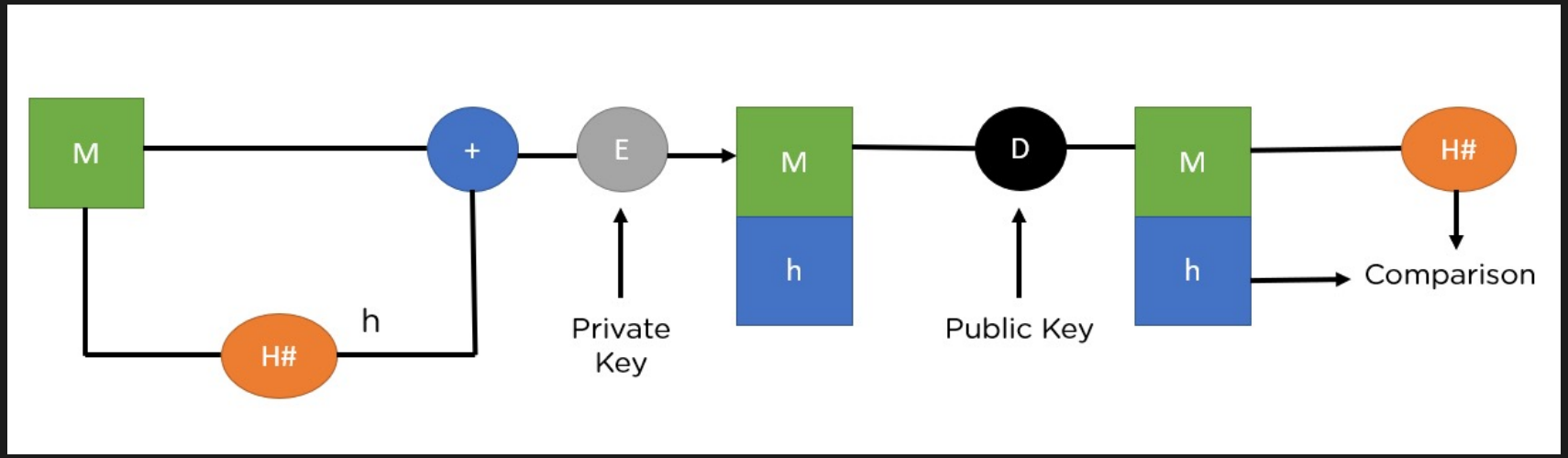
الگوریتم DSA

Digital Signature Algorithm

پویا ستاری

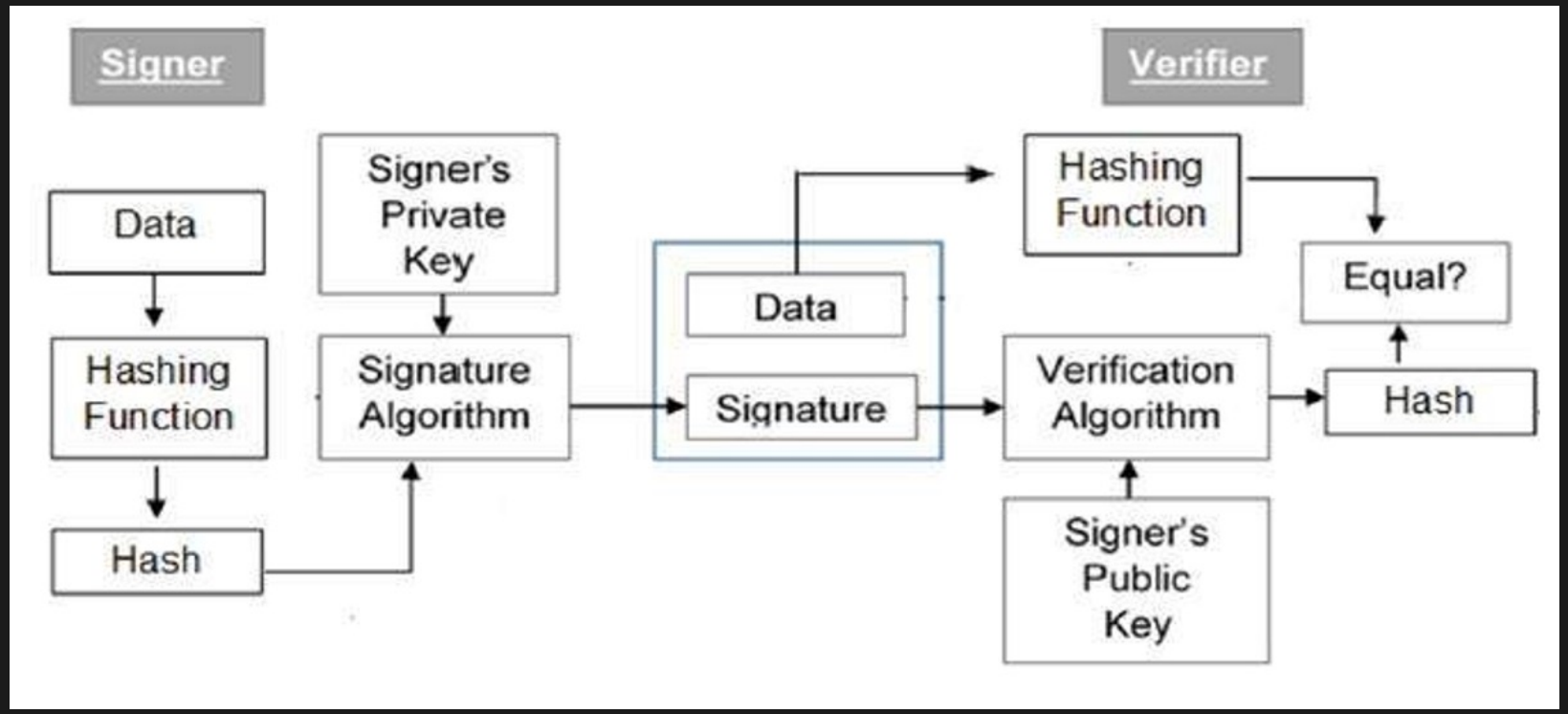
امضای دیجیتالی



M - Plaintext
H - Hash function
h - Hash digest

'+' - Bundle both plaintext and digest
E - Encryption
D - Decryption

خلاصه ای از روند امضاهای دیجیتالی



خلاصه ای از روند امضاهای دیجیتالی

a) مصرف کننده یک کلید جفتی رمز نویسی منحصر به فردی را به وجود میآورد و یا اینکه این کلید ها به او داده میشود.

b) شخص امضاء کننده یک پیامی را بر روی کامپیوتر مهیا و آماده میکند (برای مثال، به شکل یک پیام در پست الکترونیکی)

c) امضاء کننده یک خالص های از پیام را با استفاده از یک الگوریتم بازسازی ایمن آماده سازی میکند. ایجاد امضای دیجیتالی از یک نتیجه بازسازی که از پیام امضاء شده مشتق میشود استفاده میکند.

d) شخص امضاء کننده با استفاده از یک کلید خصوصی، خلاصه پیام را کشف رمز میکند. کلید خصوصی برای متن خلاصه شده پیام با استفاده از یک الگوریتم ریاضی گونه بکار برده میشود. امضاهای دیجیتالی شامل خلاصه پیامهای کشف رمز شده میشوند.

e) شخص امضاء کننده به طور برجسته، امضای دیجیتالی اش را به پیام نزدیک میکند و یا به آن ضمیمه میکند.

f) شخص امضاء کننده در اصل امضای دیجیتالی و پیام را به طور الکترونیکی به شخص مورد اعتماد میفرستد.

خلاصه ای از روند امضاهای دیجیتالی

g) شخص مورد اعتماد، کلید عمومی شخص امضاء کننده برای تصدیق و تصویب کردن امضا های دیجیتالی شخص امضاء کننده بکار میرود .تصدیق و تصویب با استفاده از کلید عمومی شخص امضاء کننده یک سطح ضمانت تکنیکی را فراهم میکند که پیام را از امضاء کننده میآورد.

h) شخص مورد اعتماد یک خالص های از پیام را با استفاده از الگوریتم بازسازی مشابه به وجود میآورد.

i) شخص مورد اعتماد دو نوع خلاصه پیام را باهم مقایسه میکند .اگر آنها یکسان باشند، آنگاه شخص مورد اعتماد میداند که پیام بعد از اینکه امضاء میشود هیچ تغییری پیدا نکرده است حتی اگر ذره ای در پیام بعد از اینکه آن به صورت دیجیتالی امضاء شده است، تغییر ایجاد شده، پیام خلاصه شده توسط شخص مورد اعتماد امضاء کننده متفاوت میشود.

تاییدیه امضای دیجیتالی

تأییدیه های دیجیتالی شامل کلید همگانی مالک، نام مالک، تاریخ انقضاء تأییدیه، نام نهاد رسمی تائید کنندهای که تأییدیه دیجیتالی را صادر کرده است، یک شماره سریال و سایر اطلاعات میباشد

یک تأییدیه از چهار بخش تشکیل شده است:

۱ .موضوع و خصوصیات آن

۲.اطلاعات کلید همگانی

۳ .مقام تأیید کننده امضاء

۴ .تاریخ انقضای تأییدیه

هر تأییدیه دارای تاریخ انقضایی میباشد. پس از انقضاء تاریخ تأییدیه، محتویات آن دیگر از طرف CA مربوطه، تضمین نمیشود.

نتیجه گیری

یکی از تکنولوژی هایی که موجب افزایش اعتماد در تجارت الکترونیک گردیده، امضای دیجیتال میباشد. این تکنیک مبتنی بر رمزنگاری باعث به رسمیت شناسی اطلاعات الکترونیکی شده به طوریکه هویت پدیدآورنده سند و جامعیت اطلاعات آن قابل بازبینی و کنترل میباشد. امضای دیجیتال، الگوریتم ها و سیستمهای آن در تئوری به خوبی مطرح شده اند. در تجارت الکترونیکی «مدارک الکترونیکی» دارای جایگاهی همانند اسناد مکتوب هستند لذا امضا در این مدارک علی االصول دارای ارزش اثباتی میباشد.