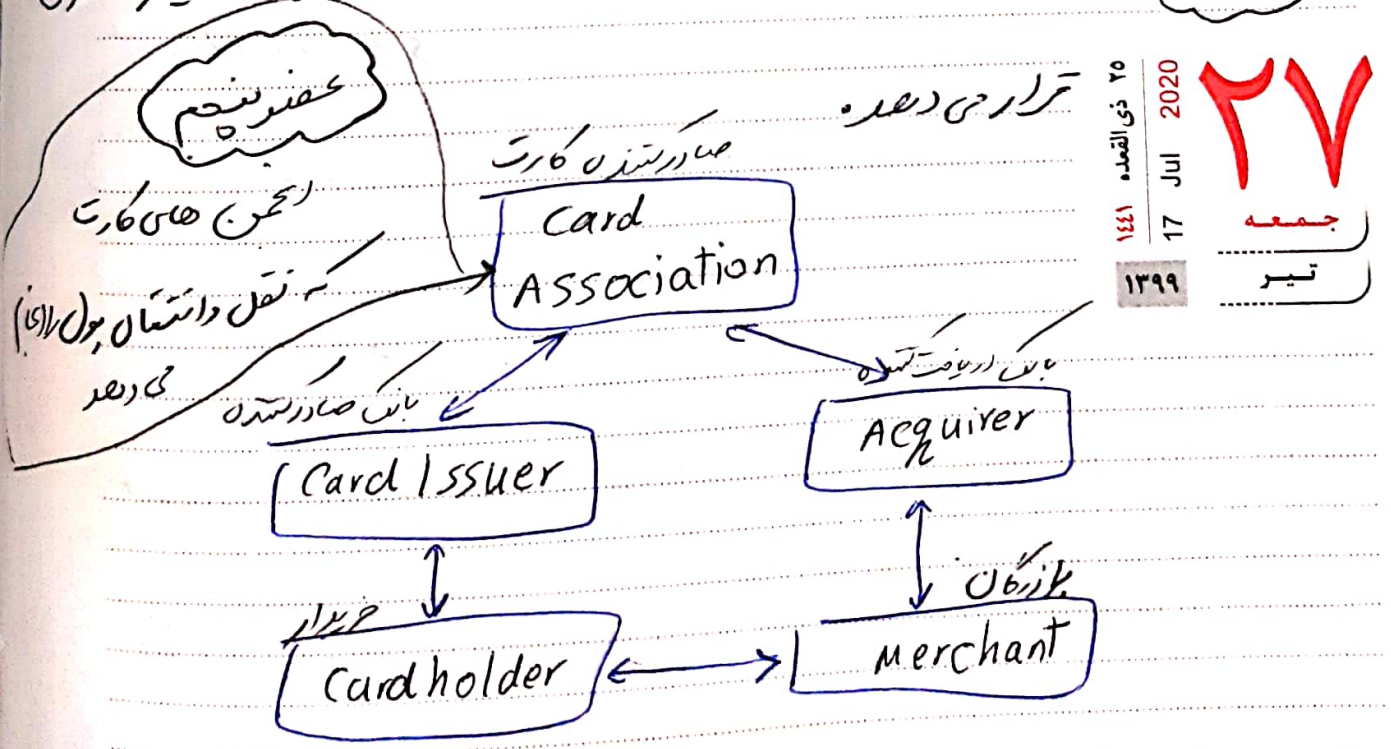
- این کارشامل تهیه تجهیزات و یا نرم افزاری است تا پرداخت های رخ داده در محل بازرگان را پردازش کند.

عضو سوم: خریدار: فردی که دارای کارت اعتباری است و خریدهای خود را از بازرگان انجام می‌دهد.

عضو چهارم: بازرگان: همان فروشنده (merchant) است که محصولات را در اختیار مشتری قرار می‌دهد.

۲۷ جمعه تیر ۱۳۹۹ | ۲۵ ذی القعده ۱۴۴۱ | 17 Jul 2020

عضو پنجم: انجمن های کارت که نقل و انتقال پول را (از طریق بانک صادرکننده) می‌دهد



+ نهادهای موجود در فرایند پرداخت کارت اعتباری

۸۵

۲۸ شنبه تیر ۱۳۹۹ — ۲۶ ذی القعده ۱۴۴۱ — 18 Jul 2020

پروتکل های پرداخت ikp :

مربوط در پرداخت سپهر

- ikp خانواده ای از پروتکل های پرداخت اعین می باشد که به

دسته IBM توسعه داده شده اند.

- پروتکل های ikp برحسب رمزنگاری کلید عمومی می باشند و تفاوت آن ها در

تعداد شرکایی است که حق های کلید عمومی آن را در اختیار دارند.

- سنیر یا را با اعداد ۱ و ۲ و ۳ جایگزین می کنیم و ikp ۱ و ikp ۲ و ikp ۳ بدست می آید

امن تر از بقیه

ikp ۱ : برحسب زیرساخت امنیتی است که تقریبا امروزه وجود دارد.

ikp ۲ و ikp ۳ : نسخه توسعه یافته ikp ۱ می باشند که در آن ها زیرساخت های

احراز هویت

تصدیق پیچیده تری استفاده می شود.

هرچند تعداد بخش هایی که حق های کلید عمومی را دارا هستند بیشتر باشد

سطح امنیت بیشتر می شود

سطح امنیت تهیه شده و روی آن پیچیدگی الگوریتم هم افزایش می یابد.

- در حال حاضر تاکید اصلی این پروتکل ها بر روی پرداخت های کارت

اعتباری می باشد.

۱۶

۲۹ یکشنبه تیر ۱۳۹۹ — ۲۷ ذی القعده ۱۴۴۱ — 19 Jul 2020

نهادهای شرکت کننده در این سیستم عبارتند از:

پرداخت ikp

① خریداران

② بازرگانان

③ بانک بازرگان: به عنوان دریافت کننده شناخته می شود زیرا برگه شارژ کاغذی را از بازرگان دریافت می کند.

④ بانک خریدار: با نام صادر کننده شناخته می شود زیرا کارت های اعتباری را برای کاربران صادر می کند.

⑤ نهاد پایاپای که عملیات تسویه مالی را انجام می دهد (انتقال صادره پایاپای)

* بانک دریافت کننده به عنوان درگاهی بین اینترنت و شبکه های مالی موجود که تراکنش های بین بانک ها را پشتیبانی می کند عمل می کند.

پرداخت خرید نیست

* پرداخت های ikp تنها برای تراکنش های پرداخت استفاده می شوند و نسبت به فرایندی که نیاز به تبادل مالی انجام دهند حساس هستند و به قبل و بعد آن کاری ندارند

* بخش های اصلی شرکت کننده در تراکنش عبارتند از:

A → درگاه دریافت کننده

C → مشتری

M → بازرگان

۸۷