مرکز صدور گواهی دیجیتال

زیرساخت کلید عمومی

Public Key Infrastructure

شرکت خدمات انفورماتیک
راهبر انفورماتیک
وابسته به وزارت دادگستری
Raahbar Informatic Services Co.

مرکز صدور گواهی دیجیتال
www.mocca.ir

فهرست

- انواع تجارت
- لازمه تجارت امن
- انواع حملات اینترنتی
- سرویس های امنیتی
- رمزنگاری
- الگوریتم های متقارن
- الگوریتم های نامتقارن
- توابع درهم سازی
- امضاء دیجیتال
- گواهی دیجیتال
- مرکز صدور گواهی
- دفتر ثبت نام
- گواهی SSL
- مروری بر گواهی ثبت سفارش

انواع تجارت

- تجارت سنتی

- تجارت الکترونیک

فهرست

تجارت سنتی

در روش سنتی؛ مکتوب بودن، اصل بودن و ممهور بودن یک سند دلیل وجود اعتبار آن است. طرفین به طور حضوری با هم مذاکره و اسناد را امضا می کنند.

فهرست

تجارت الکترونیک

- اما در تجارت الکترونیک امکان برگزاری جلسات حضوری وجود ندارد. طرفین نمی توانند با روشهای سنتی از صحت ادعاها و اسناد اطمینان حاصل کنند.
- پس باید به دنبال راهی بود تا در فضای سایبر(مجازی) نیز بتوان به مبادلهٔ اطلاعات اتکا نمود. برای این منظور باید به امنیت ارسال و دریافت اطلاعات به عنوان یک فاکتور اساسی توجه کرد.
- مفهومی که از امنیت تبادل داده‌های الکترونیکی به ذهن می رسد، باید شامل فرآیندی باشد که همهٔ عناصر اصلی تشکیل دهنده مبادله را کامل و مطمئن محافظت نماید.

فهرست

تجارت الکترونیک – ادامه

دریافت کننده باید اطمینان حاصل کند که:

فرستنده همان فرد مورد نظر است و این امر غیر قابل انکار باشد و از طرف دیگر مطمئن شود که اطلاعات پس از ارسال بواسطهٔ دسترسی غیر مجاز و یا نفوذ در آن تغییری بوجود نیامده است. از نظر فرستنده نیز این موارد دارای اهمیت هستند.

فهرست

فرآیند احراز هویت

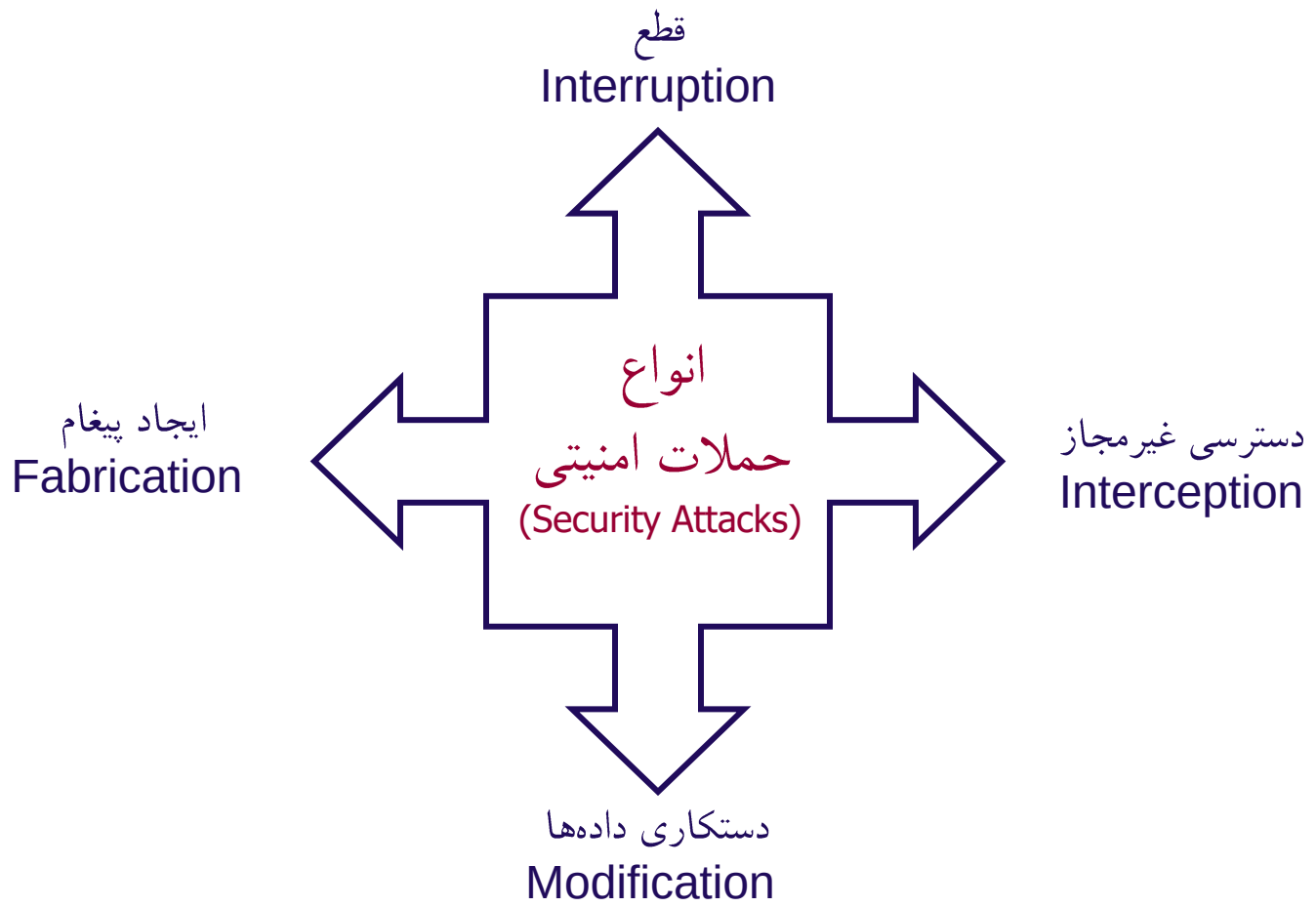
- احرازهویت در تجارت سنتی
  - شناسنامه، پاسپورت،گذرنامه، گواهینامه رانندگی، امضاء ...

- احرازهویت در تجارت الکترونیک
  - گواهی دیجیتال، امضای دیجیتال

لازمه تجارت امن

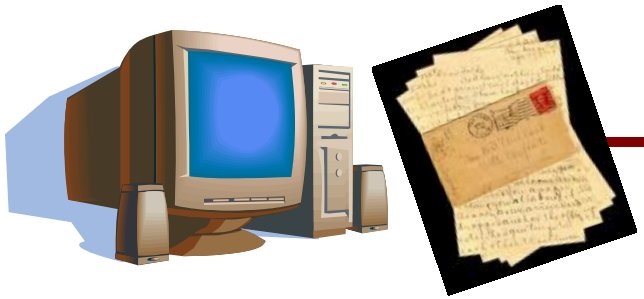
- جلوگیری ازحملات امنیتی (Security Attacks)
- تامین سرویسهای امنیتی (Security Services)
- استفاده ازسازوکارهای امنیتی (Security Mechanism)

فهرست

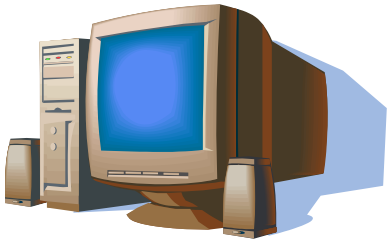


فهرست

ارسال اطلاعات به شکل امن



سیستم مبدأ

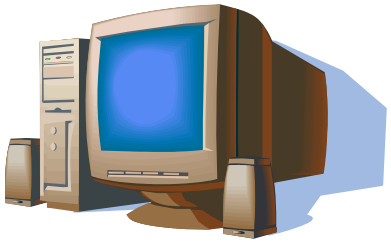


سیستم مقصد

فهرست

قطع
Interruption

سیستم مبدأ



سیستم مقصد

فهرست

دسترسی غیر مجاز
Interception

سیستم مبدأ

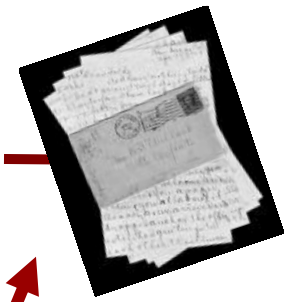
سیستم مقصد

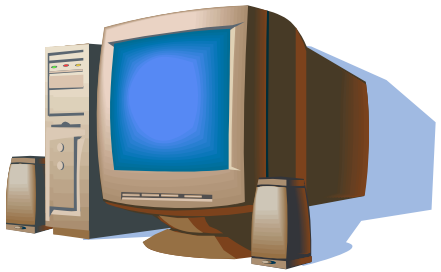
سیستم ثالث

فهرست

دستکاری
داده‌ها
Modification

سیستم مبدأ



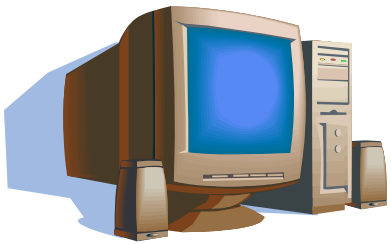


سیستم مقصد

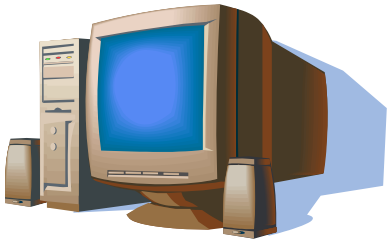
سیستم ثالث

فهرست

ایجاد پیغام
Fabrication



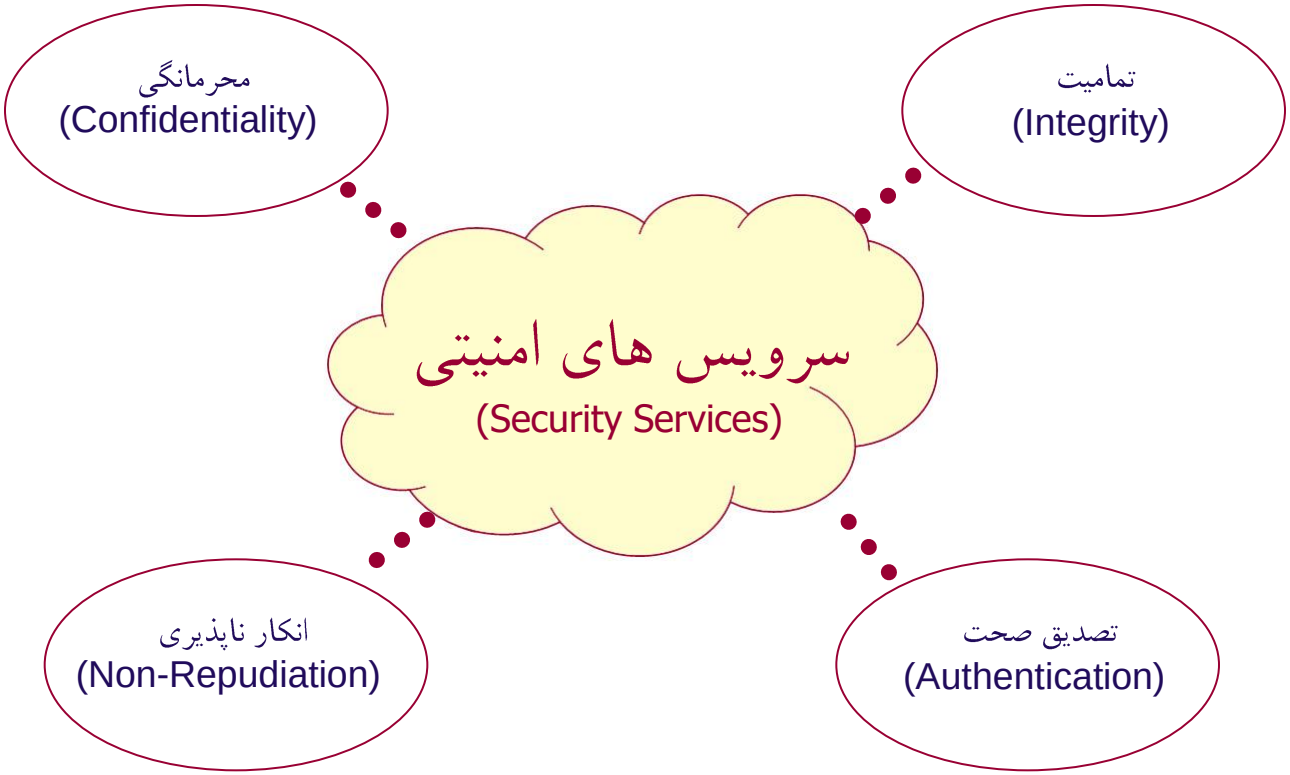
سیستم مبدأ



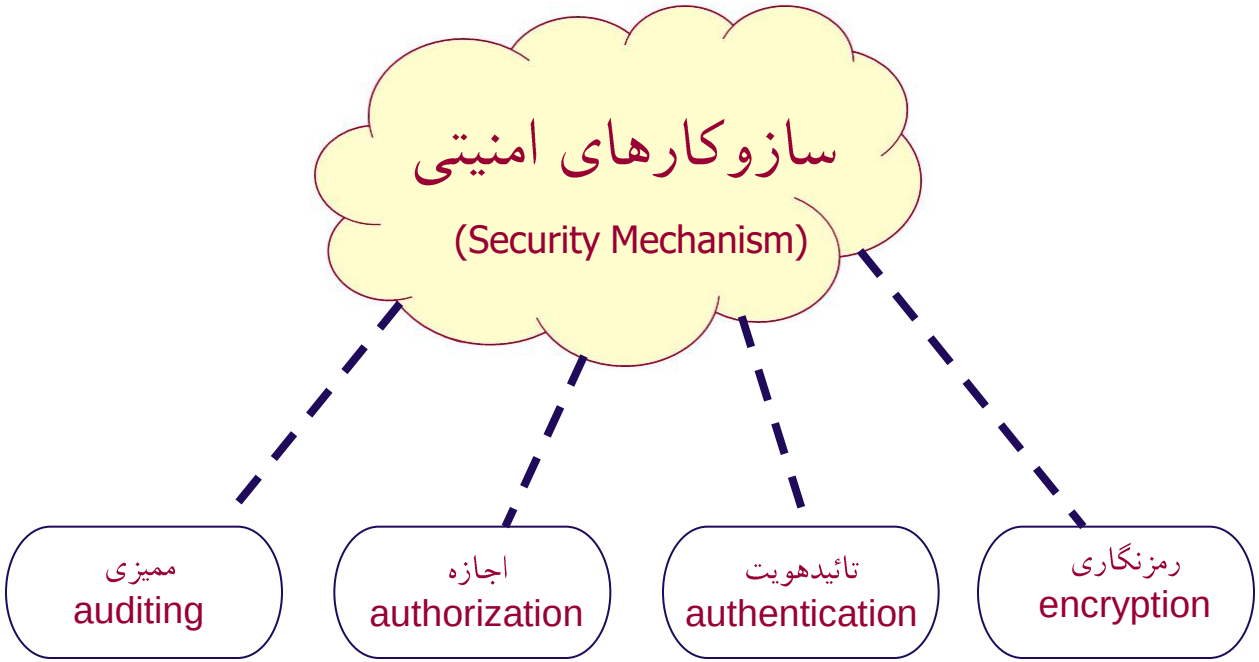
سیستم مقصد

سیستم ثالث

فهرست



فهرست



فهرست

پیغام امن

پیغامی را امن گویند اگر و فقط اگر مشخصات زیر را داشته باشد:

- هویت‌شناسی (Authentication):
گیرنده یک پیغام هویت یکتای فرستنده را شناسایی کند

- محرمانگی (Privacy):
پیغام داده‌ای تنها توسط فرستنده و گیرنده قابل مشاهده باشد

- جامعیت (Integrity) :
پیغام داده‌ای را تنها فرستنده می‌تواند بدون این که تشخیص داده شود تغییر دهد

فهرست

برقراری امنیت در تجارت الکترونیک

- محرمانگی Privacy
- تائیدهویت Authentication
- تمامیت Integrity
- انکارناپذیری None Repudiation

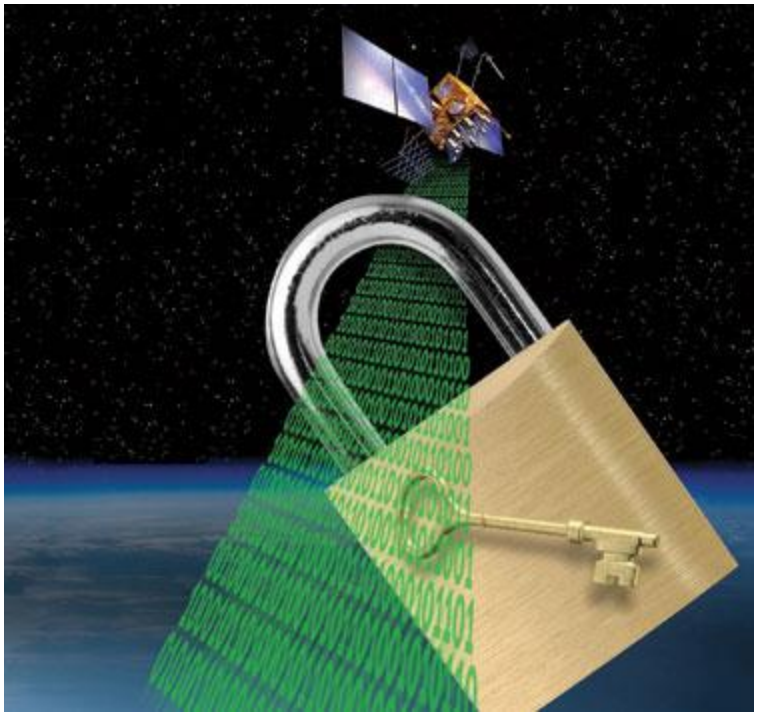
P.A.I.N

فهرست

ابزارهای ایجاد امنیت در تجارت الکترونیکی

فهرست

رمزنگاری



رمزنگاری

رمزنگاری علمی است که با استفاده از ریاضیات داده‌ها را به صورت رمز درآورده و مجدداً می‌تواند به حالت عادی برگرداند. این علم امکان ذخیره سازی اطلاعات وهمچنین انتقال اطلاعات بر بستری ناامن را محقق می‌سازد .عمل رمزنگاری با استفاده از الگوریتمهای ریاضی صورت می‌پذیرد.

در یک سیستم یک پیغام با استفاده از یک کلید رمز می شود.پس از آن پیغام رمز شده به گیرنده منتقل می شود و در آن جا با استفاده از یک کلید باز می شود تا پیغام اصلی بدست آید

فهرست

تاریخچه رمزنگاری

- سابقه رمز نمودن اطلاعات به دوران امپراطوری روم بر می‌گردد، زمانی که ژولیوس سزار پیغامی را برای فرماندهان خود می‌فرستاد چون به پیغام رسان اعتماد نداشت و از این که در راه این پیغام به دست دشمن بیافتد هراسان بود، پیغام را به نحو زیر تغییر می‌داد. تمام حروف A را در متن با حرف D جایگزین می‌کرد و تمام حروف B را در متن به حرف E جایگزین می‌نمود و بدین ترتیب برای بقیه حروف نیز عمل می‌کرد. در حقیقت تمام حروف را با سومین حرف بعد از آن جایگزین می‌کرد.
- در نتیجه اگر این متن تغییر یافته به دست کسی می‌افتاد که این الگوریتم تغییر را نمی‌دانست نمی‌توانست این متن را رمزگشایی نموده و از محتویات آن چیزی بفهمد.
- به این الگوریتم Caesar Cipher می‌گویند.

فهرست

Caesar Cipher

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

This is a test

Wklv lv d whvw

فهرست

تاریخچه رمزنگاری – ادامه

در جنگ جهانی دوم آلمانهای نازی به صورت گسترده‌ای از یک دستگاه رمزنگاری الکترومکانیکی به نام انیگما که در سال ۱۹۳۲ ساخته شده بود استفاده نمودند.

Enigma

فهرست

تاریخچه رمزنگاری – ادامه

تا اواسط دهه ۷۰ میلادی رمزنگاری جزو علومی بود که فقط در موارد ویژه توسط دولتها و متخصصین نظامی استفاده می‌گردید. این وضعیت در سال ۱۹۷۶ میلادی با پیاده سازی "رمزنگاری کلید عمومی" توسط Hellman و Diffie به نحو شایسته‌ای تغییر کرد. این کار آنها مشکل بزرگی را در سیستم‌های رمزنگار که همانا مسئله تبادل کلید بود حل کرد.

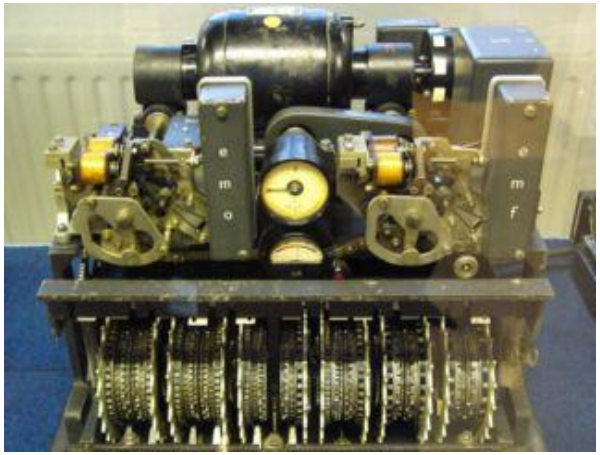
Hellman و Diffie راهی برای برپاسازی یک کانال ارتباطی ایمن بین دونفر بدون نیاز به ملاقات آنها پیدا کردند. در آن زمان رمزنگاری به خوبی درک شده بود ولی هیچکس درک درستی از شیوه مدیریت کلیدهایی که اطلاعات را رمز می‌کنند نداشت.

Hellman و Diffie راهی برای استفاده از محاسبات ساده عددی بر روی اعداد بزرگ برای توافق بر سر کلید پیدا کردند.

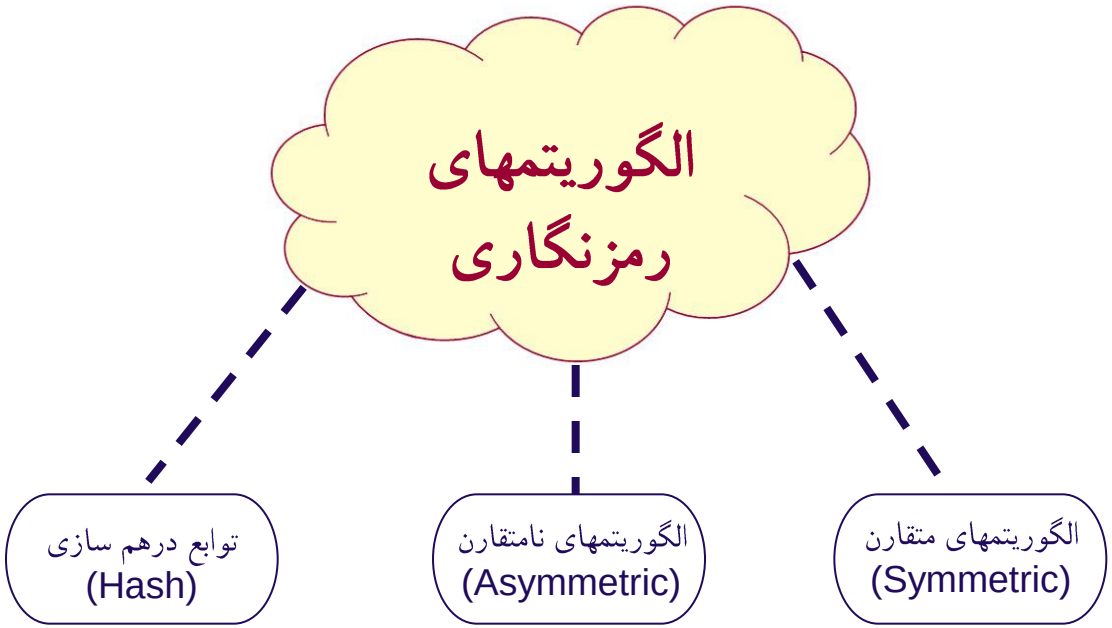
فهرست

تاریخچه رمزنگاری – ادامه

پس از نظریه رمزنگاری کلید عمومی Hellman و Diffie، سیستم‌های کلید عمومی بسیاری طراحی شده‌اند که هرکدام در کاربردی خاص برتری‌های مربوط به خود را دارا می‌باشند. سیستم‌های رمزکلید عمومی عموماً بر پایه حل‌ناپذیری محاسباتی یک مسأله پیچیده بنا می‌شوند.



فهرست



فهرست

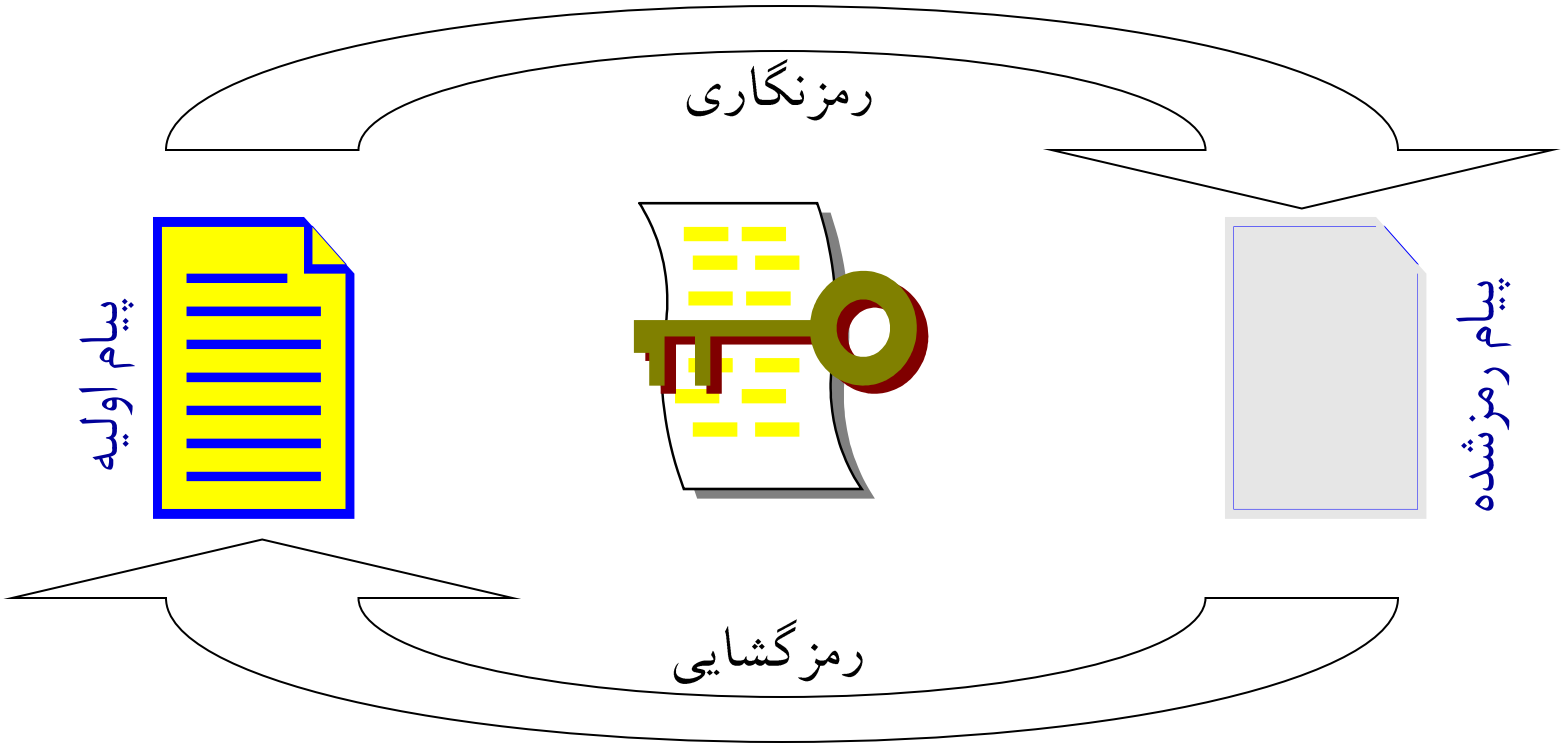
الگوریتمهای متقارن

- در رمز نگاری کلید پنهانی که به عنوان رمز نگاری متقارن شناخته می شود، از یک کلید برای رمز گذاری و رمزگشایی پیغام استفاده می شود. بنابراین فرستنده و گیرنده پیغام باید یک راز مشترک داشته باشند که آن کلید است.
- یک الگوریتم مشهور رمزنگاری "استاندارد رمزگذاری داده" یا DES (Data Encryption Standard) می باشد که در مؤسسات مالی برای رمز کردن شماره هویت فردی یا PIN (Personal Identity Number) استفاده می شود.

کاربرد رمزنگاری متقارن

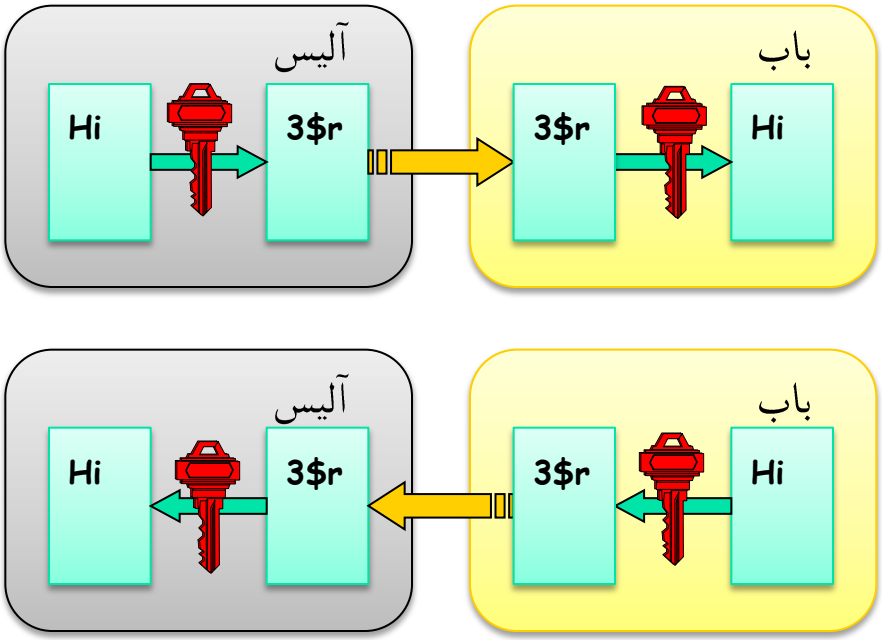
- برای رمزگذاری حجم زیادی از اطلاعات استفاده می‌شود.
- هنگامی که همراه با گواهی دیجیتال استفاده گردد؛ باعث حفظ محرمانگی اطلاعات است.
- زمانی که با امضاء الکترونیکی استفاده گردد؛ تمامیت پیغام را تضمین می‌نماید.

الگوریتم های متقارن



فهرست

الگوریتم متقارن



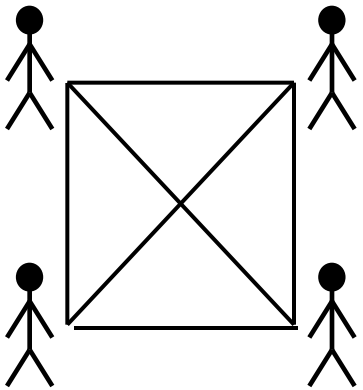
فهرست

مدیریت کلید

کلیدهای متقارن باید از طریق یک کانال ایمن توزیع شوند و باید به صورت ادواری تغییر کنند. مثال:

تعداد کلید های مورد نیاز	تعداد افراد در ارتباط
6	4
15	6
66	12
49950	1000

n*(n-1)/2



فهرست

تحلیل الگوریتمهای متقارن

- مزایا
  - سرعت بالا هنگام رمزگذاری
  - تولید کلید بطور تصادفی و سریع
- معایب
  - تعدد کلیدها برای اعضای هر ارتباط
  - توزیع کلید بین طرفین ارتباط
- موارد استفاده
  - رمزگذاری حجم زیادی از اطلاعات هنگام ذخیره روی رسانه ناامن
  - رمزنگاری داده‌ها هنگام انتقال توسط رسانه ناامن

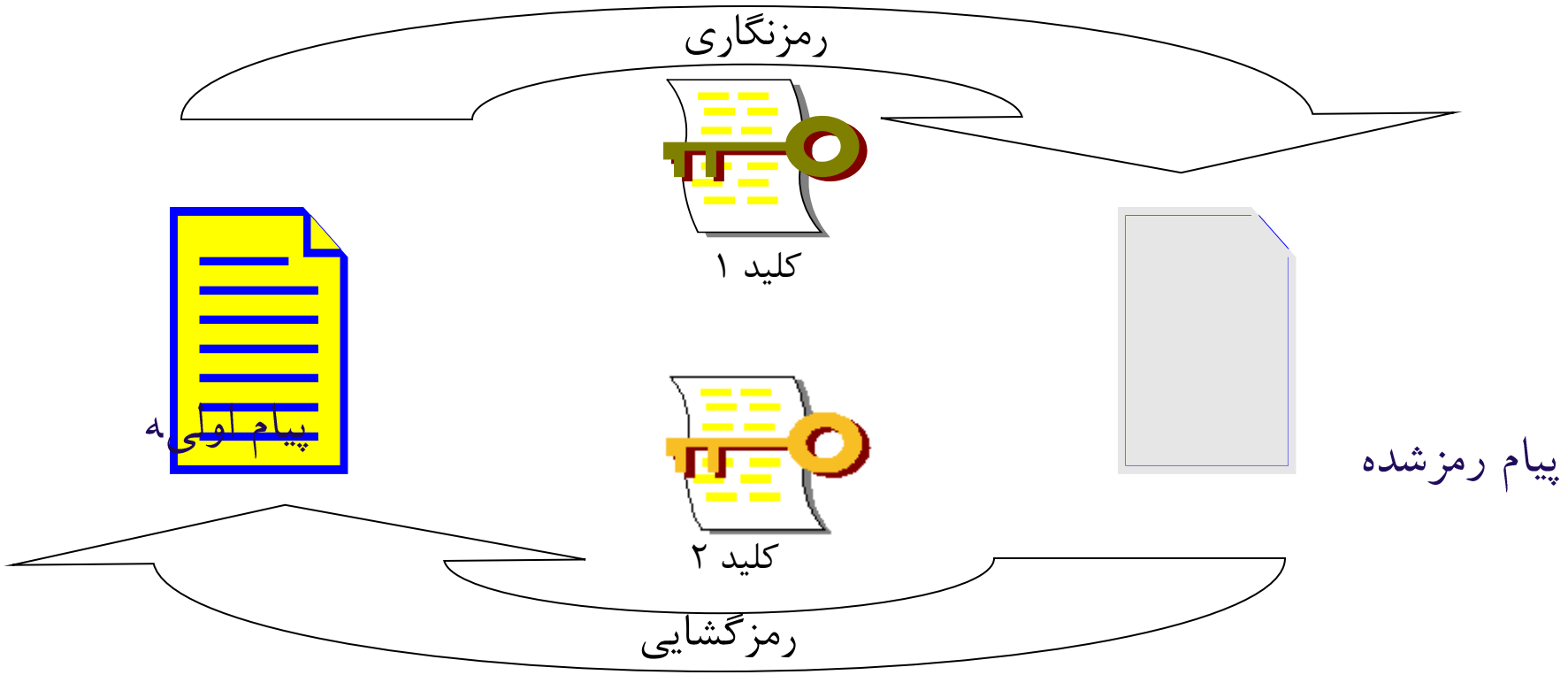
فهرست

الگوریتمهای نامتقارن

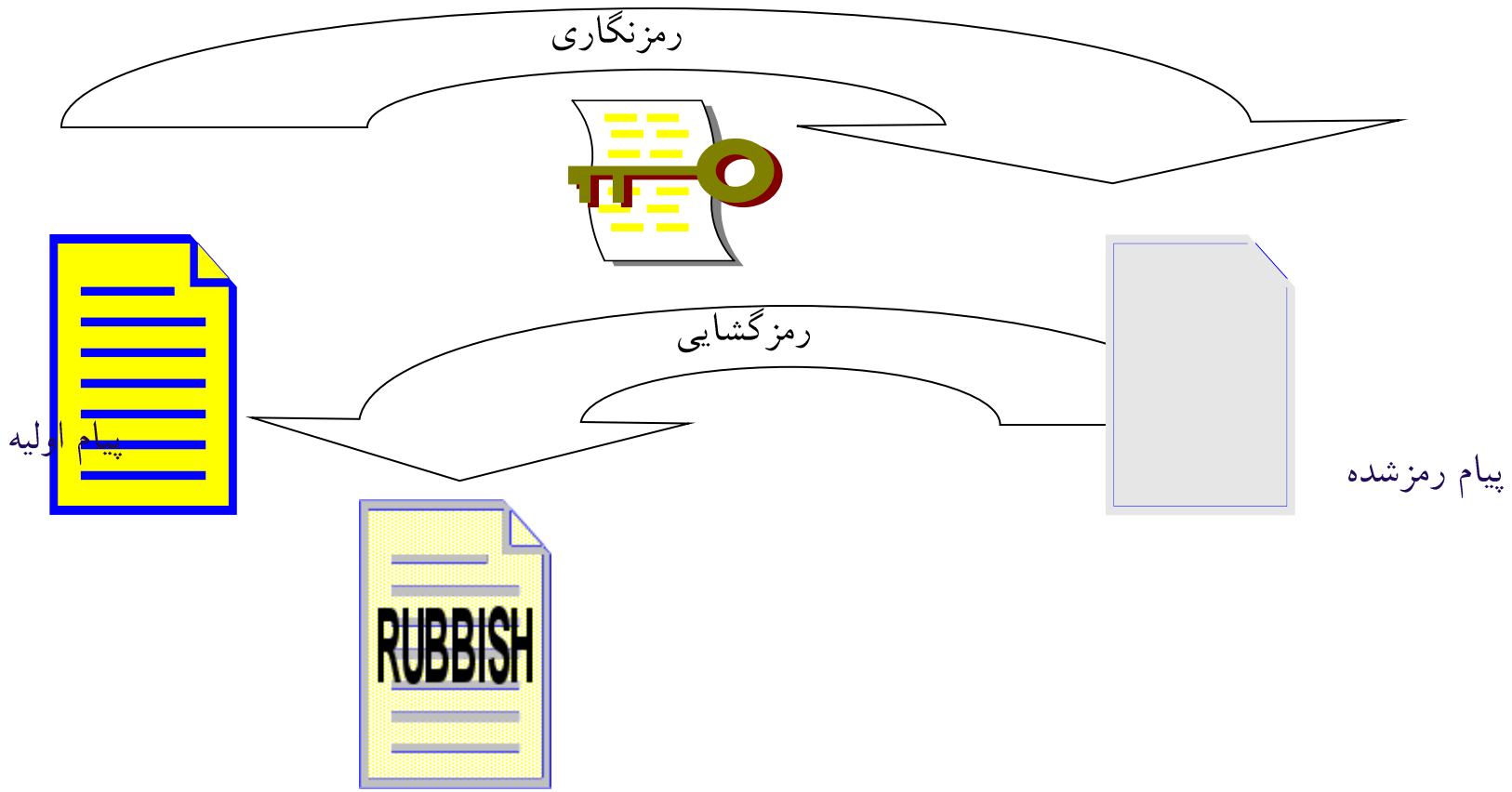
این روش از دو کلید استفاده می‌کند.

- یک کلید برای رمزنگاری و دیگری برای رمز گشایی.
- دو کلید از نظر ریاضی با هم ارتباط دارند به گونه ای که داده رمزنگاری شده با هریک قابل رمزگشایی با دیگری می باشد.
- هر کاربر دو کلید دارد: کلید عمومی و کلید خصوصی.

الگوریتم های نا متقارن
Asymmetric Algorithms

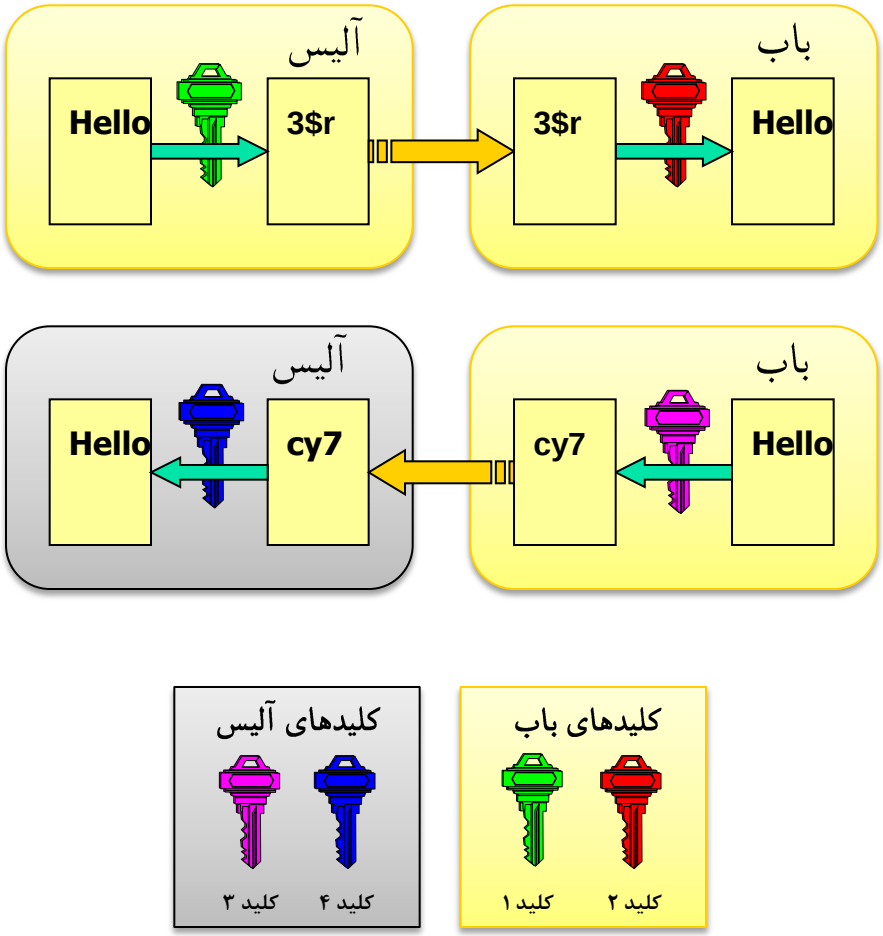


فهرست



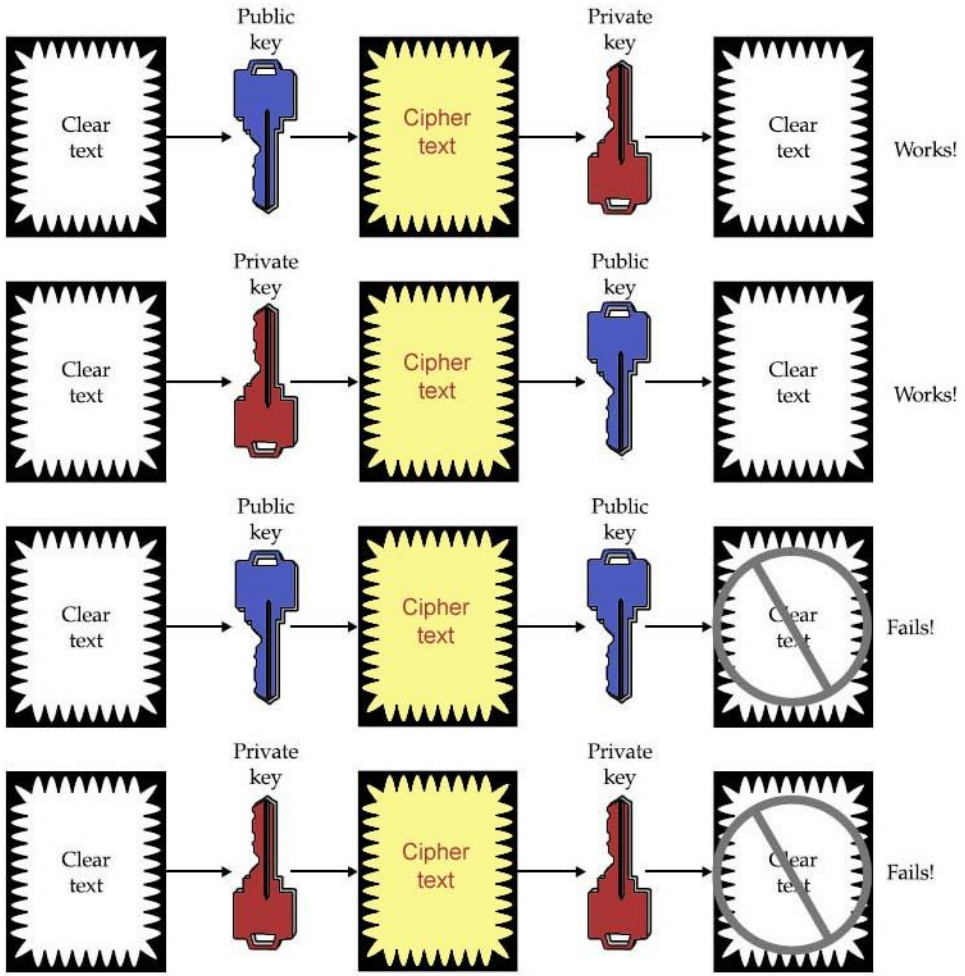
فهرست

الگوریتم های نامتقارن



فهرست

الگوریتمهای نامتقارن



فهرست

تحلیل الگوریتمهای نامتقارن

- مزایا
  - عدم نیاز به توزیع و ارسال کلید
- معایب
  - سرعت پائین در حجم اطلاعات بالا
  - پیچیدگی تولید کلید
- موارد استفاده
  - در تکنولوژی امضای دیجیتال

تحلیل الگوریتمهای نامتقارن – ادامه

- برای رمز کردن داده برای هر طرف شرکت کننده فقط به کلید عمومی آن شرکت کننده نیاز است در نتیجه تنها تأیید کلید عمومی شرکت کننده ها لازم است.

- مهم ترین ویژگی های تکنیک نامتقارن غیر قابل انکار بودن، امضای دیجیتالی وتأیید منبع داده ای صحیح می باشد.

تحلیل الگوریتمهای نامتقارن – ادامه

در رمزنگاری نامتقارن بازرگان یک جفت کلید عمومی و خصوصی ایجاد می کند و کلید عمومی را منتشر می کند تا مصرف کنندگان از طریق آن کلید، پیغامهایشان را رمز کرده برای او بفرستند.

در نهایت بازرگان به عنوان تنها دارنده کلید خصوصی، تنها کسی است که می تواند پیغامهای رمز شده با آن کلید عمومی را باز کند.

فهرست

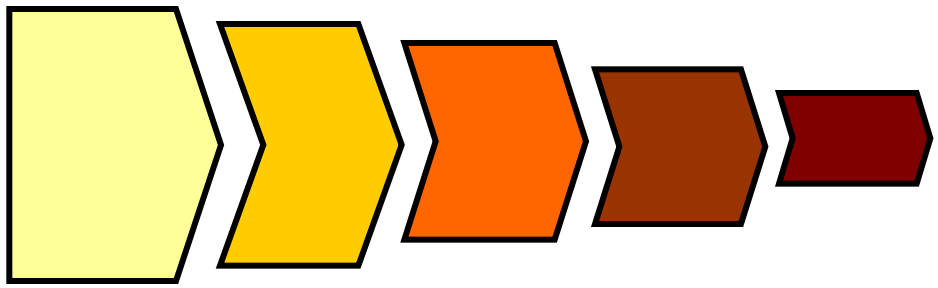
توابع درهم سازی

الگوریتمهای درهم سازی یا Hash بر خلاف دو الگوریتم ذکر شده از کلید استفاده نمی‌کنند و عمل رمزنگاری به صورت یکطرفه بر روی اطلاعات انجام می‌دهند. عملکرد این توابع بر روی داده‌ها بدین شکل است که با اعمال یک تابع Hash بر روی یک متن، یک چکیده یا دایجست از متن بدست می‌آید.

فهرست

کارکرد توابع درهم سازی

ورودی



خروجی

100010101001

Digest

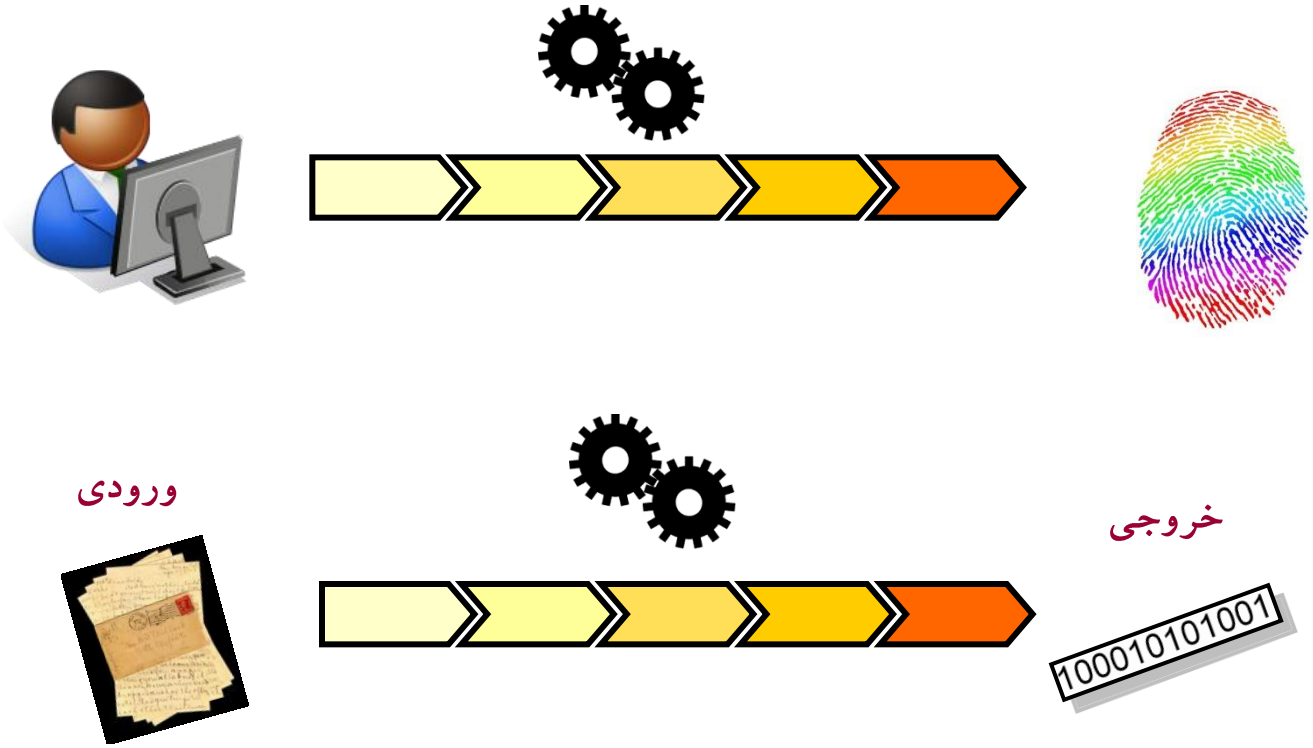
فهرست

توابع درهم سازی

- Hash فرآیندی است که بصورت ریاضی حجم یک جریان از داده را به یک طول ثابت کاهش می دهد. (معمولا ۱۲۸ و یا ۱۶۰ بیت)
- عملکرد hash مشابه اثرانگشت یک شخص می باشد.
- اثرانگشت، پارامتری منحصربفرد به منظور تشخیص هویت افراد بوده و در ادامه با استفاده از آن امکان دستیابی به سایر مشخصات افراد نظیر: رنگ چشم، قد، جنسیت و سایر موارد دلخواه، فراهم می گردد.

فهرست

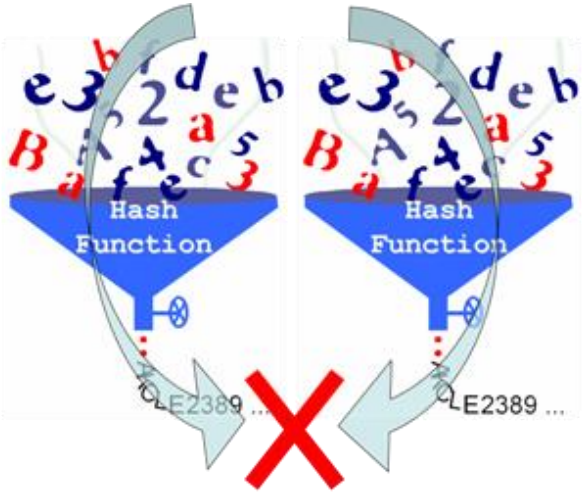
کارکرد توابع درهم سازی



فهرست

ویژگی های توابع درهم سازی

- امکان استنتاج ورودی از طریق خروجی وجود ندارد.
- نمی توان دو ورودی را پیدا کرد که به ازای آنان خروجی یکسانی تولید گردد. درواقع احتمال تولید مقادیر Hash یکسان برای دو مجموعه متفاوت از داده ها کمتر از ۰.۰۰۱ درصد است.

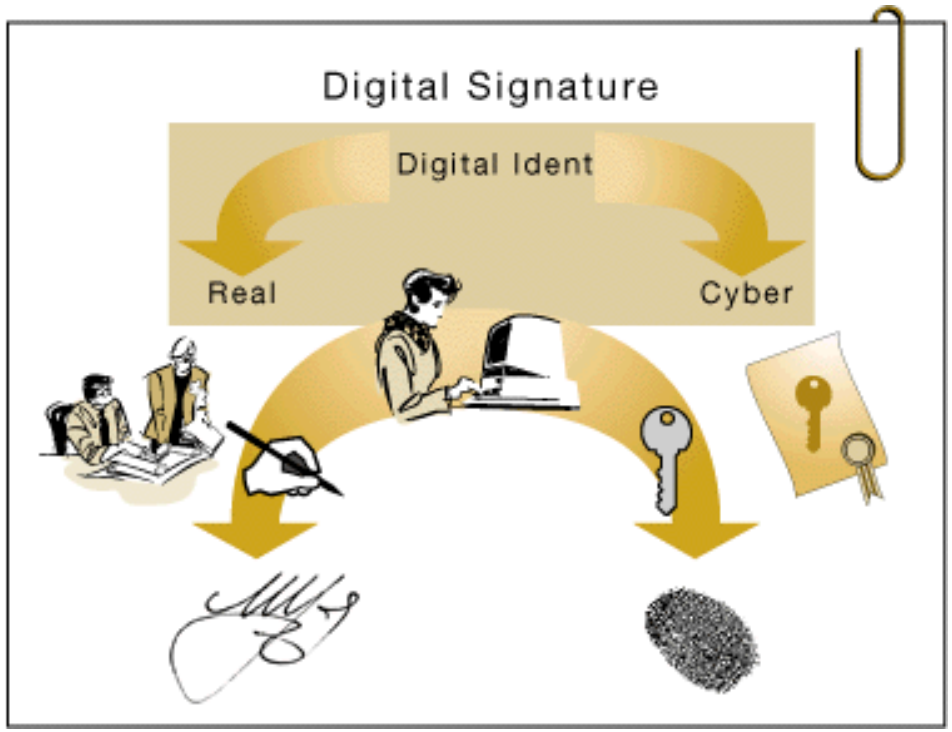


فهرست

تحلیل توابع درهم سازی

- مزایا
  - عدم نیاز به تولید و ارسال کلید
  - سرعت بسیار بالا
- موارد استفاده
  - تضمین تمامیت پیغام

امضاء دیجیتال



فهرست

امضای دیجیتال

- تعاریف و مفاهیم اولیه
- نحوه بکارگیری و پوشش امنیتی

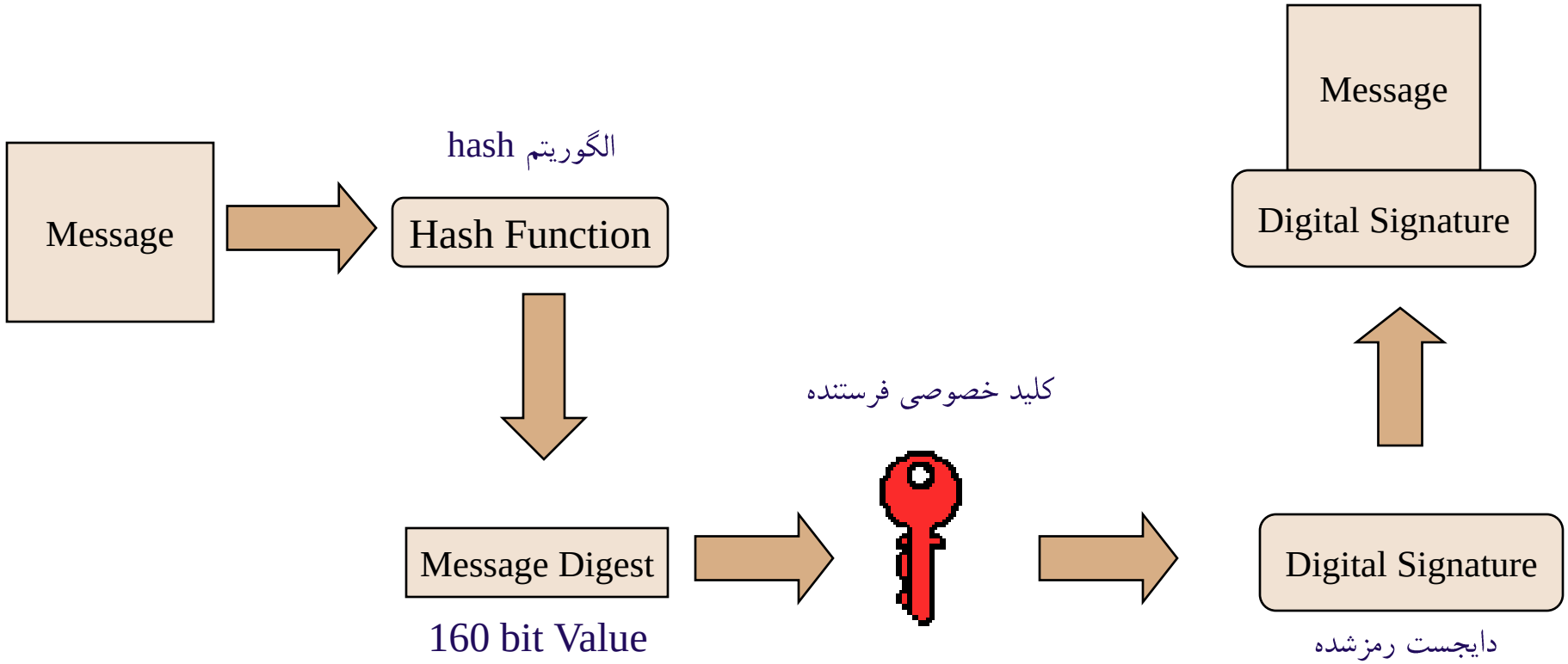
تعریف

- امضا دیجیتال
  - همان قفل کردن اطلاعات می باشد.
  - قابل جعل و تغییر نمی باشد.
  - براساس رمزنگاری می‌باشد.

- امضا دستی
  - تقریباً همیشه همانند به نظر می‌آید.
  - می‌تواند جعل شود.

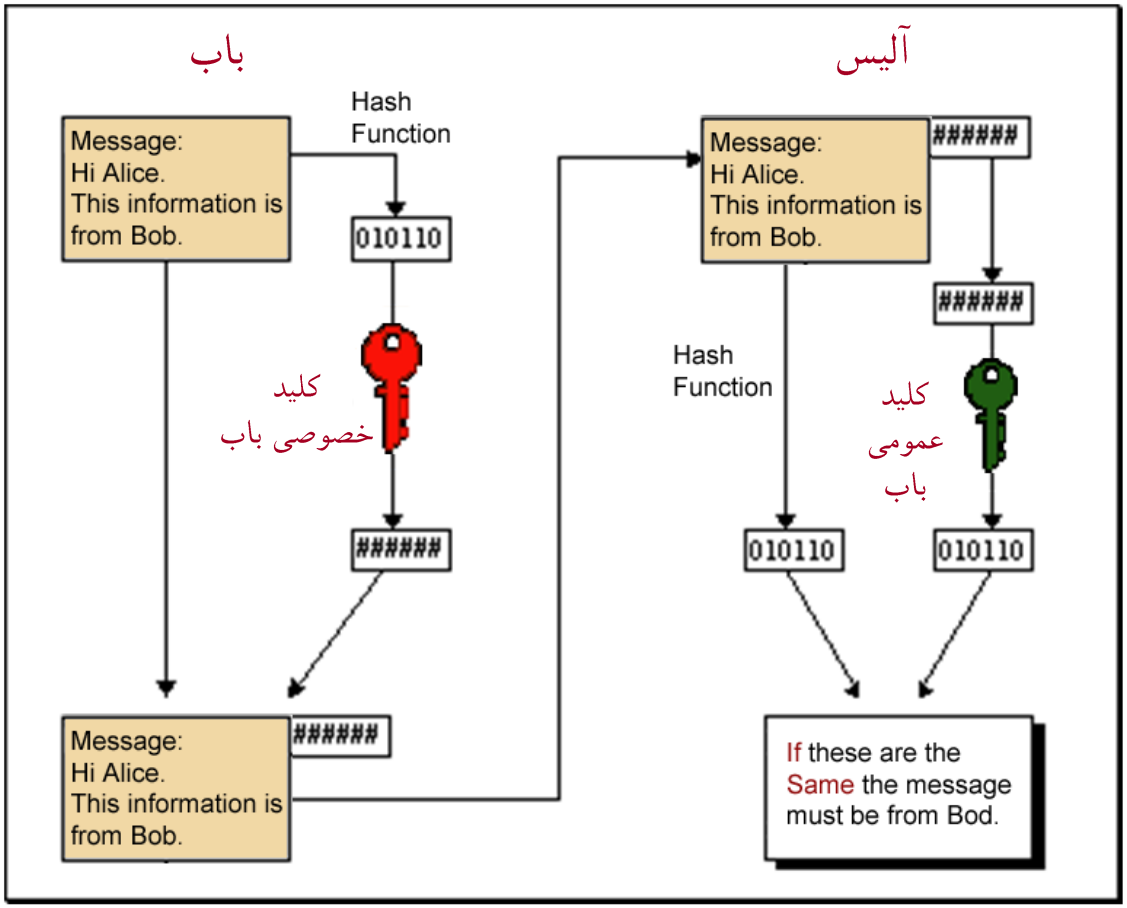
فهرست

نحوه امضاء یک پیغام دیجیتال



فهرست

اعتبارسنجی امضاء دیجیتال



فهرست

کارکرد امضاء دیجیتال

- فرستنده از پیغام یک دایجست ایجاد می‌کند.
- آنرا با کلید خصوصی خود رمز می‌کند.
- به همراه پیغام ارسال می‌دارد.
- گیرنده از متن پیغام دریافت شده یک دایجست ایجاد می‌کند.
- گیرنده از کلید عمومی فرستنده استفاده می‌کند.
- دایجست رمز شده را از حالت رمز خارج می‌سازد.
- گیرنده دو دایجست را با هم مقایسه می‌کند.
- اگر همسان بودند، تمامیت داده و هویت فرستنده مورد تائید قرار می‌گیرد.

فهرست

اجزاء اصلی الگوی جامع شناسایی امضای دیجیتال

- ارائه مجوز به مرکز گواهی هویت.
- صدور، تعلیق و لغو گواهی صادر شده به وسیله مرکز.
- وظایف، ضمانت ها و تعهدات مراجع دارای مجوز، مشترکین، طرف های سوم و محل نگهداری کلید.
- قواعد مخصوص شناسایی و اعتبار امضای دیجیتال.

فهرست

امضای الکترونیکی زمانی معتبر است که :

- اختصاص به شخص استفاده کننده داشته باشد.
- قابلیت تطبیق‌دهی داشته باشد.
- تحت کنترل انحصاری شخص استفاده کننده باشد.
- طوری به داده متصل شود که اگر داده تغییرکرد امضا بی اعتبار شود.

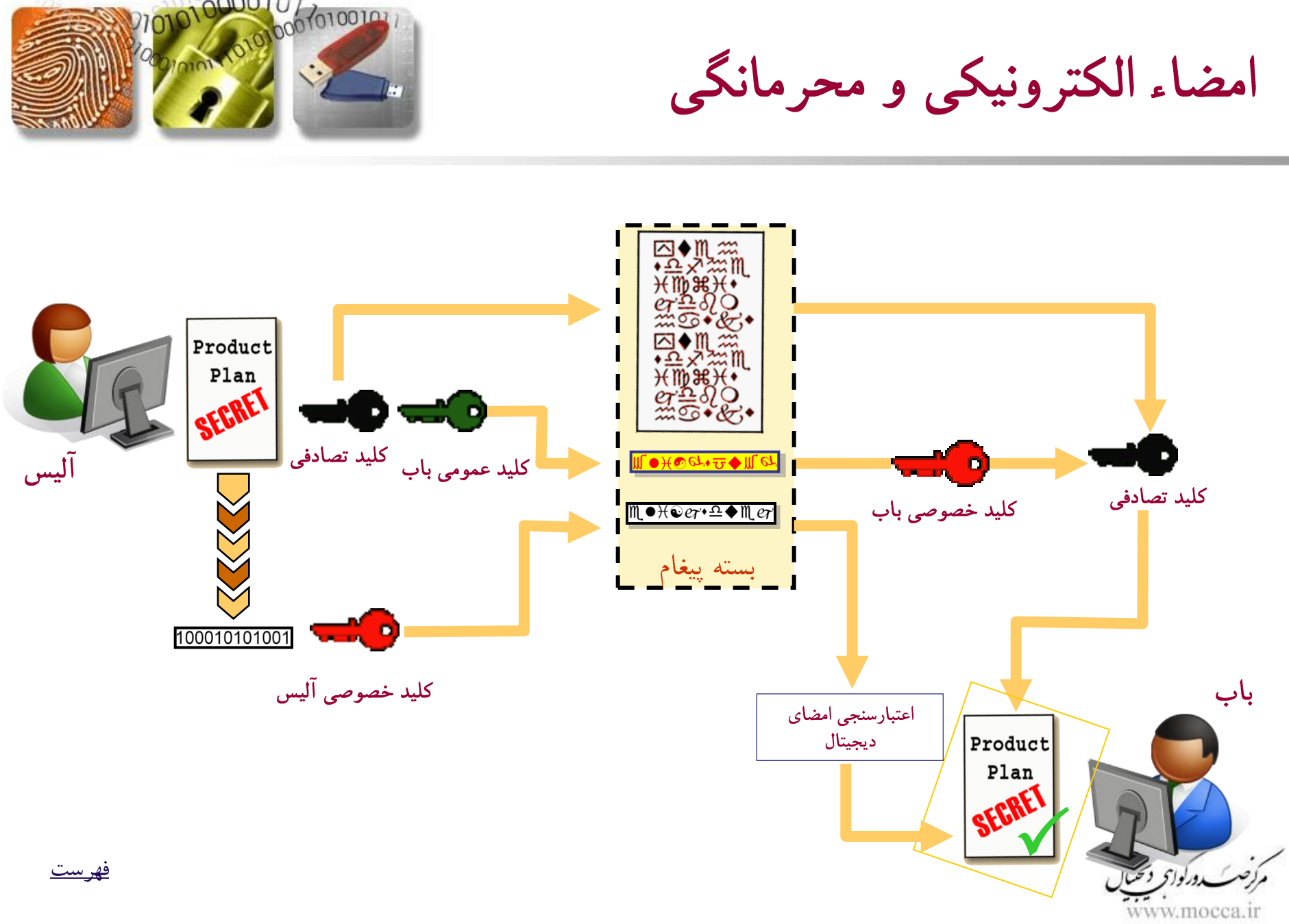
فهرست

خدمات ارائه شده توسط امضاء دیجیتال

- تائید هویت Authentication
  - گیرنده می‌تواند مطمئن باشد که فرستنده کیست.
- تمامیت Integrity
  - گیرنده می‌تواند مطمئن باشد که اطلاعات حین انتقال تغییر پیدا نکرده است.
- انکارناپذیری None Repudiation
  - فرستنده نمی تواند امضا داده را انکار نماید.

فهرست

امضاء الکترونیکی و محرمانگی



فهرست

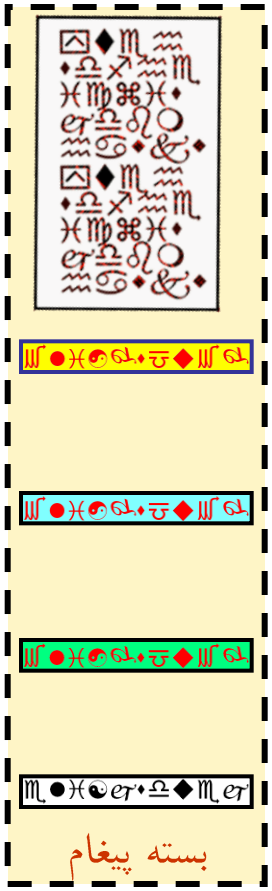
ارسال یک متن برای چند نفر

آلیس

کلید عمومی باب

کلید عمومی بیل

کلید عمومی تام



بسته پیغام

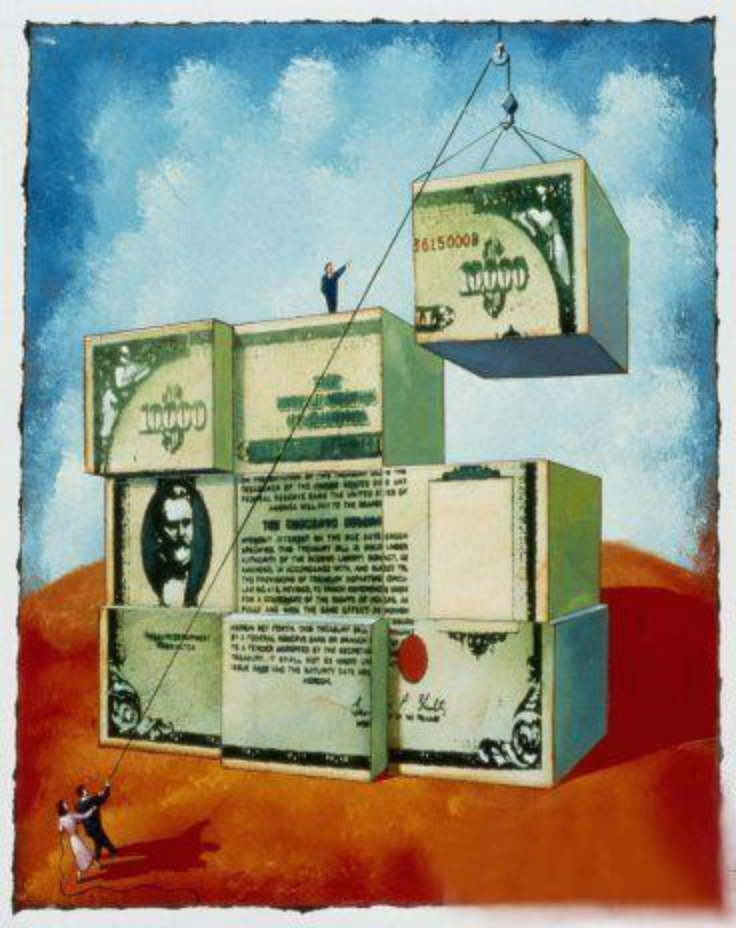
کلید خصوصی باب

کلید خصوصی بیل

کلید خصوصی تام

فهرست

گواهی دیجیتال



فهرست

گواهینامه دیجیتال چیست؟

- سازوکاری برای توزیع کلیدهای عمومی.
- حاوی اطلاعات مربوط به هویت و کلید عمومی صاحب آن.

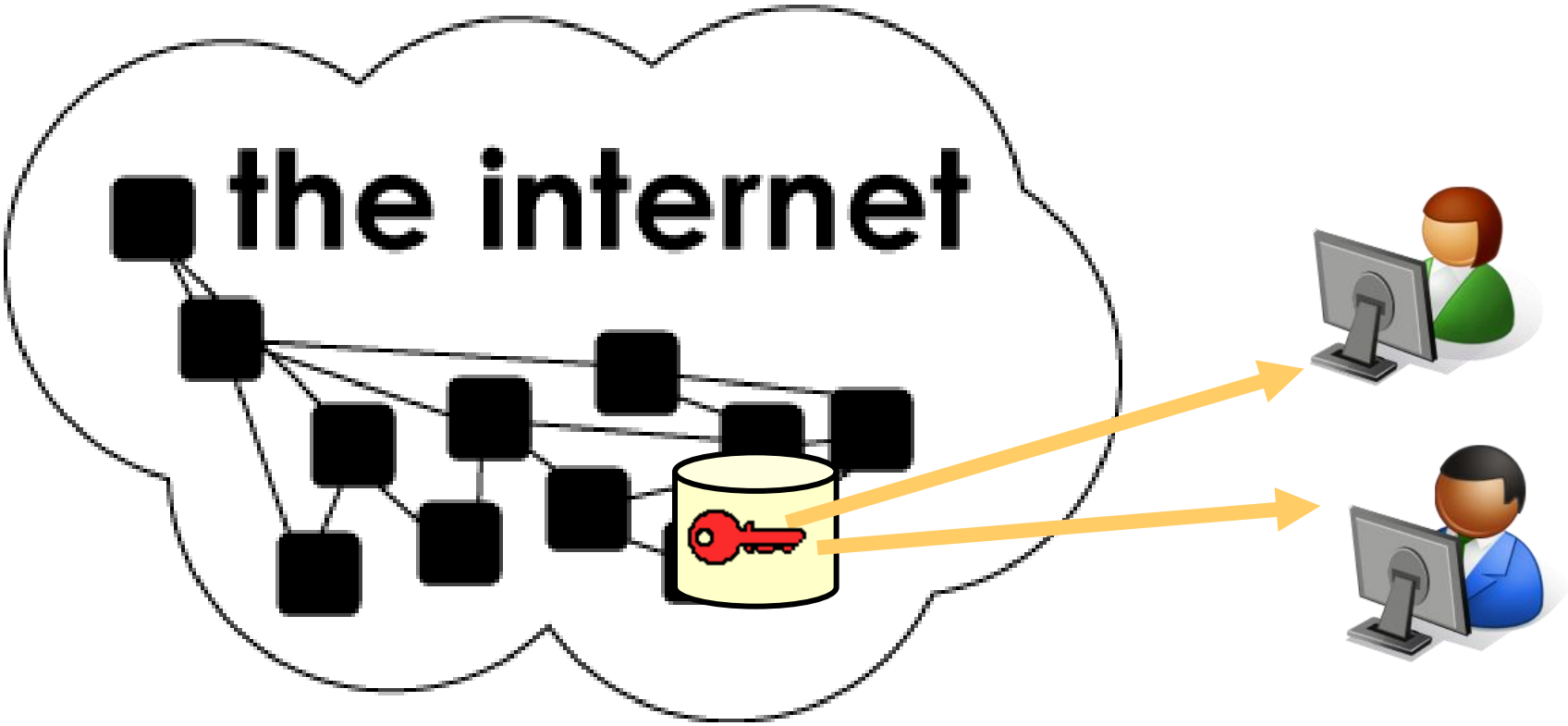






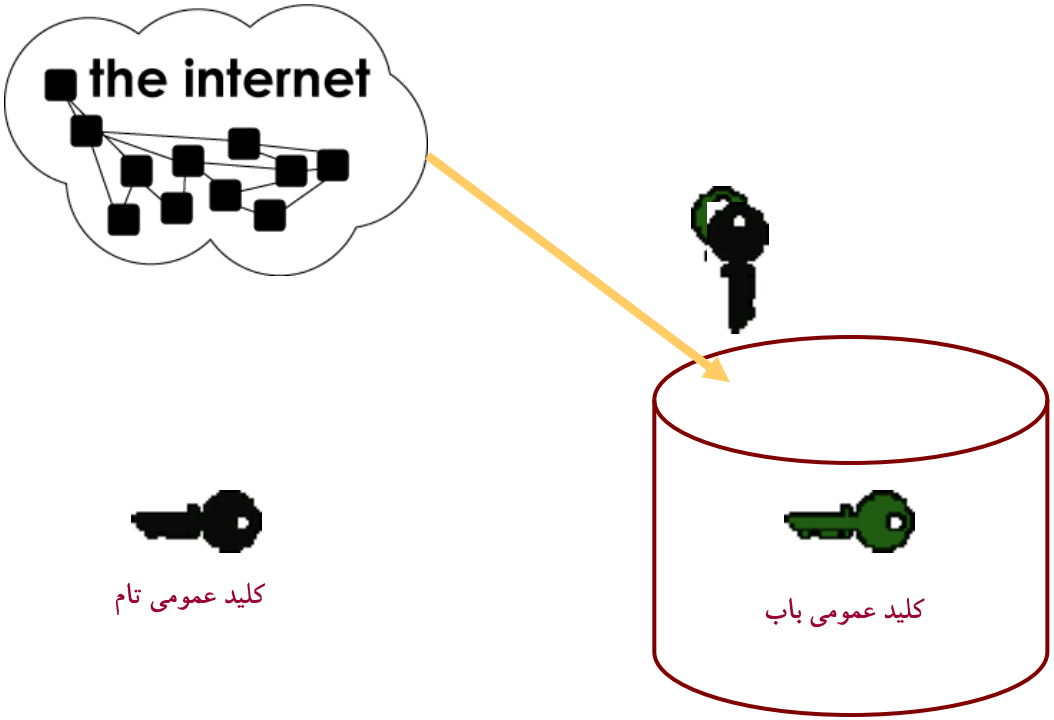

فهرست

کلید عمومی و صاحب آن



فهرست

حمله امنیتی



فهرست

حمله امنیتی –ادامه

باب

کلید خصوصی باب

آلیس

کلید عمومی تام

تام

کلید خصوصی تام

تغییر

کلید عمومی باب

[فهرست]

الگوریتم های یک امضای دیجیتال

- الگوریتم برای ایجاد کلید
- الگوریتم برای ایجاد امضا
- الگوریتم برای تأیید امضا

مروری بر گواهی دیجیتال

گواهی دیجیتال، یک کلید عمومی را به مجموعه‌ای از اطلاعات شناسایی یک موجودیت پیوند می‌دهد. این کلید عمومی با یک کلید خصوصی مرتبط می‌باشد. طرف متکی به صحت کلید عمومی موجود در گواهی اعتماد می‌کند. میزان اعتماد طرف متکی به یک گواهی به عوامل متفاوتی بستگی دارد. این عوامل شامل روال تایید هویت درخواست‌کننده گواهی، روال‌های اجرایی مرکز صدور گواهی، کنترل‌های امنیتی، تعهدات صاحب امضا (مانند حفاظت از کلید خصوصی) و تعهدات مرکز صدور گواهی (مانند ضمانت‌ها و رفع مسئولیت‌ها) می‌باشد.

فهرست

استاندارد X.509

- بر طبق این استادارد اطلاعاتی که در گواهی‌نامه دیجیتال صادر می‌شود شامل موارد زیر می‌باشد:
  - نسخه گواهی‌نامه
  - شماره سریال
  - الگوریتم مورد استفاده
  - صادر کننده گواهی
  - بازه زمانی اعتبار
  - کلید عمومی فردی که گواهی‌نامه برای او صادر شده است.
  - امضای صادر کننده گواهی‌نامه
  - هویت فردی که گواهی‌نامه برای او صادر شده است.
- مشخصاتی که در این قسمت ثبت می‌شود متفاوت بوده و وابسته به نوع گواهی‌نامه می‌باشد.

فهرست

امنیت امضای دیجیتال

- امنیت الگوریتم رمزنگاری کلید عمومی
- امنیت توابع درهم سازی
- امنیت کلید خصوصی

فهرست

مروری بر گواهی دیجیتال

سندی است که:

- توسط یک موجودیت قابل اعتماد صادر و امضاء شده است.
- بر اساس تائید هویتی است که توسط یک مرکز صورت گرفته است.
- حاوی یکسری اطلاعات و کلید عمومی شخص یا سازمان است.
- مورد استفاده آن در گواهی قید شده است.
- دارای مدت اعتبار مشخص و محدود است.

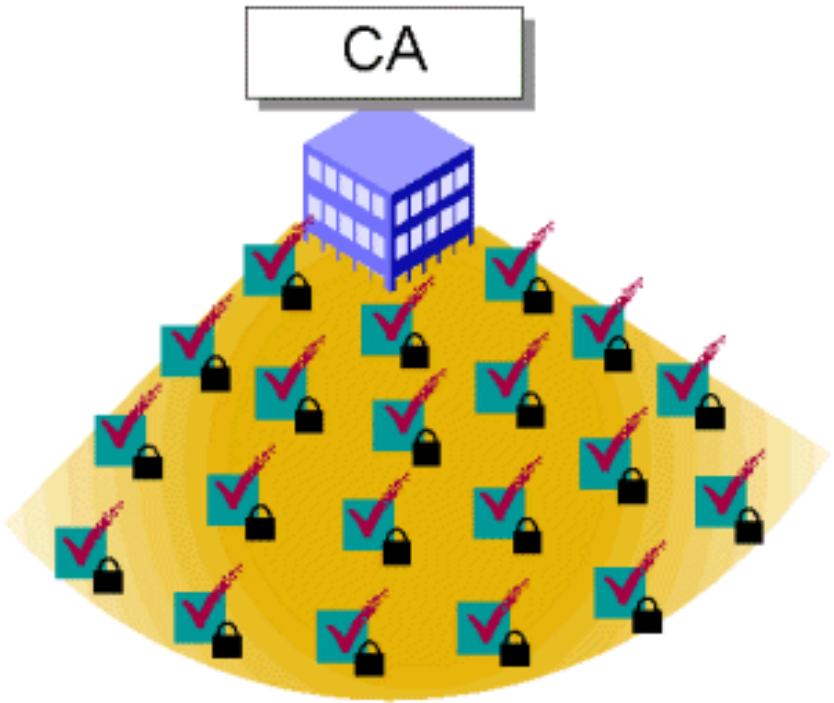
فهرست

کارکرد گواهی دیجیتال

- فرستنده یک کلید متقارن تولید می‌کند.
- داده‌ها را بوسیله کلید متقارن به رمز درمی‌آیند.
- فرستنده از کلید عمومی گیرنده استفاده می‌کند.
- کلید متقارن را به حالت رمز درمی آورد.
- به همراه متن رمزنگاری شده برای گیرنده ارسال می‌نماید.
- گیرنده از کلید خصوصی خود استفاده کرده.
- کلید متقارن را از حالت رمز خارج می‌سازد.
- گیرنده با استفاده از کلید متقارن پیغام را رمزگشایی میکند.

فهرست

مرکز صدور گواهی



فهرست

مرکز صدور گواهی (Certification Authority)

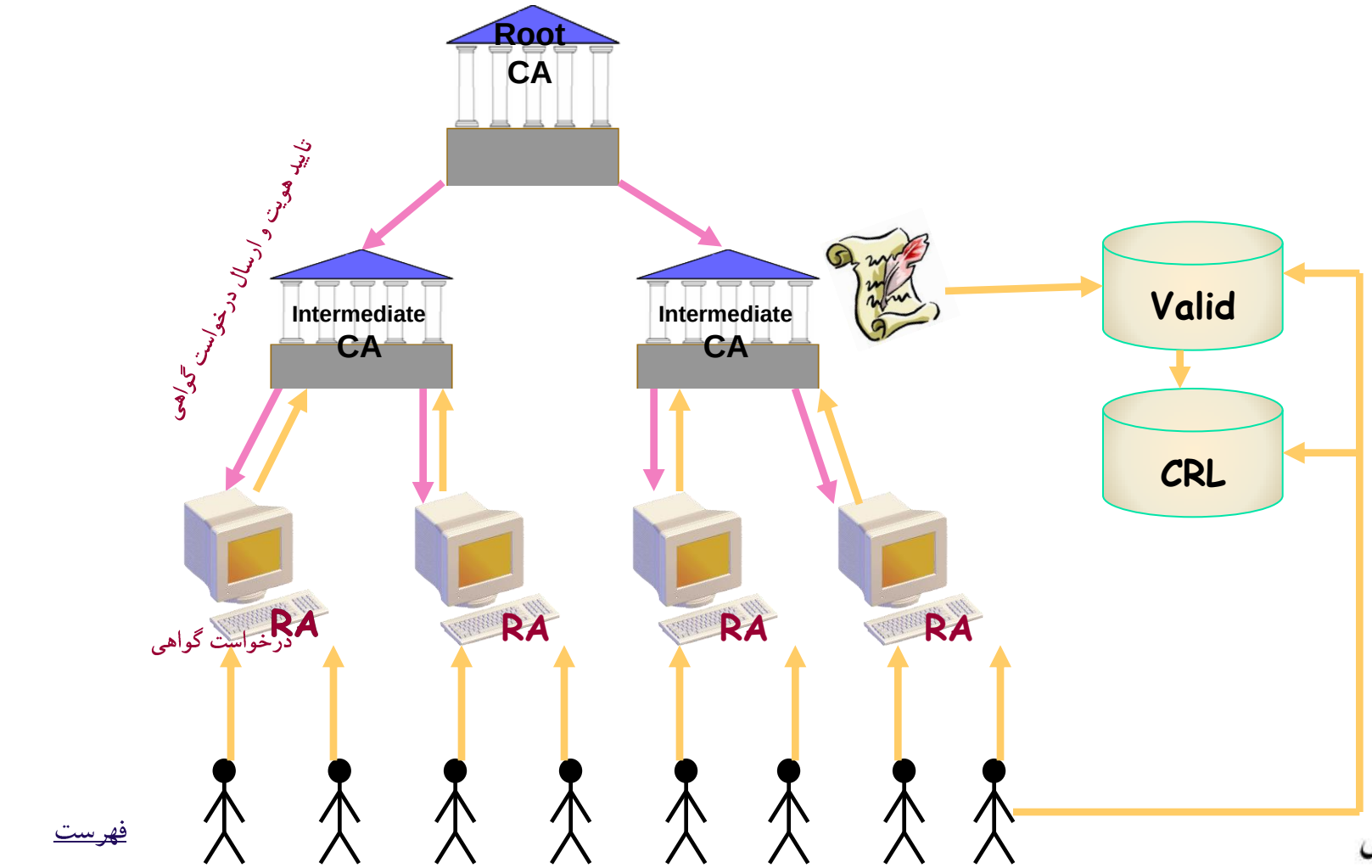
- مراکزی هستند که وظیفه صدور، حفاظت، انتشار و ابطال گواهی‌نامه دیجیتال را بر عهده دارند.
- کلیدهای عمومی این شرکت‌ها به صورت پیش فرض در مرورگرهای اینترنتی قرار دارد.
- تأیید هویت افراد به صورت سلسله مراتبی انجام می‌شود:
  - مراکز صدور گواهی ریشه
  - مراکز میانی صدور گواهی
  - دفاتر ثبت نام

فهرست

انواع مراکز صدور گواهی

- مرکز صدور گواهی ریشه (Root CA)
  - وظیفه مرکز صدور گواهی ریشه صدور گواهی برای مراکز صدور گواهی میانی است.
- مرکز صدور گواهی میانی (Intermediate CA)
  - وظیفه مرکز صدور گواهی میانی، صدور گواهی برای درخواست کنندگانی است که هویت آنها مورد تأیید دفتر ثبت‌نام است.

معرفی اجزاء و کارکرد آنها



فهرست

اجزاء مرکز صدور گواهی

- مرکز صدور گواهی
- دایرکتوری
- مرکز اعلام وضعیت گواهی
- سیاست‌نامه و آیین‌نامه گواهی دیجیتال
- کمیته سیاست گذاری و راهبری
- نرم‌افزار صدور و مدیریت گواهی
- سخت‌افزارهای رمزنگاری

فهرست

وظایف مراکز صدور گواهی

- تولید گواهی
- انتشار گواهی
- ابطال گواهی
- تجدید گواهی
- مدیریت بانکهای اطلاعاتی
- تدوین سیاستهای امنیتی

فهرست

دفتر ثبت‌نام (Registration Authority)

- دفتر ثبت‌نام مرکزی است که متقاضیان دریافت گواهی دیجیتال برای ارائه درخواست و تحویل مدارک به آنجا مراجعه می‌نمایند.

وظایف دفتر ثبت‌نام

- دریافت درخواست گواهی
- تائید هویت
- ارسال درخواست به مرکز صدور
- دریافت و تحویل گواهی به صاحب امضاء
- دریافت و بررسی درخواستهای ابطال یا تمدید گواهی

فهرست

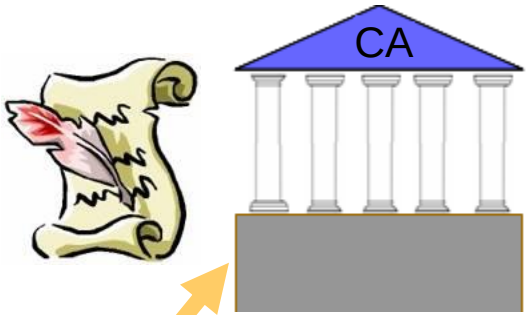
اهداف دفاتر ثبت نام

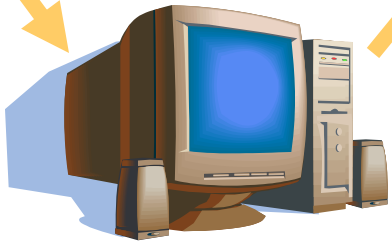
- تامین امنیت لازم در انجام معاملات و محیط های الکترونیکی و ترویج فرهنگ استفاده از هویت الکترونیکی است.
- تولید و ارائه گواهینامه دیجیتال برای تبادلات تجارت الکترونیکی B۲C و B۲B)در حوزه کالا و خدمات)
- تدوین آیین نامه ها و مقررات مربوط به مدیریت بر گواهی دیجیتال تولید و عرضه شده.
- ارائه خدمت به دفاتر ثبت گواهی دیجیتال (RA) و دفاتر خدمات گواهی دیجیتال در سراسر کشور.
- ارائه خدمات آموزشی برای استفاده از این فناوری در سراسر کشور.

فهرست

فرآیند درخواست گواهی

صاحب امضا





دفتر ثبت‌نام

فهرست

مراحل دریافت گواهینامه دیجیتال

- فرد A، از طریق یک نرم افزار تولید کلید، زوج کلیدی برای خود تولید می‌کند.
- فرد A، کلید خصوصی خود را در یک محل امن نزد خود نگهداری کرده و کلید عمومی را به همراه اطلاعات هویت خود به مرکز صدور گواهی‌نامه ارسال می‌کند.
- مرکز صدور گواهی‌نامه، صحت اطلاعات ارسال شده از سوی A را بررسی کرده و در صورت درست بودن آن‌ها یک گواهی‌نامه دیجیتالی برای A صادر می‌کند.
- مرکز صدور گواهی‌نامه (CA)، گواهی صادر شده را برای A، ارسال می‌کند.
- فرد A، گواهی‌نامه دریافت شده را بررسی می‌کند تا مطمئن گردد، کلید عمومی درج شده در گواهی‌نامه، کلید خودش است.

فهرست

مراحل ابطال گواهی‌نامه دیجیتال

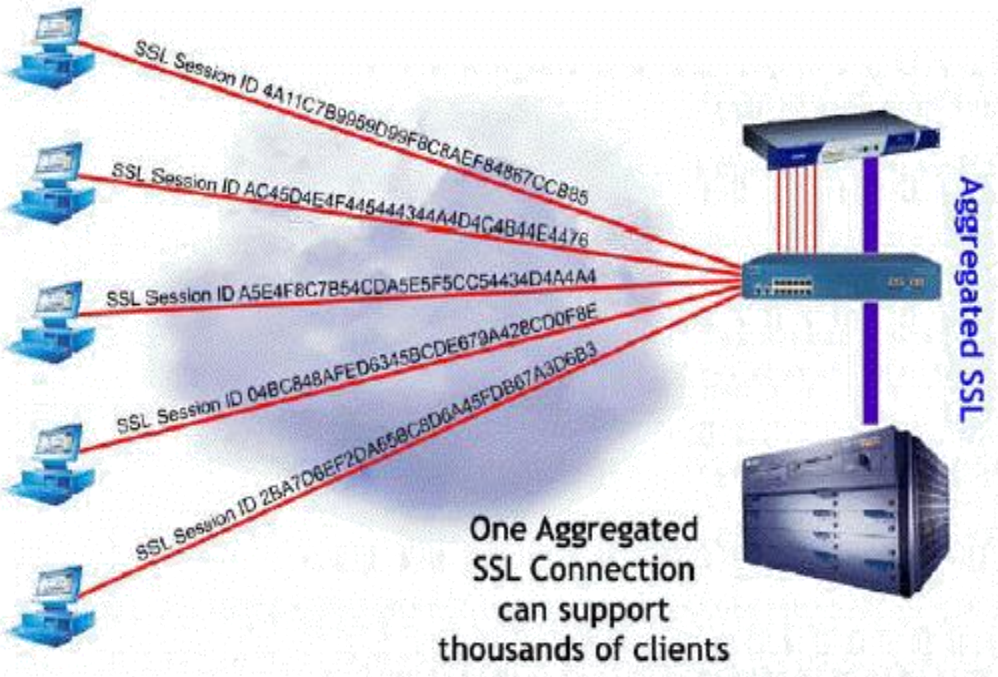
- وارد کردن گواهی در لیست گواهی‌نامه‌های باطل شده (CRL)
- گواهی‌نامه به دو صورت ممکن است باطل شود:
  - ابطال دائمی:
    - زمانی که کلید خصوصی یک فرد دزدیده شود
  - ابطال موقتی:
    - زمانی که فردی کلید خصوصی خود را گم کند
    - زمانی تاریخ اعتبار گواهی‌نامه به اتمام برسد

نحوه دریافت امضاء یا گواهی دیجیتال

- دریافت گواهی دیجیتال بر روی لوح فشرده
- دریافت گواهی دیجیتال بر روی کارت هوشمند
- دریافت گواهی دیجیتال بر توکن

فهرست

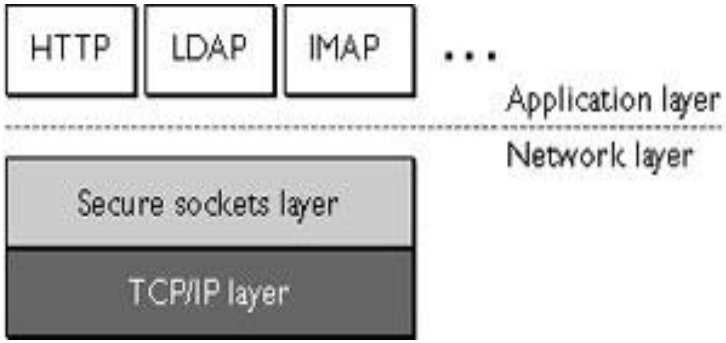
گواهی SSL



فهرست

SSL چیست؟

- Secure Socket Layer
- راه حلی جهت برقراری ارتباط ایمن میان یک وب سرور و یک مرورگر اینترنت
- پروتکلی پایین تر از لایه کاربرد و بالاتر از لایه انتقال
- پروتکل امنیتی است که توسط Netscape ابداع شده است.



فهرست

ملزومات یک ارتباط مبتنی بر گواهی SSL

- دو نوع گواهی دیجیتال SSL یکی برای سرویس دهنده و دیگری برای سرویس گیرنده

- یک مرکز صدور و اعطای گواهینامه دیجیتال یا CA

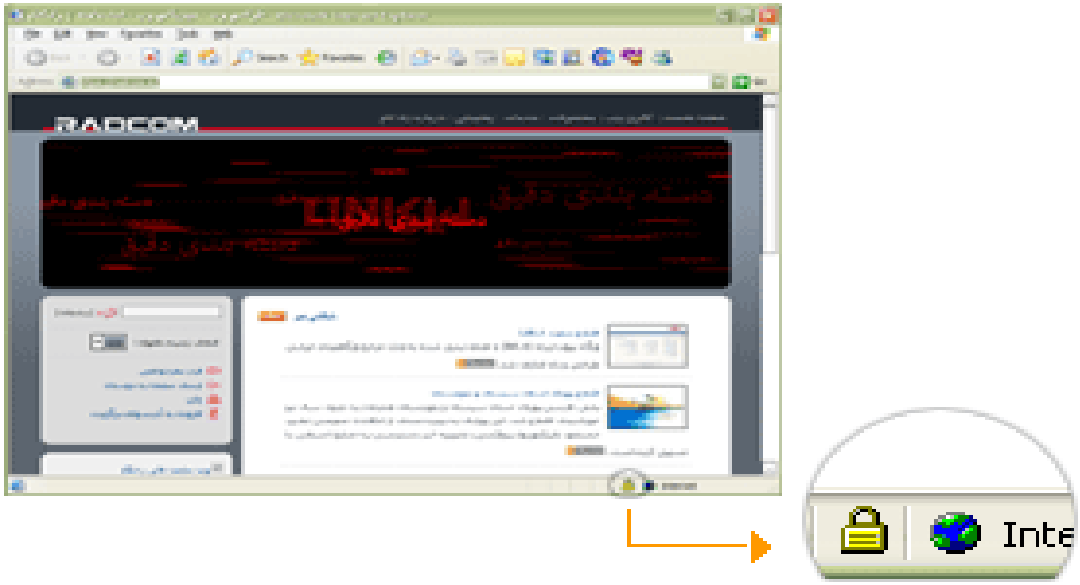
سازوکارهای تشکیل دهنده SSL

- تأیید هویت سرویس دهنده
- تأیید هویت سرویس گیرنده
- ارتباطات رمز شده

فهرست

نمایش قفل امنیت SSL

قفل کوچک زرد رنگ در نوار وضعیت مرورگر امنیت سایت توسط گواهی SSL می‌باشد.



فهرست

وظایف مرکز صدور گواهی SSL

- صدور و انتشار گواهی ها
- ابطال گواهی ها در صورت لزوم
- ارسال گواهی ها و لیست گواهی های باطل شده به مخزن
- اطمینان از نگهداری ایمن کلیدهای خصوصی این مرکز
- آگاه سازی و عرضه کننده سرویس مخزن از این تعهدات
- تولید کلیدهای خصوصی مرکز صدور گواهی SSL به طور ایمن

فهرست

وظایف دفاتر ثبت نام گواهی SSL

- اطمینان از این که عملیات آن ها مطابق با دستورالعمل اجرایی انجام می گیرد.
- احراز هویت صاحبان امضا هنگام درخواست گواهی SSL یا درخواست ابطال گواهی.
- اطلاع رسانی به درخواست کننده گواهی در مورد صدور گواهی درخواست شده.
- اطلاع رسانی به صاحبان امضا در مورد ابطال گواهی آن ها.

فهرست

روند کار SSL

- هویت سرویس دهنده برای سرویس گیرنده مشخص می‌گردد
- توافق سرویس دهنده و گیرنده بر سر نوع الگوریتم رمزنگاری
- احراز هویت سرویس گیرنده برای سرویس دهنده
- ایجاد کلیدهای اشتراکی مخفی
- رمزنگاری ارتباطات بر مبنای SSL

فهرست

نحوه عملکرد گواهی SSL

- برنامه مرورگر یک کلید متقارن تولید می‌کند وداده‌ها را به وسیله آن به رمز در می‌آورد.
- مرورگر از کلید عمومی وب سایت استفاده می‌کند و کلید متقارن را به حالت رمز در آورده و به همراه متن رمزنگاری شده برای وب سرور ارسال می‌نماید.
- وب سرور از کلید خصوصی خود استفاده کرده و کلید متقارن را از حالت رمز خارج می‌سازد.
- وب سرور با استفاده از کلید متقارن اطلاعات فرستاده شده از برنامه مرورگر را رمزگشایی می‌کند.

فهرست

استفاده گواهی SSL از الگوریتم‌ها

- استفاده از الگوریتم متقارن و تولید کلید تصادفی برای رمزگذاری اطلاعات رد و بدل شده بین مرورگر و وب سرور.

- استفاده از کلید عمومی وب سایت برای رمزنگاری کلیدتصادفی.

فهرست

گواهی ثبت سفارش

فهرست

جایگاه زیرساخت کلید عمومی در ثبت سفارش

- ماهیت ثبت سفارش
  - دولت الکترونیک، تجارت الکترونیک، شفاف سازی
- مخاطبان سیستم
  - بازرگانان و تجار، کارشناسان، مدیران
- نیازهای امنیتی ثبت سفارش اینترنتی
  - محرمانگی، تمامیت، امضای دیجیتال، عدم انکار

فهرست

پیاده سازی زیرساخت کلید عمومی در ثبت سفارش

- استفاده از بستر SSL به منظور تامین امنیت بستر انتقال اطلاعات
- استفاده ازگواهی دیجیتال به منظور احراز هویت کاربر
- استفاده از امضای دیجیتال به منظور:
  - اطمینان از صحت اطلاعات ارائه شده توسط کاربر
  - اطمینان از تمامیت داده های موجود در بانک اطلاعاتی
  - تشخیص دسترسی و تغییر غیرمجاز اطلاعات

روش اجرائی پیاده سازی

- فرآیند ورود به سیستم
  - کنترل گواهینامه دیجیتال
  - امضای کد کاربری و رمز عبور ارسالی به سرور
  - تصدیق اطلاعات ارسالی از کلاینت به سرور با امضای دیجیتال
- فرآیند ثبت نام
  - ایجاد هش از محتویات ارائه شده و تصدیق آن با بانک اطلاعاتی
  - امضای محتویات ارائه شده از طرف کاربر
  - تصدیق محتویات ثبت شده در بانک اطلاعاتی توسط امضای کاربر
- ثبت سفارش
  - امضای محتویات ارائه شده از طرف کاربر
  - تصدیق محتویات ثبت شده در بانک اطلاعاتی توسط امضای کاربر
  - استفاده از مهر زمانی به منظور تعیین زمان دقیق انجام عملیات

فهرست