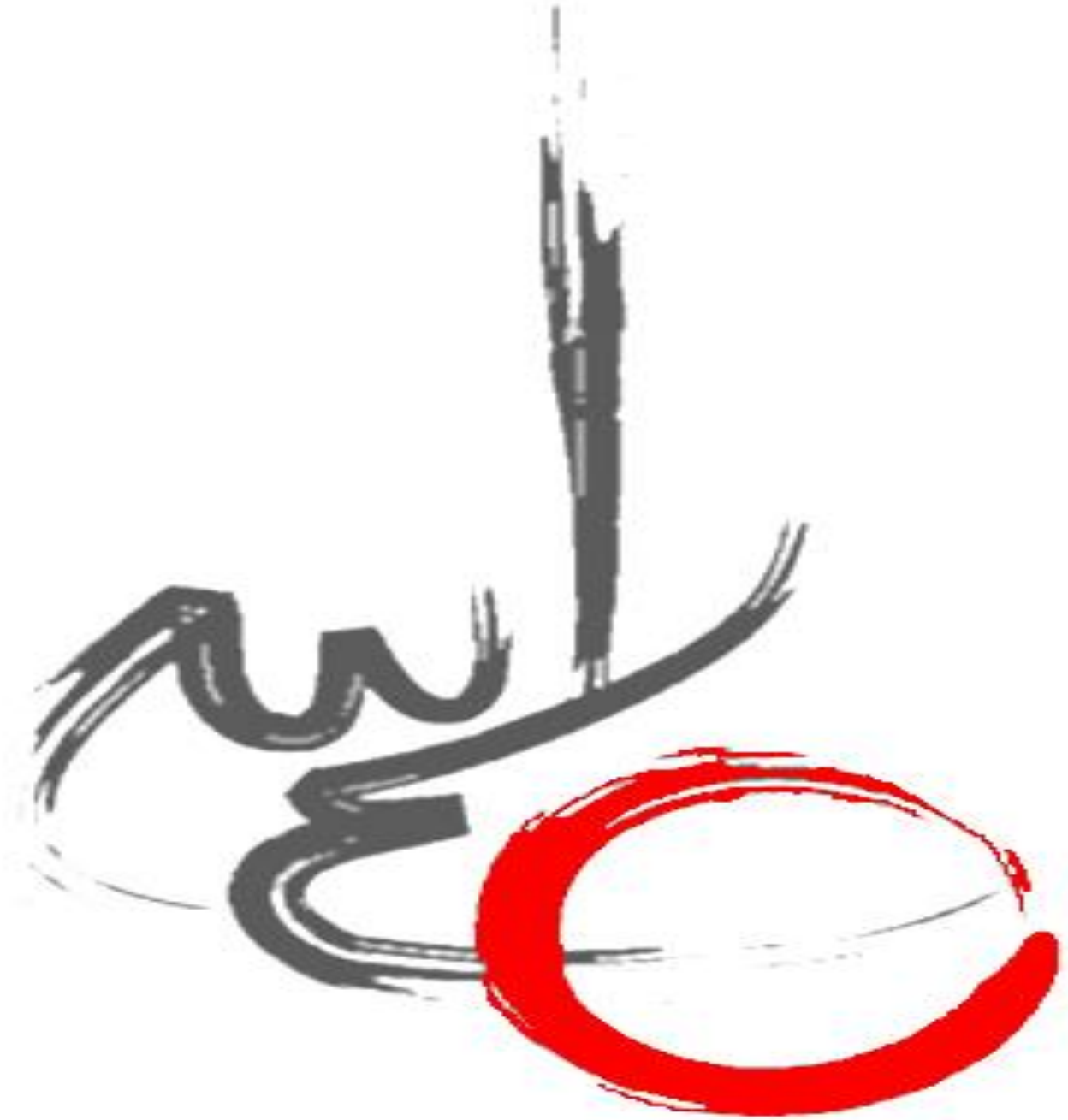
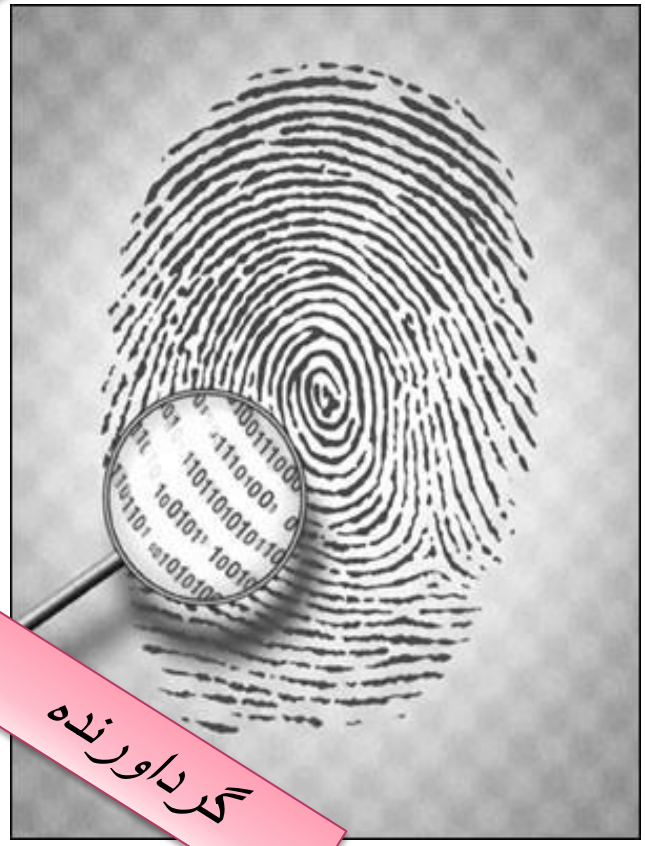


امضای الکتریکی

استاد مربوطه:



گردآورنده

عناوین

I. مقدمه

II. معرفی امضای دیجیتال

III. دلایل استفاده از امضای دیجیتال

IV. فرق امضای دیجیتال با دستی

V. پیاده سازی یک امضای دیجیتالی

VI. نتیجه گیری

مقدمه

- کاغذ به عنوان حامل اطلاعات مهم جای خود را کم‌کم به دیگر راههای تبادل اطلاعات می‌دهد. در واقع کاغذ دارای معایبی از قبیل انتقال آهسته و پرهزینه اسناد می‌باشد. همچنین شیوه‌های ذخیره‌سازی اطلاعات نیز بسرعت در حال تغییر است و بجای بایگانی انبوه دسته‌های کاغذ از روشهای الکترونیکی استفاده می‌شود.

- فن‌آوریهای جدید انتقال اطلاعات، مانند:پست الکترونیك، ارسال و ذخیره اطلاعات را ساده‌تر، سریعتر و حتی ایمن‌تر ساخته است.

معرفي امضاي ديجيتالي

- يکی از تکنولوژيهايی که موجب افزايش اعتماد گرديده، امضای ديجيتالی می‌باشد. اين تکنيك مبتنی بر رمزنگاری باعث به رسميت شناسی اطلاعات الکترونيکی شده به طوريکه هويت پديدآورنده سند و جامعيت اطلاعات آن، قابل بازبينی و کنترل می‌باشدوبخاطر ساختار غيرفيزيکی واسطه (وسيله حامل داده)، روشهای سنتی علامتگذاری فيزيکی واسطه توسط مهر يا امضاء (برای مقاصد تجاری و حقوقی) غيرقابل استفاده می‌باشند

- برای اینکه هویت فرستنده سند تایید شود و نیز برای اطمینان از اینکه سند در طول مدت انتقال به گیرنده دستکاری نشده است از امضای دیجیتالی استفاده می شود . میتوان کل یك سند و یا قسمتی از آن را امضا کرد .

دلایل استفاده از امضای دیجیتال

- به طور کلی سه دلیل برای استفاده از امضای دیجیتالی وجود دارد که شامل:

1- استفاده از کلید عمومی این اجازه را به هر شخصی می دهد که کلید خود را به سمت فرستنده اطلاعات بفرستد و سپس گیرنده پس از دریافت اطلاعا ت، آن را توسط کلید خصوصی خود بازگشایی میکند، بنابراین امضای دیجیتالی این امکان را مي دهد که فرستنده یا گیرنده مطمئن شوند که اطلاعات از محل یا شخص مورد نظر دریافت میشود .

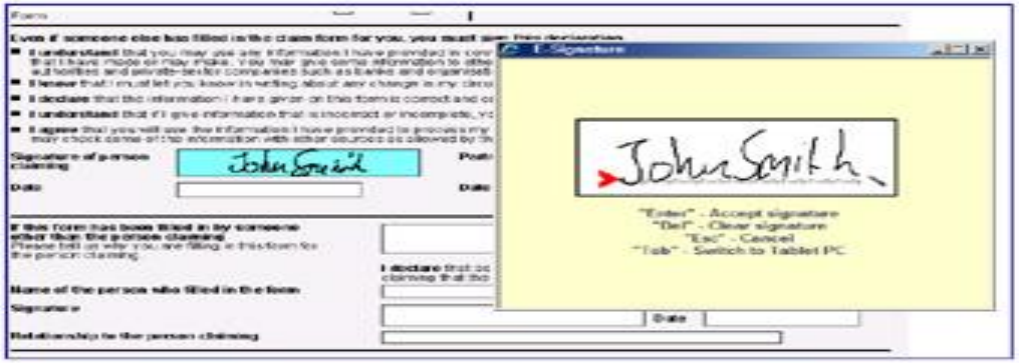
2- اطلاعات در طول مدت انتقال ممكن است توسط ديگران دستكاري شود . براي اينكه از صحت اطلاعات رسيده مطمئن شويم نياز به يك امضاي ديجيتالي در اين حالت احساس مي شود.

3 - رد كردن اطلاعات فرستاده شده . گيرنده اطلاعات براي اينكه مطمئن شود فرستنده بعدا از اطلاعاتي كه فرستاده اعلام بي خبري نكند و آنها را رد نكند از فرستنده يك امضا درخواست ميكند تا شاهدي بر اين ادعا باشد .

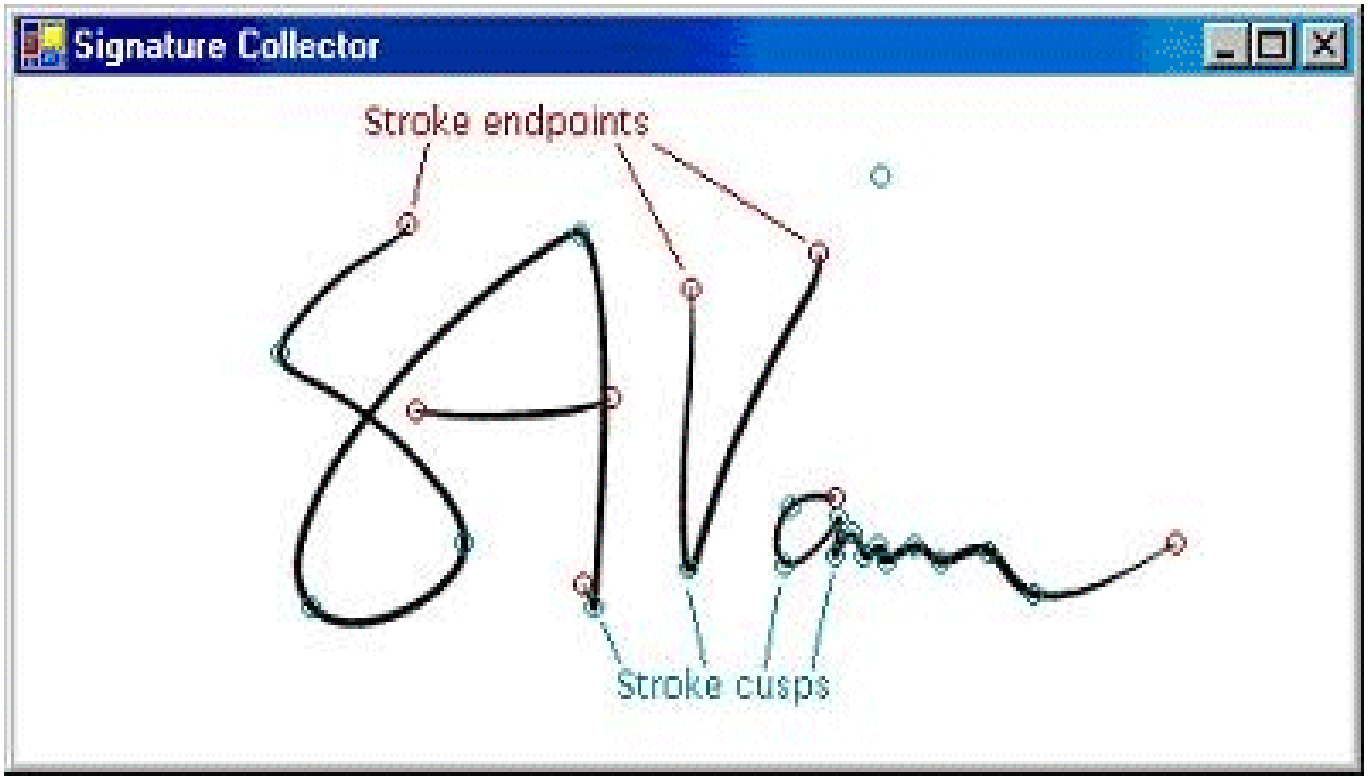
فرق امضای دیجیتالی با دستی

- 1) امضای دیجیتال نوعی رمزنگاری نامتقارن است که خصوصیات امضای دستی را در فضای مجازی فراهم می کند.
- 2) هر فرد در فضای مجازی دارای امضای دیجیتالی خاص خود است وتنها این فرد قادر به تولید این امضاست.

3) اما امضای دیجیتال دارای خصوصیات دیگری نیز هست که امضای دستی فاقد آن است.بوسیله امضای دیجیتال می توان مطمئن بود که محتوای سند یا پیغام تغییر نکرده وافراد غیر مجاز سند الکترونیکی مربوطه را مخدوش نکرده اند.این بدان دلیل است که امضای دیجیتال به ازای هر سند یا پیام وابسته به متن ،تولید می شود و امضای تولید شده برای هر سند، منحصر به فرد می باشد.



4) امضای دیجتال برای هر مستند یا پیغام بوسیله کلید خصوصی فرد تولید میشود و در واقع یک عدد با طول بلند است. کلید خصوصی فرد به صورت امن در وسیله ای مانند کارت هوشمند نگهداری می شود .بدین ترتیب جعل امضای دیجیتال بسیار مشکل تر از امضای دستی است.



- 5)توسط امضای دیجیتال سندیت خاصی به اسناد الکترونیکی داده می شود. بدین ترتیب می توان بصورت قابل اعتماد و مطمئن ارسال کننده سند را شناسایی کرد. در نتیجه اسناد الکترونیکی قابل پیگیری بوده وبه کمک آن فعالیت افراد در فضای مجازی جنبه حقوقی پیدا می کند وقوانین حقوقی اسناد کاغذی در مورد اسناد الکترونیکی قابل اجرا می شود.

6) از طرف دیگر با توجه به عدم امکان جعل امضای دیجیتال،اسناد یا پیام های امضا شده قابل انکار از طرف امضا کننده نیست.بدین وسیله مراجع قضایی می توانند از این خصوصیت جهت استناد قانونی به سند الکترونیکی استفاده کنند.

برای پیاده سازی یك امضای دیجیتالی نیاز به سه الگوریتم داریم :

A. یك الگوریتم برای ایجاد کلید
B. الگوریتم برای ایجاد امضا
C. الگوریتم برای تایید امضا

برای ایجاد یك امضای دیجیتالی باید یك عدد checksum برای سند مورد نظر محاسبه شود.

برای مثال

فرض کنید مینا قصد ارسال یك پیام به سارا را دارد

مینا پیام خود را همراه با امضای دیجیتالی براي سارا می فرستد.

این امضای دیجیتالی توسط کلید خصوصی که مالك آن مینا می باشد ایجاد شده است . در سمت دیگر سارا با استفاده از الگوریتم تایید امضا و کلید عمومی که از مینا دریافت کرده صحت امضا و اینکه امضا از طرف مینا می باشد را تایید میکند.

جمع بندی

- در جهان امروز مدیریت اسناد الکترونیکی و ارسال ودریافت اطلاعات الکترونیکی بخش بزرگی از تبلیغات و فعالیت‌های اجرایی را شامل می‌شود. استفاده از اطلاعات مبتنی بر کامپیوتر در سطح جهان به طرز قابل توجهی در حال گسترش می‌باشد. یکی از تکنولوژیهایی که موجب افزایش اعتماد گردیده، امضای دیجیتالی می‌باشد. این تکنیك مبتنی بر رمزنگاری باعث به رسمیت شناسی اطلاعات الکترونیکی شده به طوریکه هویت پدیدآورنده سند و جامعیت اطلاعات آن، قابل بازبینی و کنترل می‌باشد.

- در نتیجه می توان مستندات،پیغام ها وداده های الکترونیکی را توسط امضای دیجیتال تایید کرده و سندیت بخشید،به شکلی که مطمئن بود که تولید کننده امضا چه کسی است ومتن پیغام امضا شده،پس از امضا تغییر نکرده است. بدین وسیله متن سند یا پیغام امضا شده قابل استناد وپیگیری بوده وغیرقابل انکار است.

پایان