

امنیت داده ها

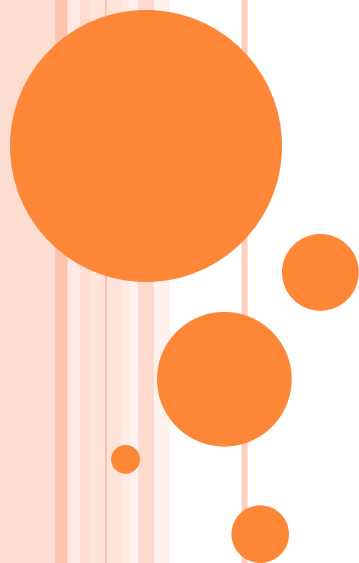
امنیت داده ها

دکتر یعقوب فرجامی

دکتر یعقوب فرجامی

عضو هیات علمی دانشکده فنی قم

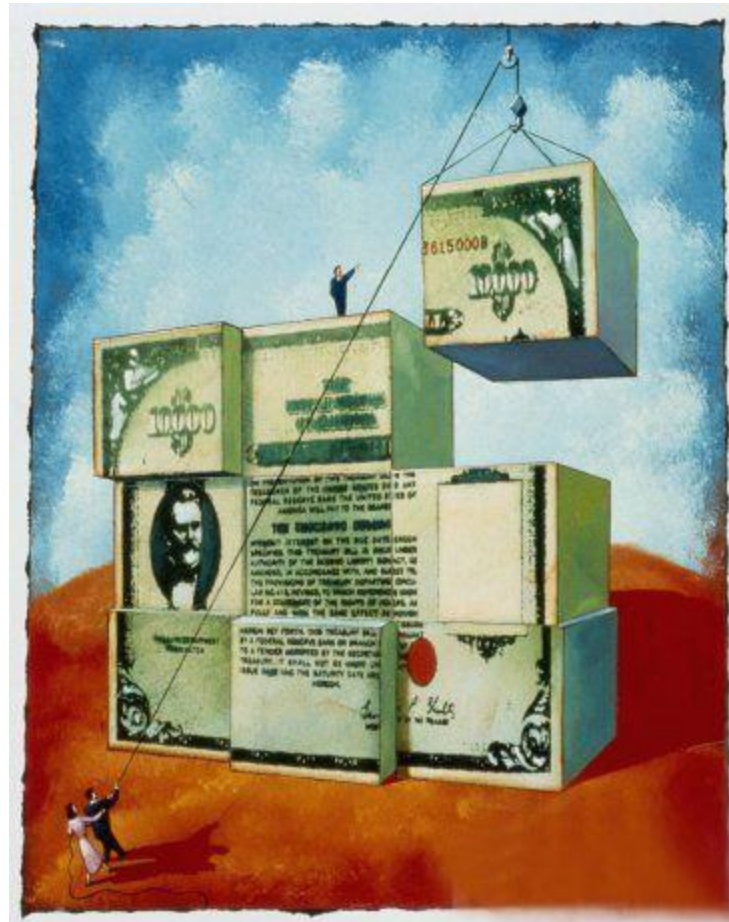
عضو هیات علمی دانشکده فنی قم



فصل دوازدهم: گواهینامه دیجیتال و ساختار PKI

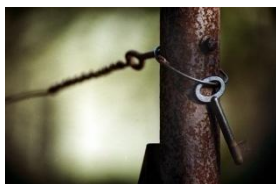


گواهی دیجیتال



گواهینامه دیجیتال چیست؟

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

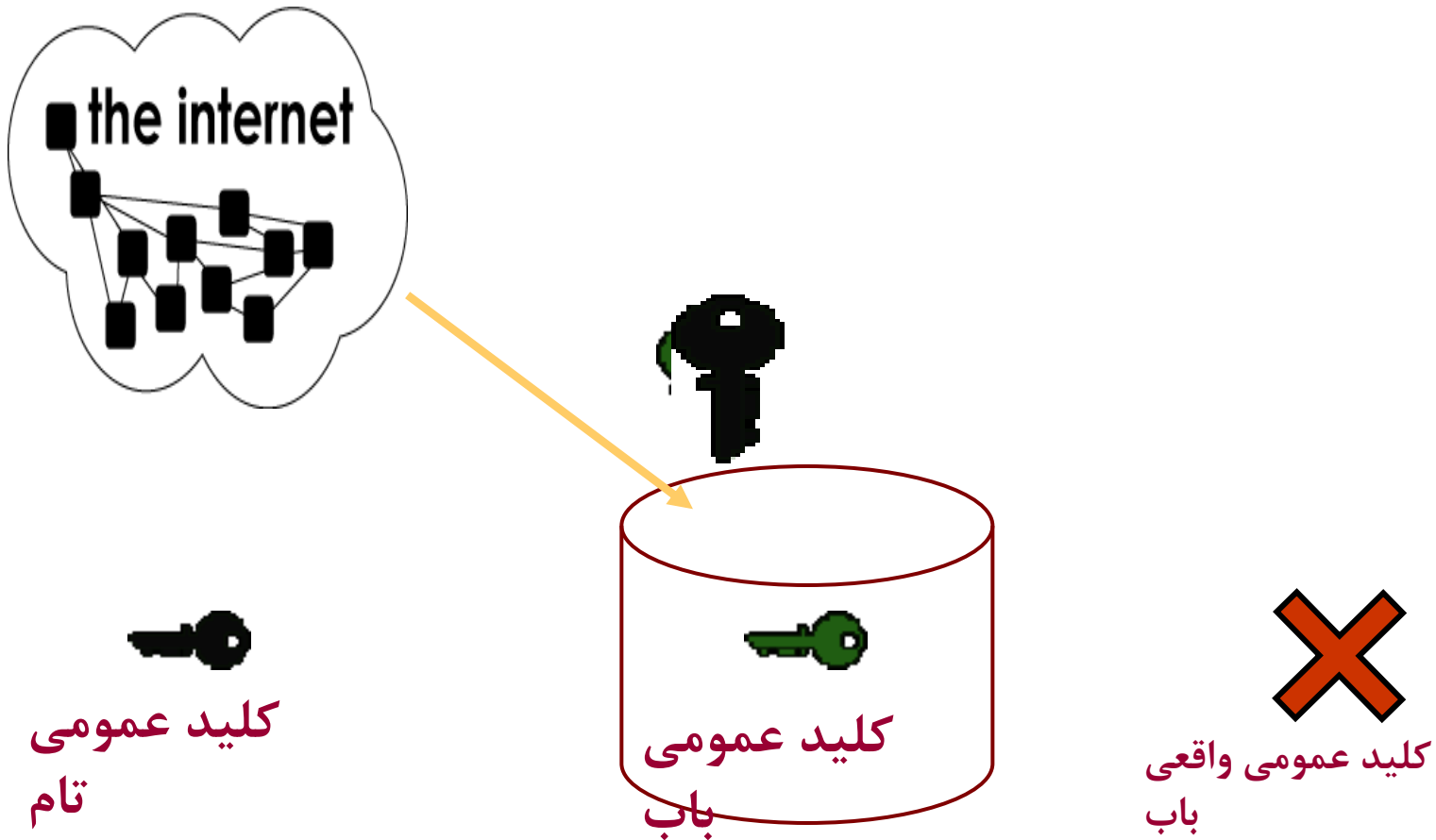


مروری بر گواهی دیجیتال

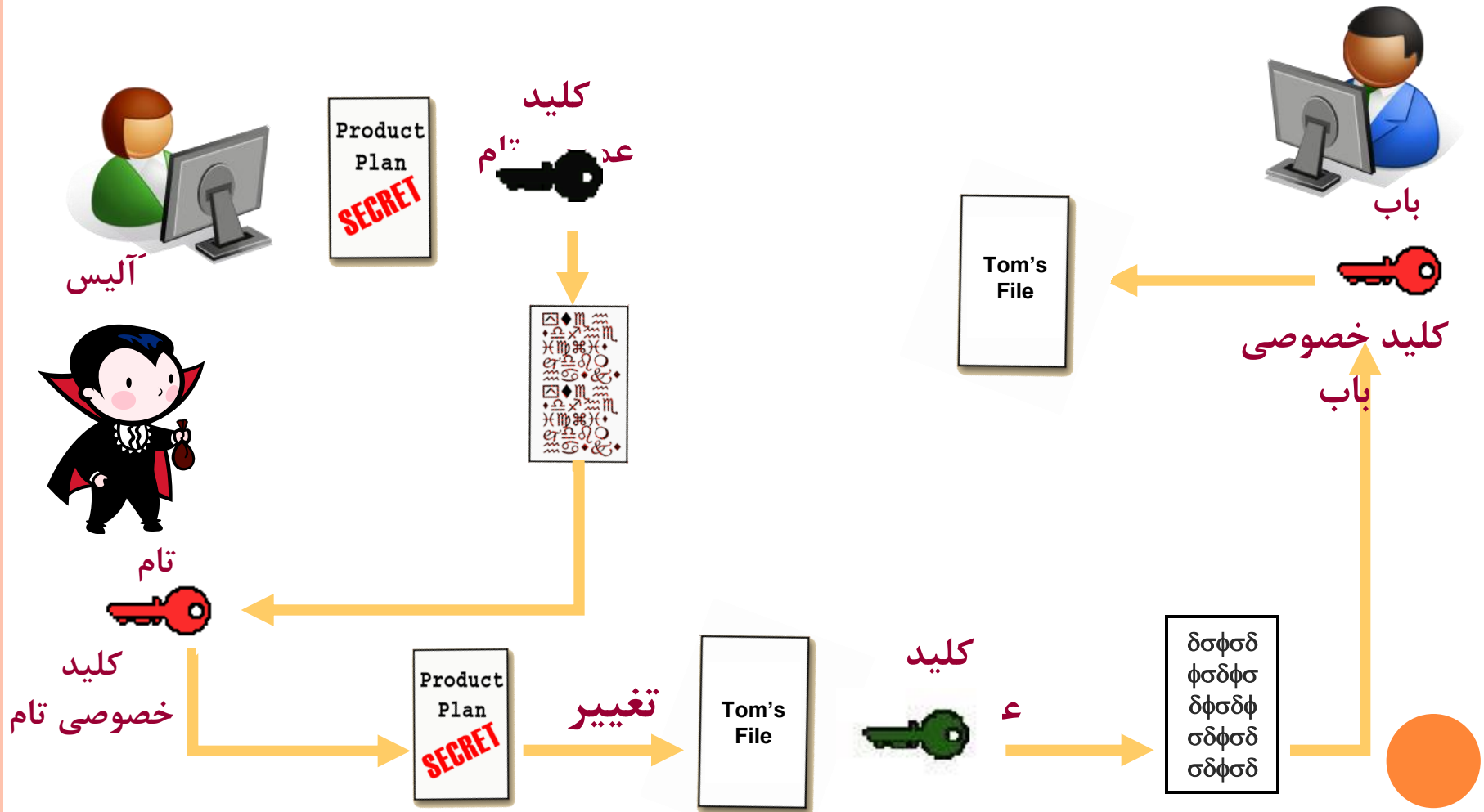
گواهی دیجیتال، یک کلید عمومی را به مجموعه‌ای از اطلاعات شناسایی یک موجودیت پیوند می‌دهد. این کلید عمومی با یک کلید خصوصی مرتبط می‌باشد. طرف متکی به صحت کلید عمومی موجود در گواهی اعتماد می‌کند. میزان اعتماد طرف متکی به یک گواهی به عوامل متفاوتی بستگی دارد. این عوامل شامل روال تایید هویت درخواست‌کننده 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.



حمله امنیتی



حمله امنیتی - ادامه



استاندارد X.509

بر طبق این استاندارد اطلاعاتی که در گواهی نامه دیجیتال صادر می شود شامل موارد زیر می باشد:

- نسخه گواهی نامه
 - شماره سریال
 - الگوریتم مورد استفاده
 - صادر کننده گواهی
 - بازه زمانی اعتبار
 - کلید عمومی فردی که گواهی نامه برای او صادر شده است.
 - امضای صادر کننده گواهی نامه
 - هویت فردی که گواهی نامه برای او صادر شده است.
- مشخصاتی که در این قسمت ثبت می شود متفاوت بوده و وابسته به نوع گواهی نامه می باشد.

مروری بر گواهی دیجیتال

سندی است که:

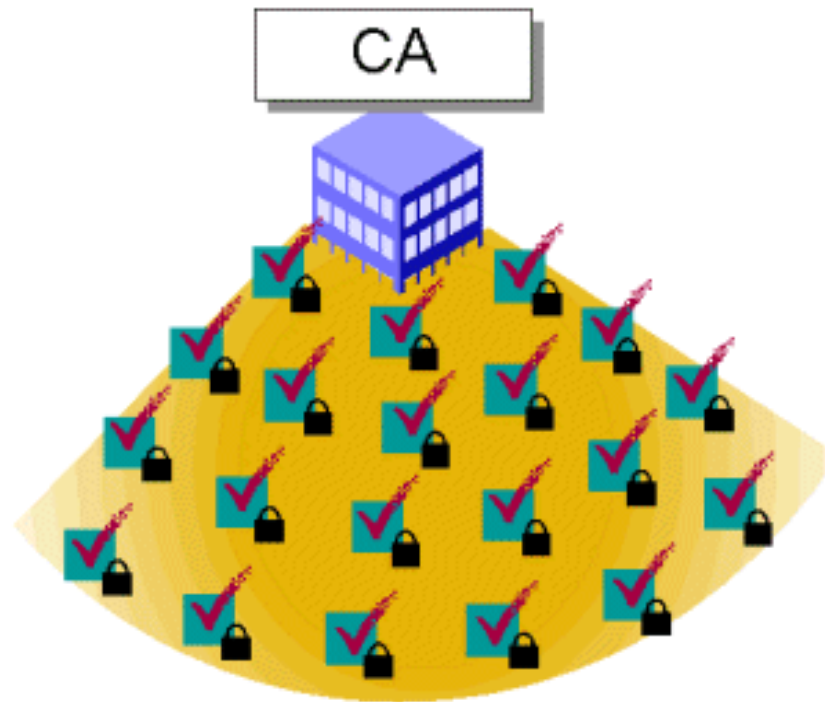
- توسط یک موجودیت قابل اعتماد صادر و امضاء شده است.
- بر اساس تائید هویتی است که توسط یک مرکز صورت گرفته است.
- حاوی یکسری اطلاعات و کلید عمومی شخص یا سازمان است.
- مورد استفاده آن در گواهی قید شده است.
- دارای مدت اعتبار مشخص و محدود است.



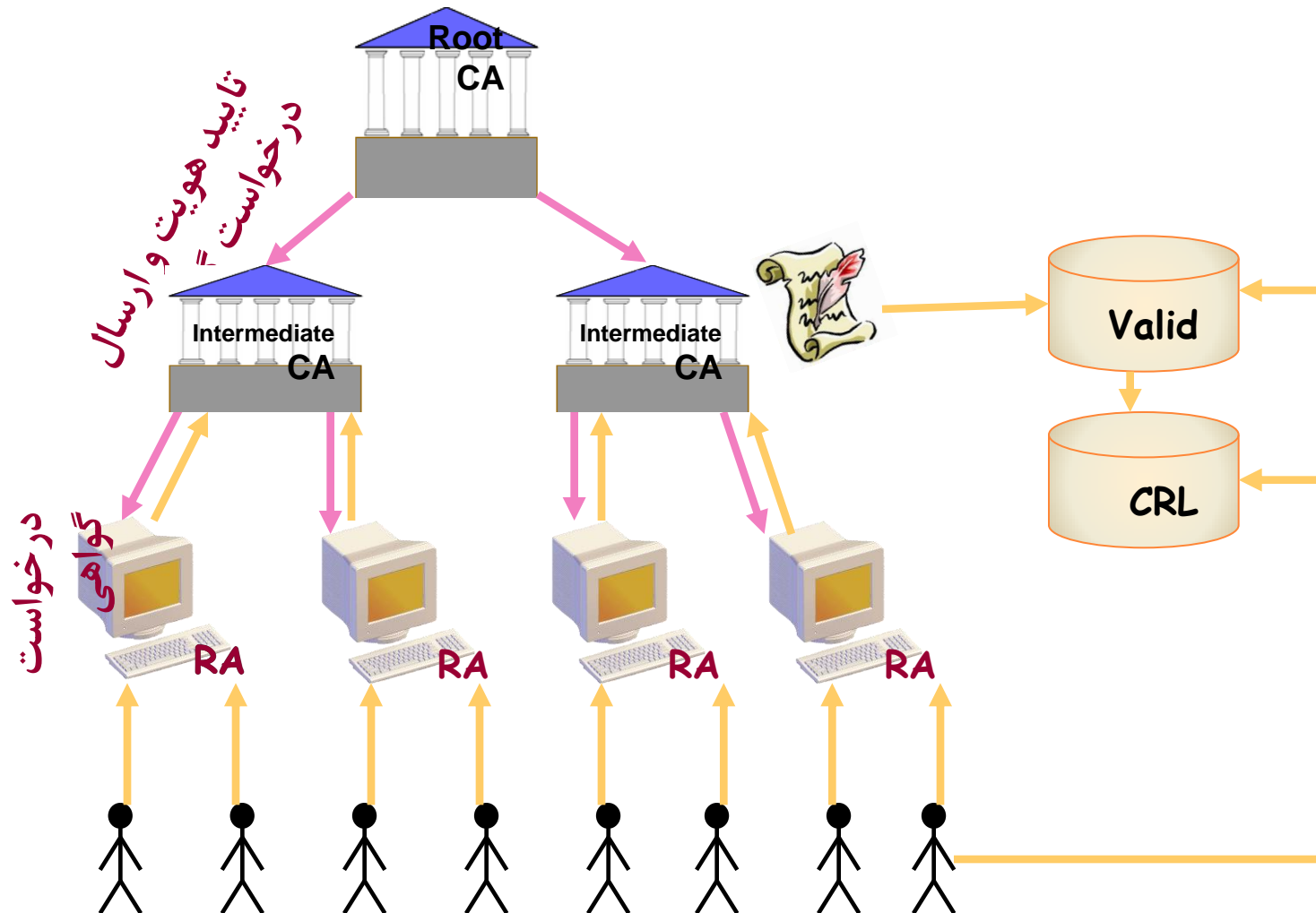
کارکرد گواهی دیجیتال

- 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 درمی‌آورد.
- 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.

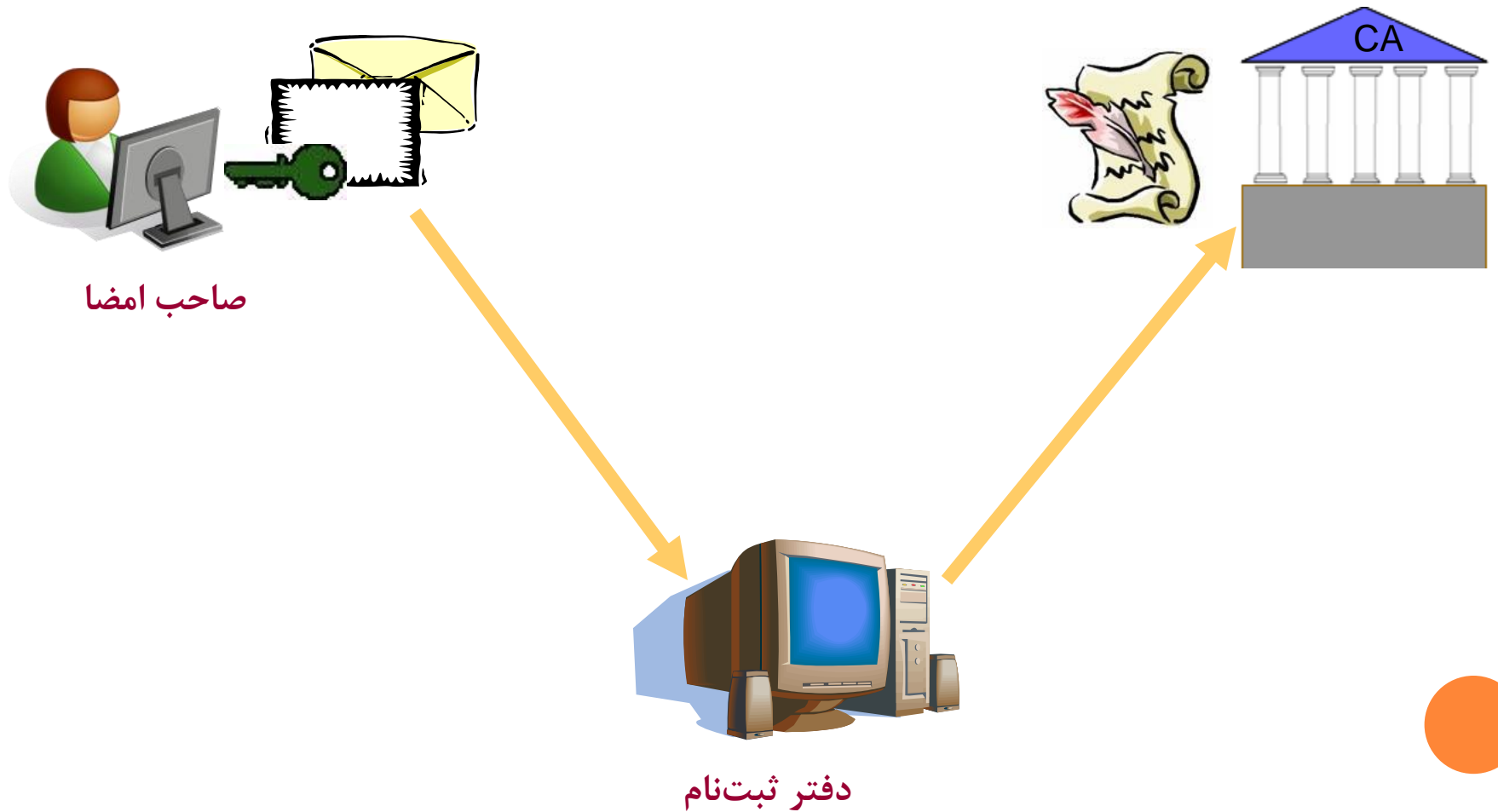
مرکز صدور گواهی



معرفی اجزاء و کارکرد آنها



فرآیند درخواست گواهی



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



DIGITAL SIGNATURE

```
graph TD; DS[DIGITAL SIGNATURE] --> PK[Public Key]; DS --> PRK[Private Key]; PK --- PKI[PKI  
Public Key Infrastructure]; PRK --- PKI; PKI --- PKD[Public Key  
can be distributed]; PKI --- PRKS[Private Key  
should be secret];
```

Public
Key

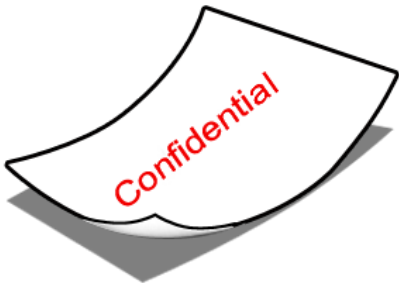
Private
Key

Public Key
can be distributed

PKI
Public Key Infrastructure

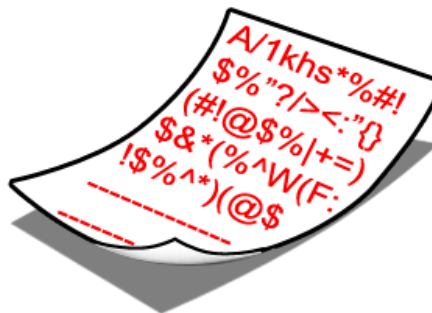
Private Key
should be secret

Encryption

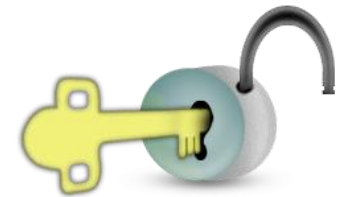
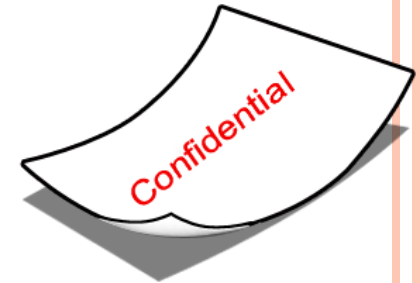


رمزگذاری

با استفاده از کلید عمومی



رمزگذاری شده (Encrypted)

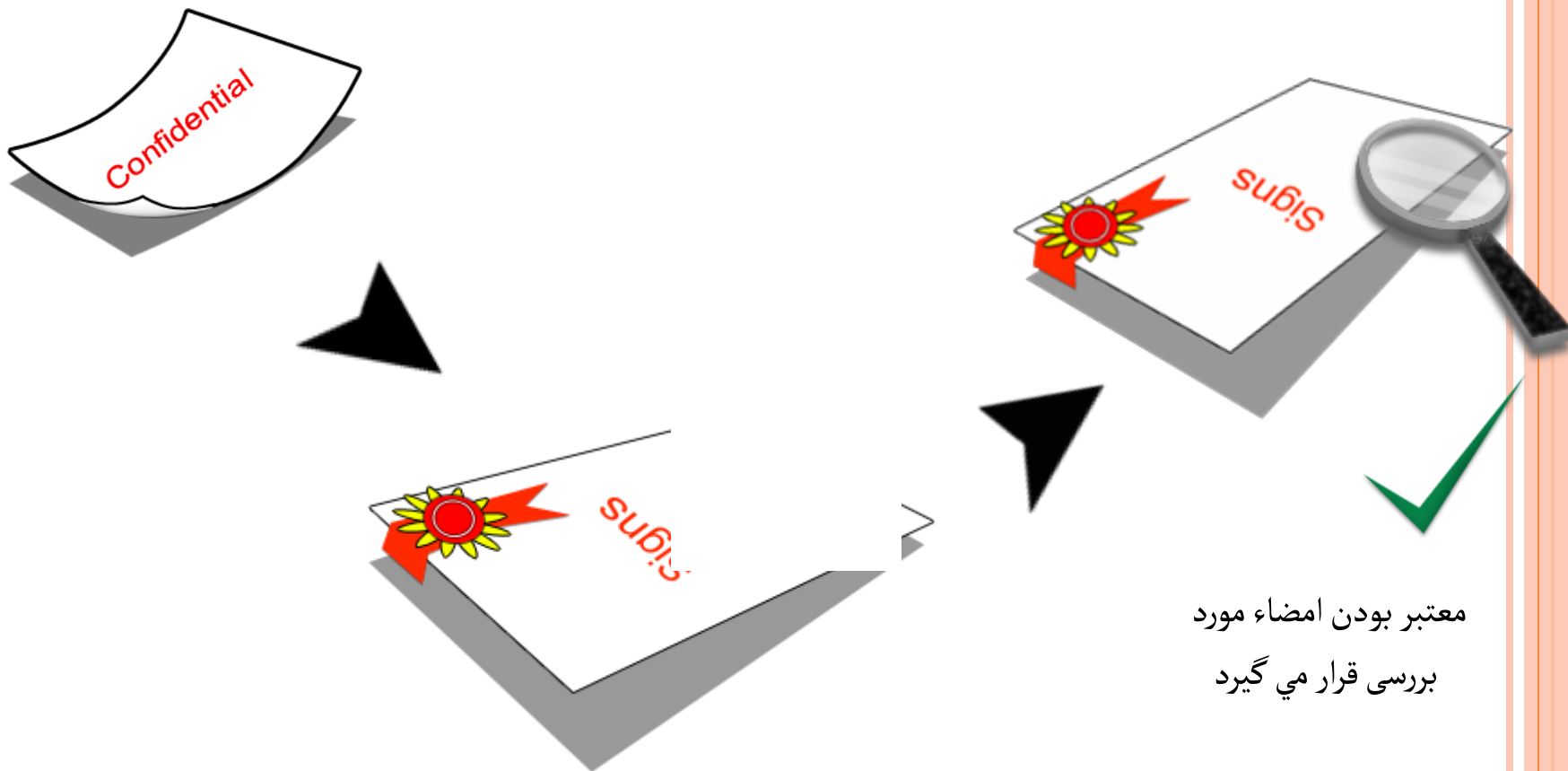


رمز گشایی

با استفاده از کلید خصوصی



Certification

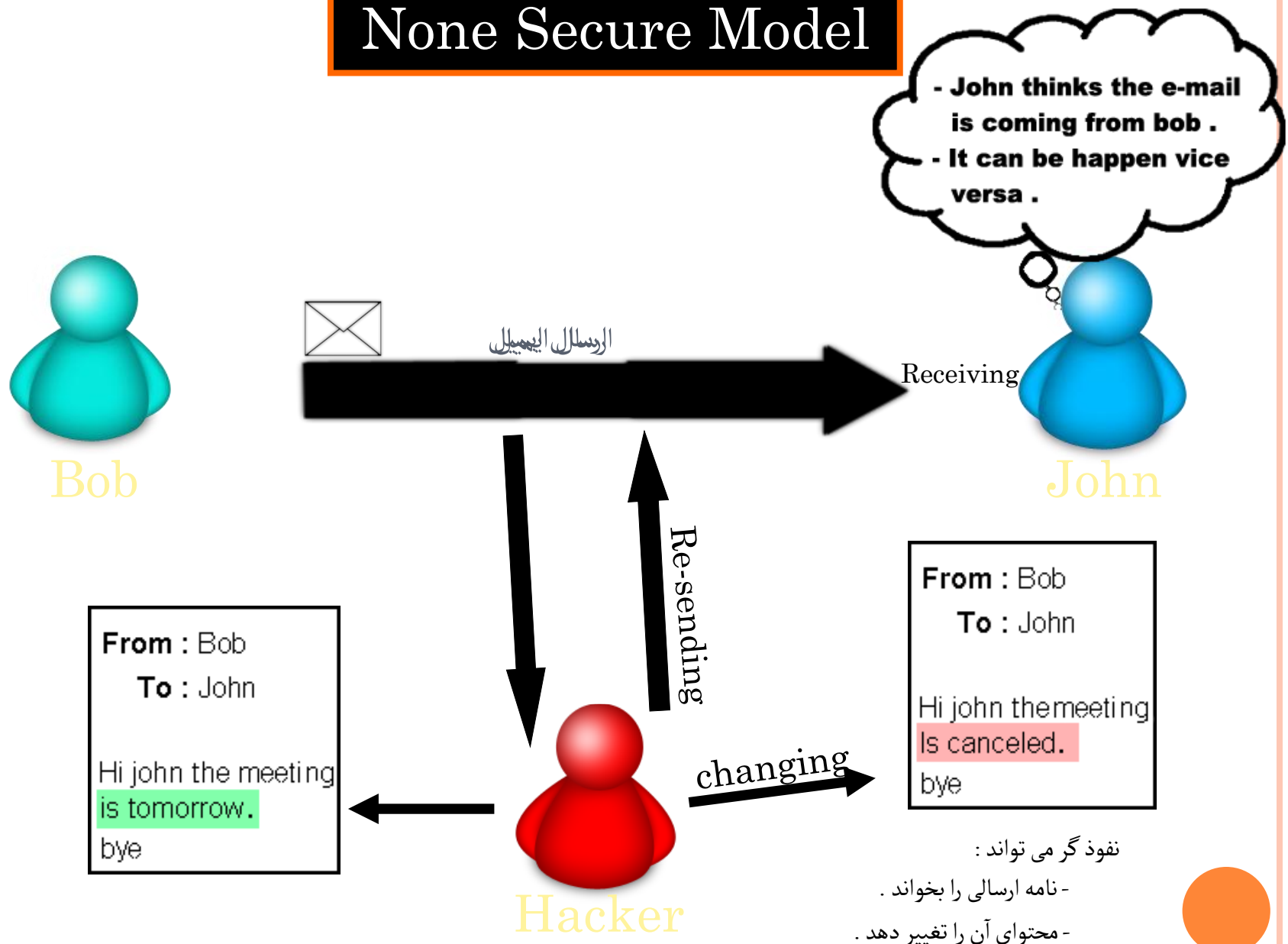


فرستنده پیام را امضاء می کند

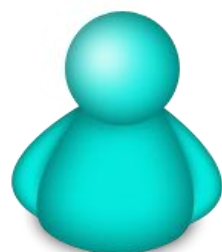
معتبر بودن امضاء مورد
بررسی قرار می گیرد



None Secure Model



Secure Model



Bob



ایمیل توسط کلید خصوصی

باب امضاء شده است.



ایمیل توسط کلید عمومی

جان امضاء شده است.

```
A.?:d"y-=@dg^
$&%_#$!Z"";I}[P|
\*-+@.?:h"-9@
dg^$&))$!Z"";&
%_#$_@.?:h$!Z"
';@!Z"";I}[Pd"y-57
```



ارسال ایمیل



John

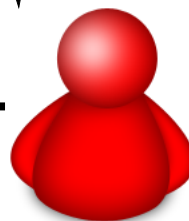
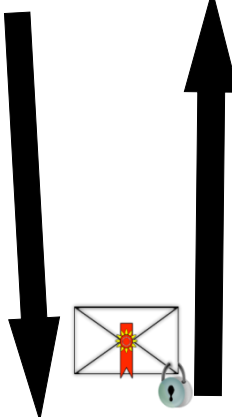
- "جان" ایمیل ارسالی را بدون تغییر دریافت میکند.

- کلید عمومی باب را دریافت میکند.

- ایمیل را توسط کلید خصوصی خود باز می کند.

- می تواند نامه امضاء و رمزگذاری شده برای "باب"

ارسال کند.



Hacker

- نفوذگر نامه ارسالی را ناخوانا می بیند چون

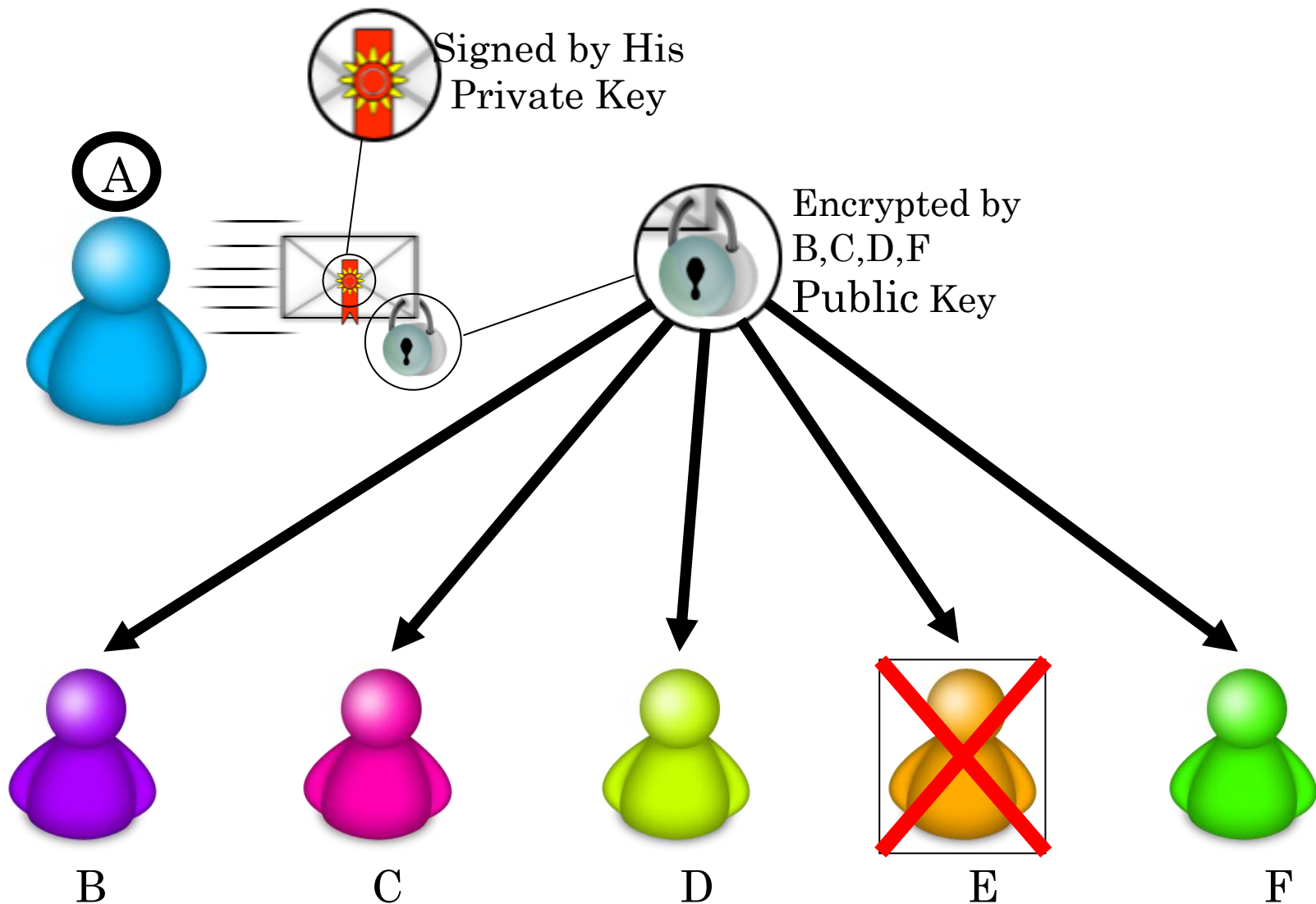
او کلید خصوصی "جان" (دریافت کننده) را

در اختیار ندارد.

- نفوذ گر نمیتواند نامه امضاء شده ارسال کند چون

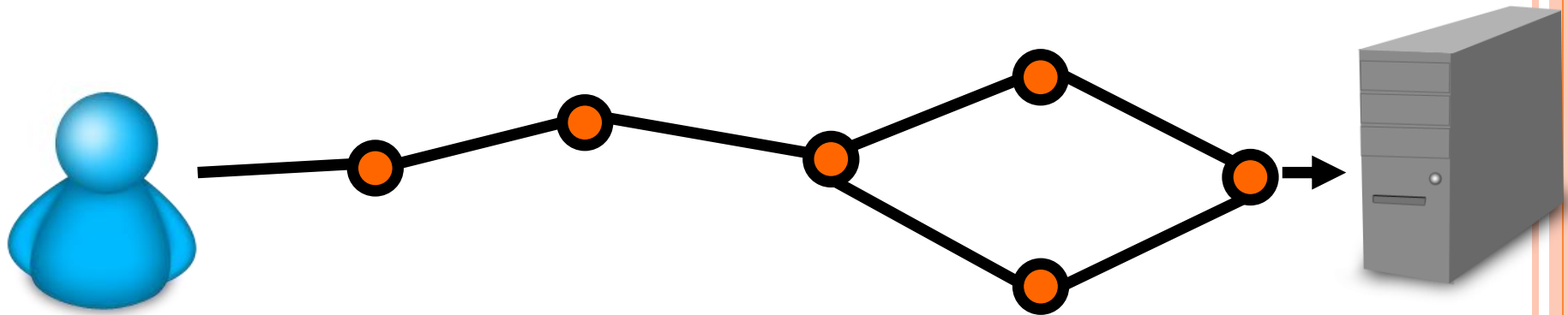
او کلید خصوصی "باب" (فرستنده) را ندارد.





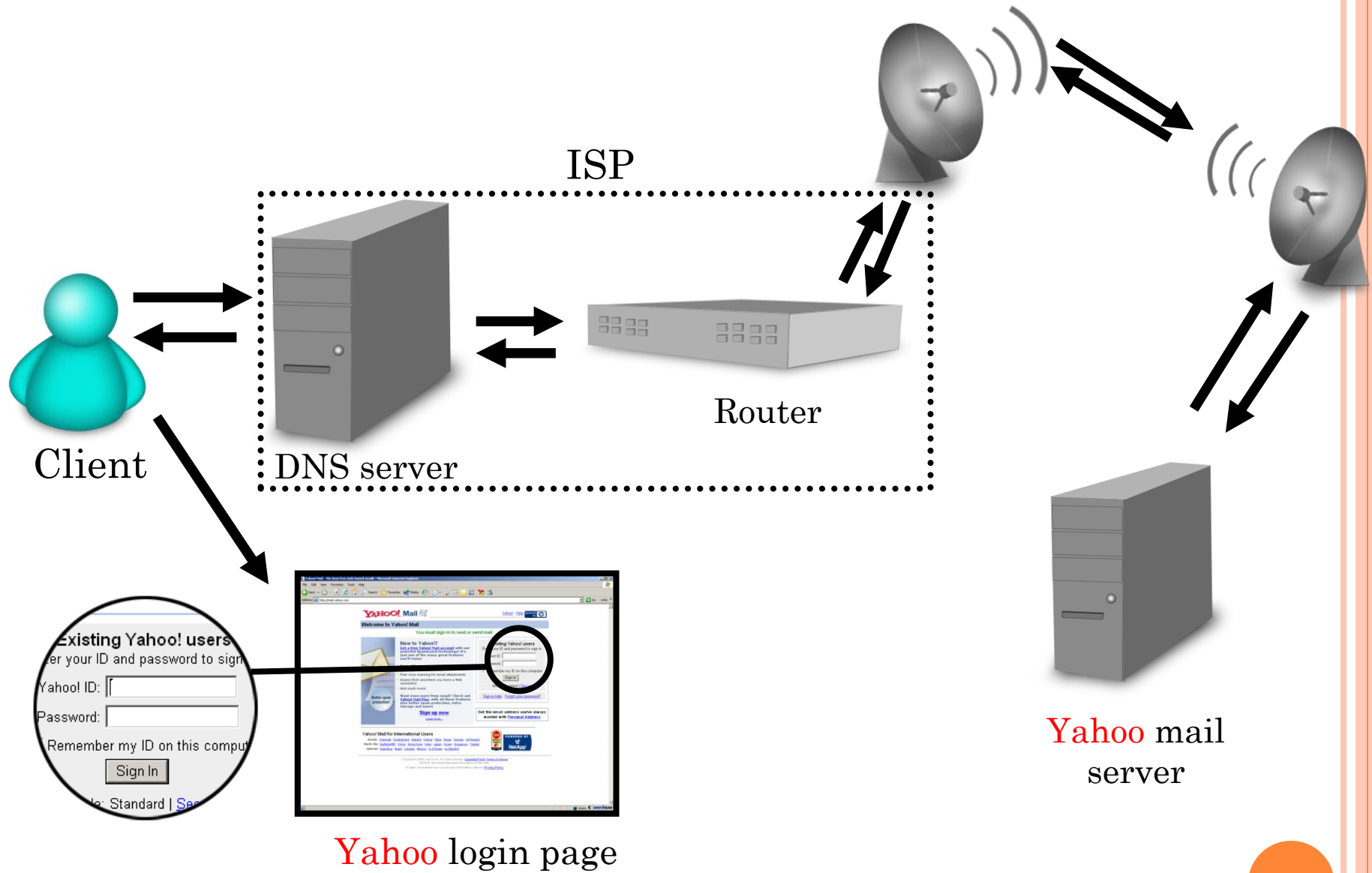
نمی تواند نامه را بخواند زیرا نامه با کلید
عمومی او رمزگذاری نشده است .

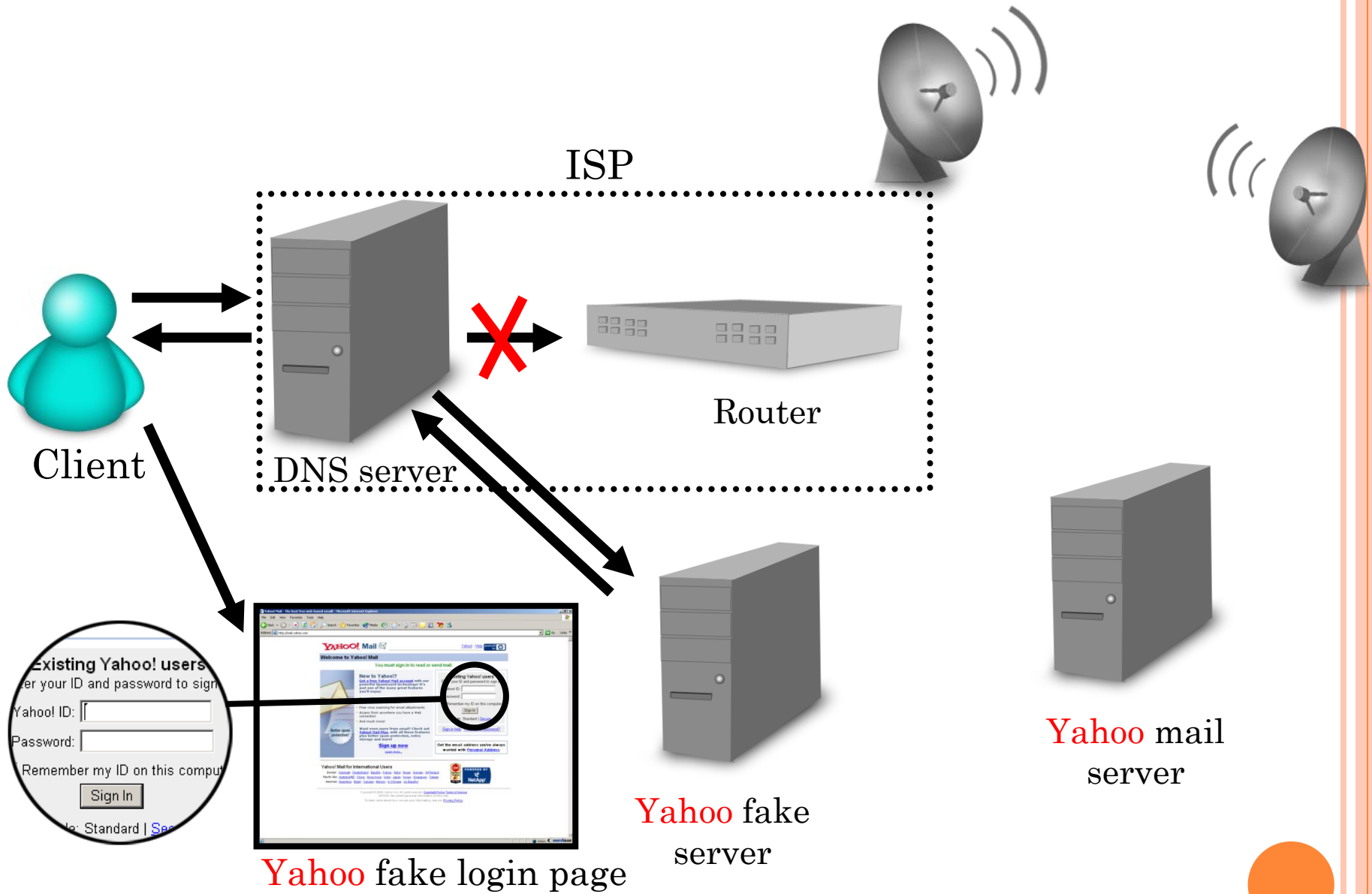




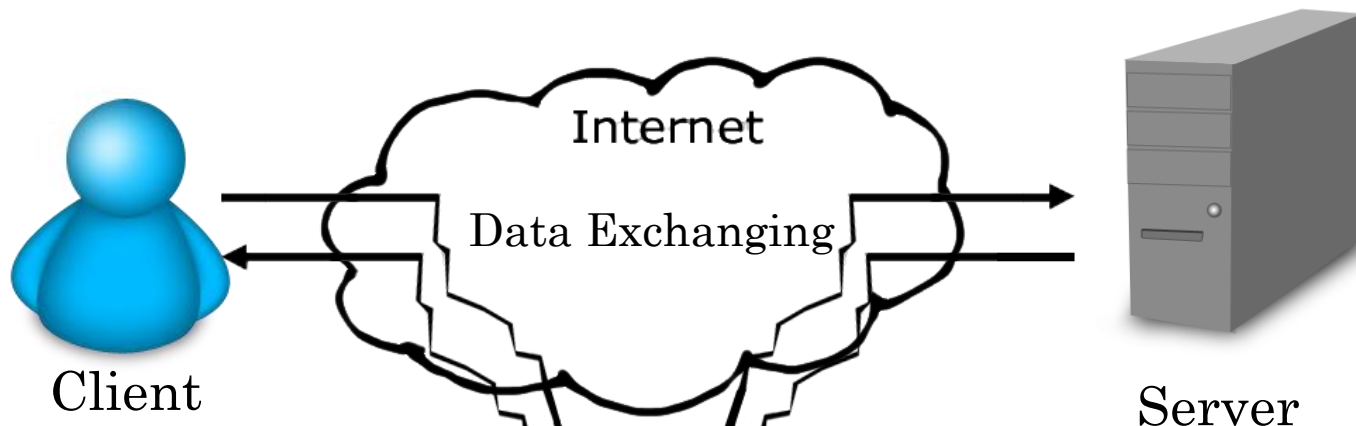
Server







None Secure Model



http session pocket

```
GET /u HTTP/1.1 Accept: image/gif, image/x-bitmap, image/jpeg, application/vnd.ms-excel, application/vnd.ms-powerpoint, application/msword, application/x-shockwave-flash, */* Accept-Language: fa Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; .NET CLR 1.0.3705) Host: aboo Connection: Keep-Alive HTTP/1.1 302 Object Moved Location: http://aboo/u/ Server: Microsoft-IIS/5.1 Content-Type: text/html Content-Length: 137
Object Moved
This document may be found hereGET /u HTTP/1.1 Accept: image/gif, image/x-bitmap, image/jpeg, image/pjpeg, application/vnd.ms-excel, application/vnd.ms-powerpoint, application/msword, application/x-shockwave-flash, */* Accept-Language: fa Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; .NET CLR 1.0.3705) Host: aboo Connection: Keep-Alive HTTP/1.1 200 OK Server: Microsoft-IIS/5.1 Date: Sat, 18 Oct 2003 15:16:26 GMT Content-Length: 420 Content-Type: text/html Set-Cookie: ASPSESSIONIDGGQGLNC=NGEBPLKANKGABPGDBDOOGPIB; path=/ Cache-control: private
Username :
Password :

POST /u/result.asp HTTP/1.1 Accept: image/gif, image/x-bitmap, image/jpeg, image/pjpeg, application/vnd.ms-excel, application/vnd.ms-powerpoint, application/msword, application/x-shockwave-flash, */* Referer: http://aboo/u/ Accept-Language: fa Content-Type: application/x-www-form-urlencoded Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; .NET CLR 1.0.3705) Host: aboo Content-Length: 48 Connection: Keep-Alive Cache-Control: no-cache Cookie: ASPSESSIONIDGGQGLNC=NGEBPLKANKGABPGDBDOOGPIB username=administrator&password=44gtfDs43&Submit=SubmitHTTP/1.1 100 Continue Server: Microsoft-IIS/5.1 Date: Sat, 18 Oct 2003 15:16:37 GMT HTTP/1.1 200 OK Server: Microsoft-IIS/5.1 Date: Sat, 18 Oct 2003 15:16:37 GMT Content-Length: 180 Content-Type: text/html Cache-control: private Welcome administrator
```

Can see the screen

Sniffer

Can affect
information

User name : --

Password : ---

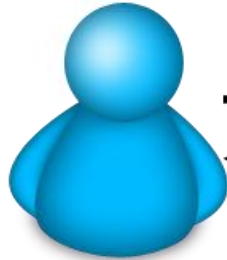
Catch user
Confidential
Information

User name : administrator


Password : =44gtfDs43

Changing Password-
Using the account Resources-

Secure Model



https session pocket



مواردی که در زمان ورود کاربر به یک شبکه امن مورد بررسی قرار می گیرد .



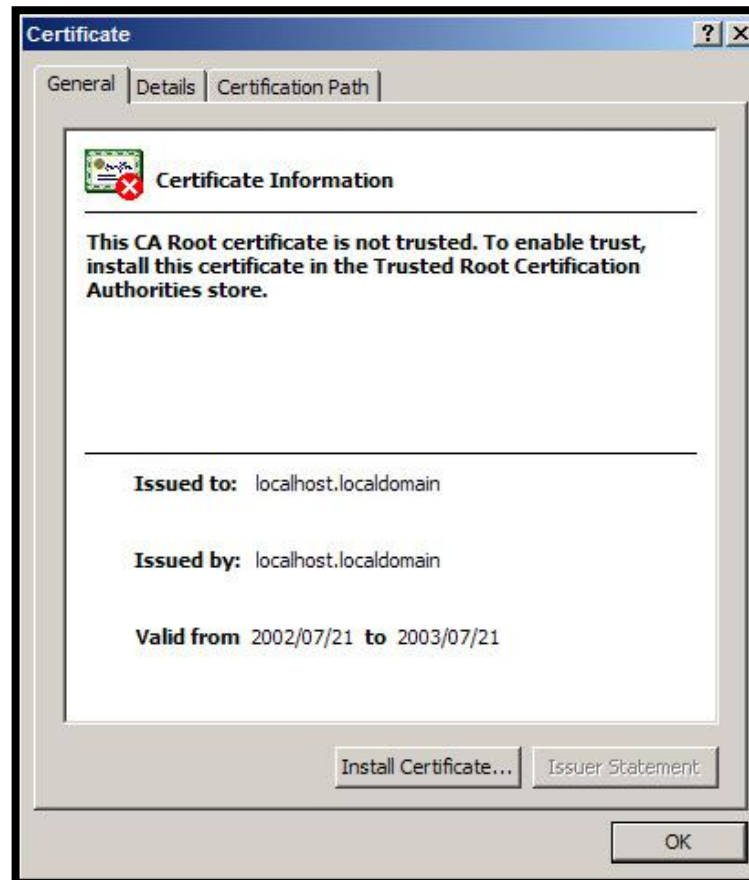
معتبر بودن صادر کننده
گواهینامه در صورتیکه صادر کننده
گواهینامه معتبر
نباشد پیام خطا نمایش داده میشود

استفاده کننده
نام سایت استفاده کننده
بایستی با نام مندرج در
گواهینامه یکسان باشد
در غیر اینصورت پیغام
خطا داده می شود

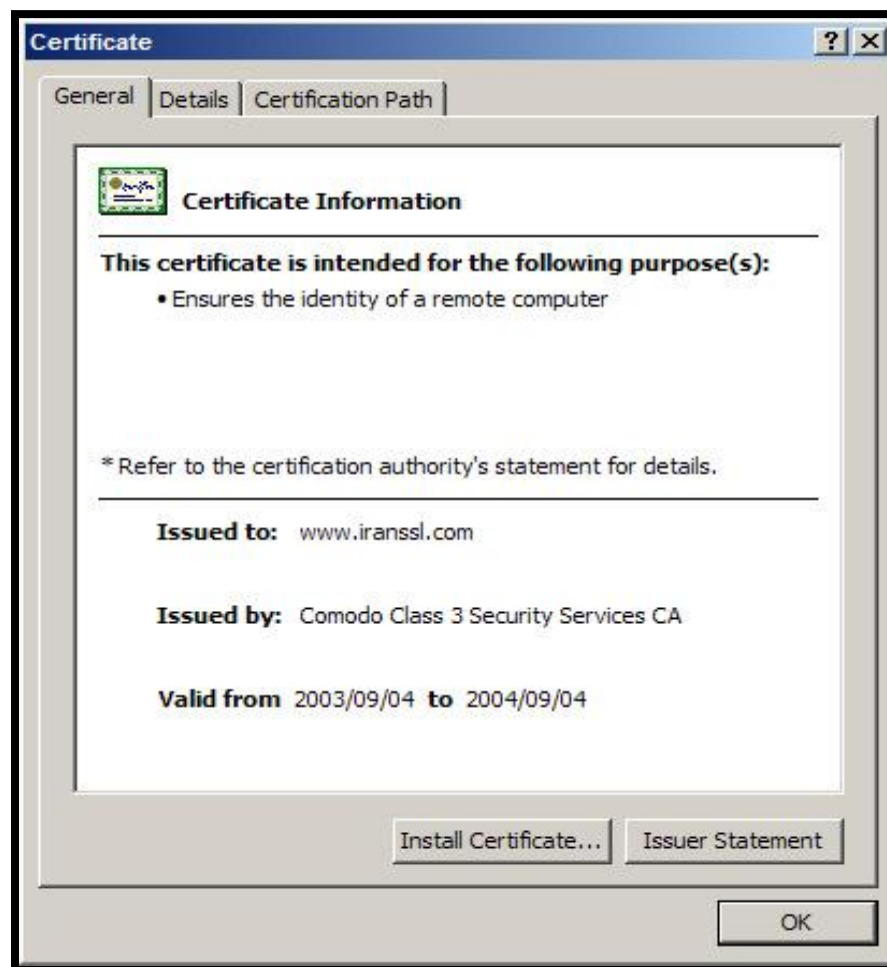
تاریخ اعتبار
در صورت گذشتن از
زمان تاریخ اعتبار
گواهینامه عدم اعتبار
آن به کاربر اعلام میشود



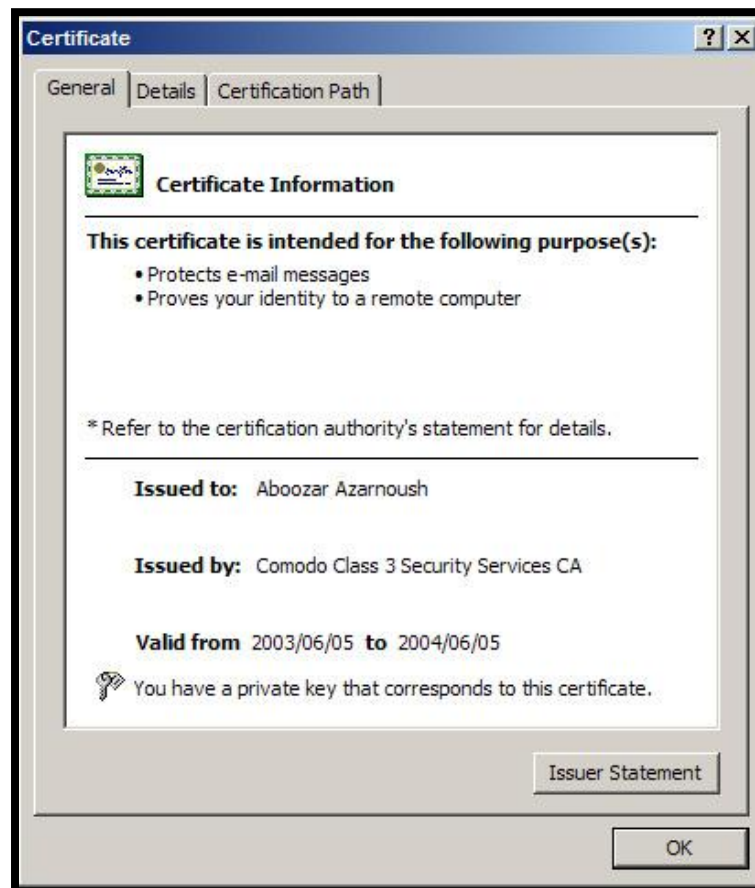
نمونه ای از گواهینامه غیر معتبر



نمونه ای از گواهینامه معتبر



نمونه ای از گواهینامه شخصی



صفحه ورود به سیستم با استفاده از گواهینامه شخصی

