سیستم های اطلاعاتی حسابداری

نویسندگان:

دکتر مهدی مرادی

(دانشیار دانشگاه فردوسی مشهد)

نعیمه بیات

بسم الله الرحمن الرحیم

فصل نهم:

کنترل در سیستم های اطلاعاتی رایانه ای

محرمانگی داده ها و حفظ حریم خصوصی

پس از مطالعه این فصل، خواننده با مفاهیم ذیل آشنا می شود:

۱. آشنایی با مفاهیم حفظ محرمانگی اطلاعات یا سیستم
۲. آشنایی با انواع روش‌های حفظ محرمانگی اطلاعات
۳. آشنایی با اهمیت حفظ حریم خصوصی و اصول پذیرفته شده درباره حفظ حریم خصوصی
۴. آشنایی با انواع روش‌های رمزنگاری
۵. آشنایی با شبکه‌های خصوصی مجازی
۶. آشنایی با انواع کنترل‌های انتقال داده‌ها

خدمات امنیت محرمانگی به صورت ممانعت از انتشار غیرمجاز داده تعریف می‌شود. این خدمات این اطمینان را به وجود می‌آورد که اطلاعات در اختیار افراد غیرمجاز و یا پردازش‌های غیرمجاز قرار نمی‌گیرد.

مراحل پیاده سازی امنیت در رابطه با اطلاعات

شناسایی وطبقه بندی اطلاعات

اطلاعات را باید به گونه‌ای طبقه‌بندی کرد که اهمیت، اولویت و درجه‌بندی حفاظت از هر دسته از آن‌ها به طور کامل مشخص باشد.

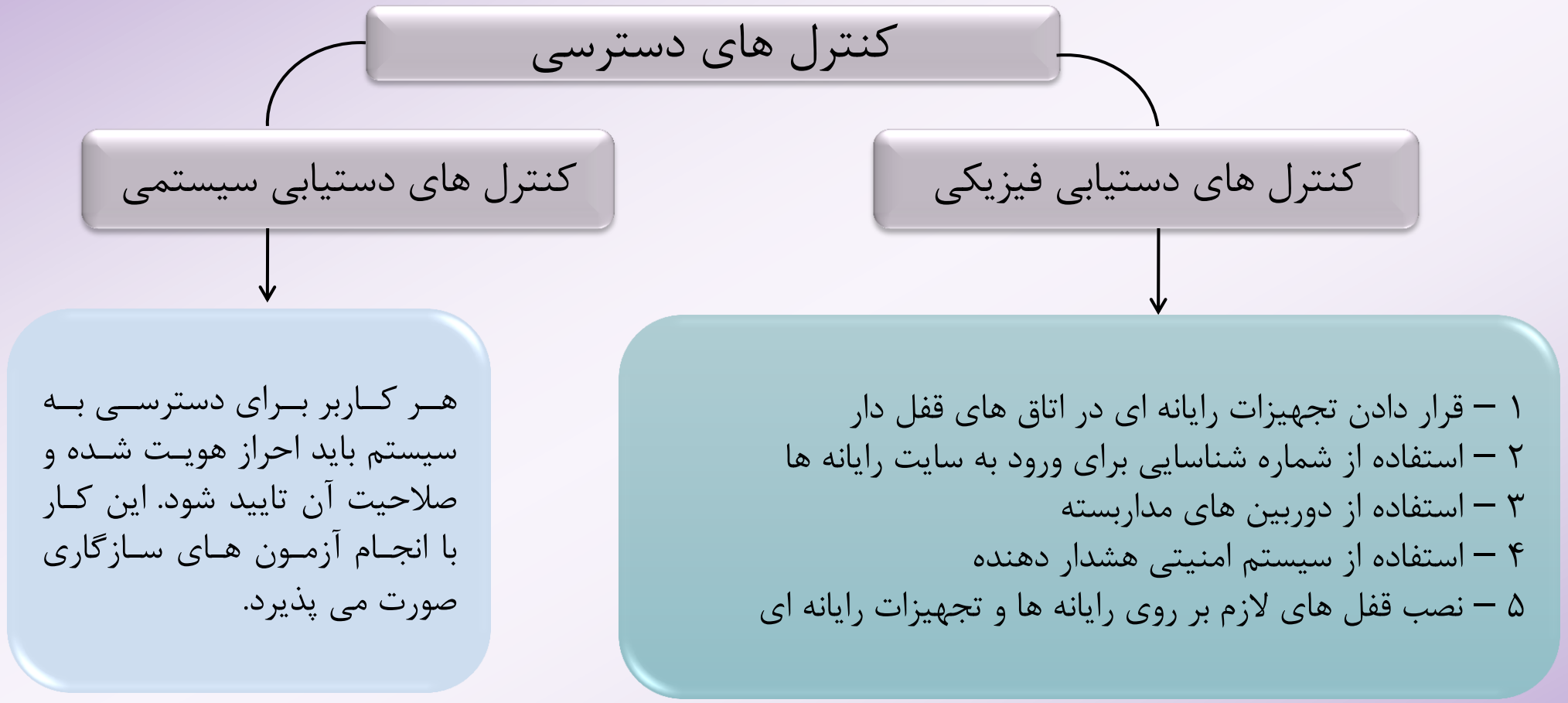
حفظ محرمانگی اطلاعات با رمزنگاری

رمزنگاری برای حفظ محرمانگی اطلاعات و به عنوان یکی از کنترل‌های پیش‌گیرانه می‌تواند مورد استفاده قرار گیرد.

کنترل دسترسی به اطلاعات حساس

هدف از کنترل دسترسی، دادن اجازه دسترسی بـه افـراد و وسایل مجاز و عدم پذیرش افراد غیرمجاز است.

سومین مرحله پیاده سازی امنیت : کنترل دسترسی به اطلاعات حساس



آزمون سازگاری مشخص می کند که آیا کاربری که سعی در فعال کردن سیستم دارد، مجاز به ورود به سیستم و انجام کار است یا خیر.

مشخصات کاربر		دسترسی و تغییر در فایل‌های				
شماره شناسایی	کلمه عبور	فایل حقوق و دستمزد	فایل فروش	فایل موجودی کالا	فایل اسامی کارمندان	فایل اسامی فروشندگان
۹۱۲۲۱	FG25	۰	۱	۰	۰	۰
۹۱۲۰۸	EBHZ	۱	۰	۰	۱	۰
۹۱۲۵۹	SMBF	۱	۱	۱	۱	۱

آموزش کارمندان

کلیه کارمندان سازمان باید آموزش‌های مناسب را در زمینه حفظ امنیت اطلاعات فرا گرفته و در جریان مقررات و رویه‌های تعیین شده بر اساس سیاست‌های امنیتی سازمان قرار بگیرند.

حفظ حریم خصوصی

برخی از اطلاعات جمع‌آوری شده توسط سازمان‌ها مربوط به اطلاعات شخصی افراد است که سازمان باید در رابطه با آن‌ها اقدامات حفاظتی لازم را اعمال نماید.


اصول پذیرفته شده درباره حفظ حریم خصوصی
اطلاع رسانی در مورد روش های حفظ حریم خصوصی
کسب رضایت افراد
حدود جمع آوری اطلاعات
استفاده و نگهداری از اطلاعات
دسترسی به اطلاعات
افشا اطلاعات برای اشخاص ثالث
امنیت اطلاعات
کیفیت
نظارت و اجرا
مسئولیت مدیریت

فاکتورهای مهم در استحکام رمزنگاری

- طول کلید
- الگوریتم رمزنگاری
- مدیریت حفاظت از کلیدهای رمزنگاری

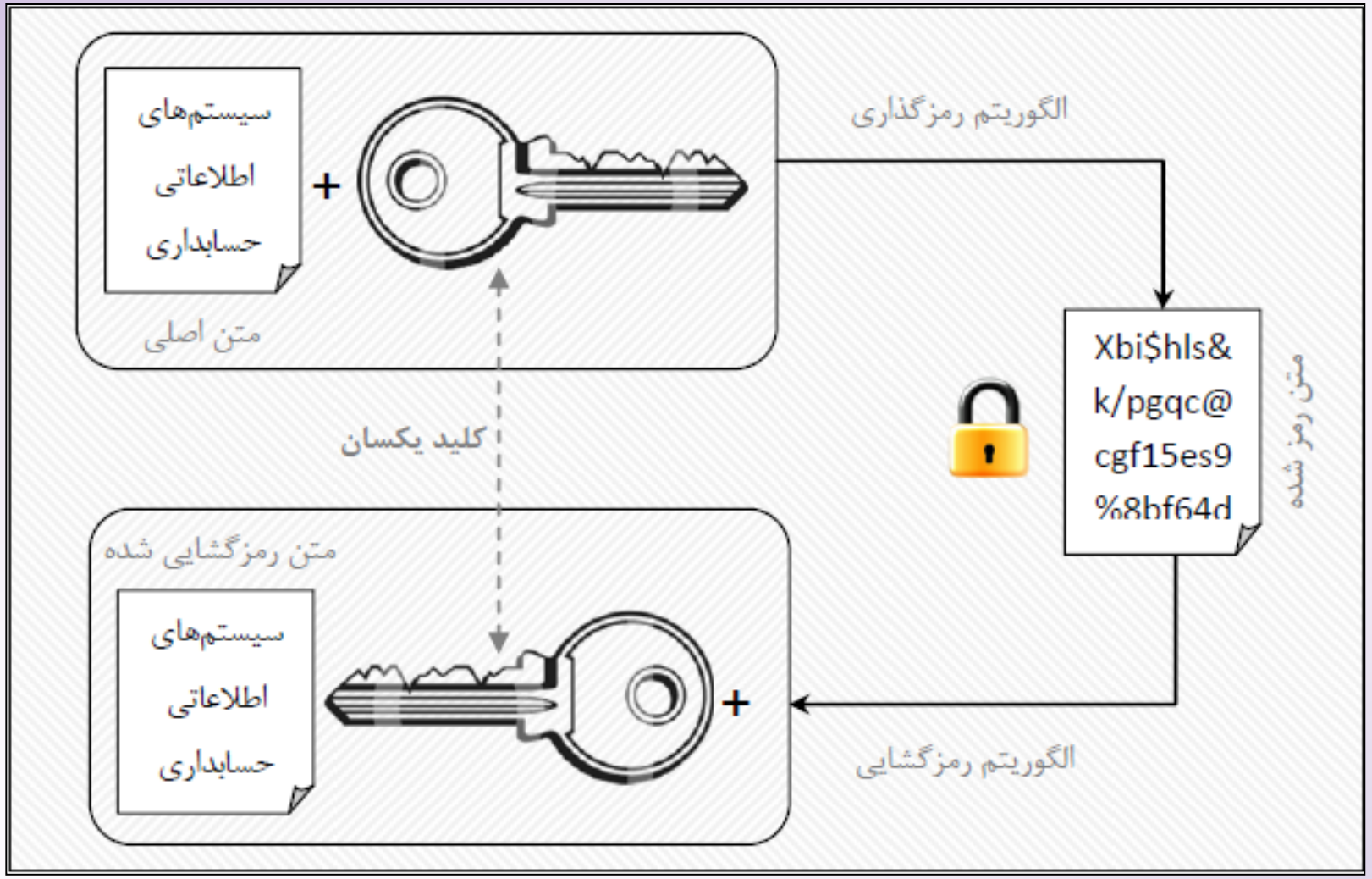
انواع الگوریتم های رمزنگاری

رمزنگاری متقارن- کلید اختصاصی

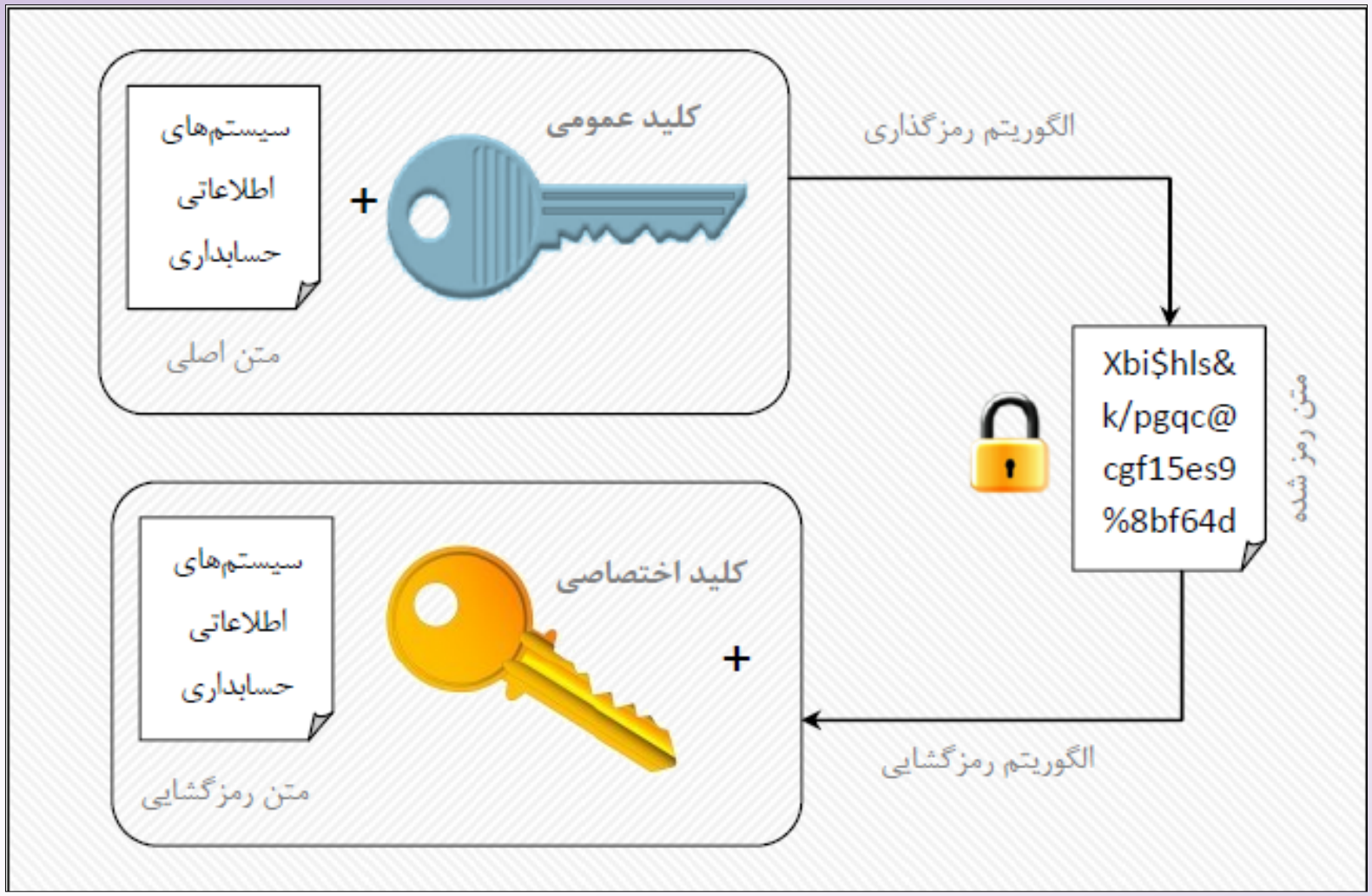
- در رمزنگاری با الگوریتم‌های متقارن استفاده از یک کلید مشابه برای به رمز درآوردن و رمزگشایی الزامی است.
- این موضوع امکان سرّی بودن کلید را از بین می‌برد و ممکن است اطلاعات توسط افراد غیرمجاز رمزگشایی شود.

رمزنگاری نامتقارن- کلید عمومی

- در این روش از دو کلید استفاده می‌شود.
- یک کلید مشترک یا عمومی که برای هرکسی قابل دسترسی است و یک کلید اختصاصی که تنها برای کاربر قابل شناسایی است.
- از یک کلید برای رمزنگاری و از دیگری برای رمزگشایی استفاده می شود.



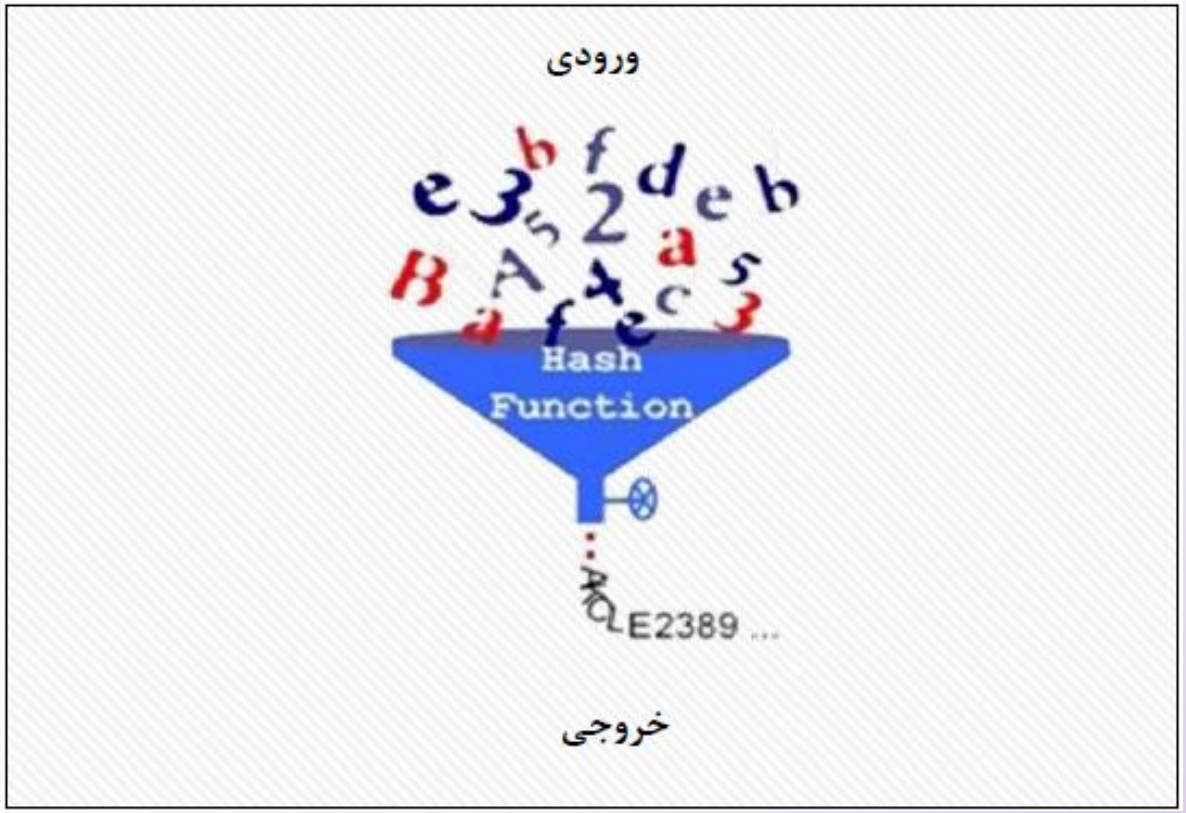
رمزنگاری متقارن



رمزنگاری نامتقارن

درهم سازی

درهم‌سازی فرآیندی است که به صورت ریاضی حجم یک جریان از داده را به یک طول ثابت کاهش می‌دهد. فرآیند درهم سازی یک فرآیند یک طرفه است.



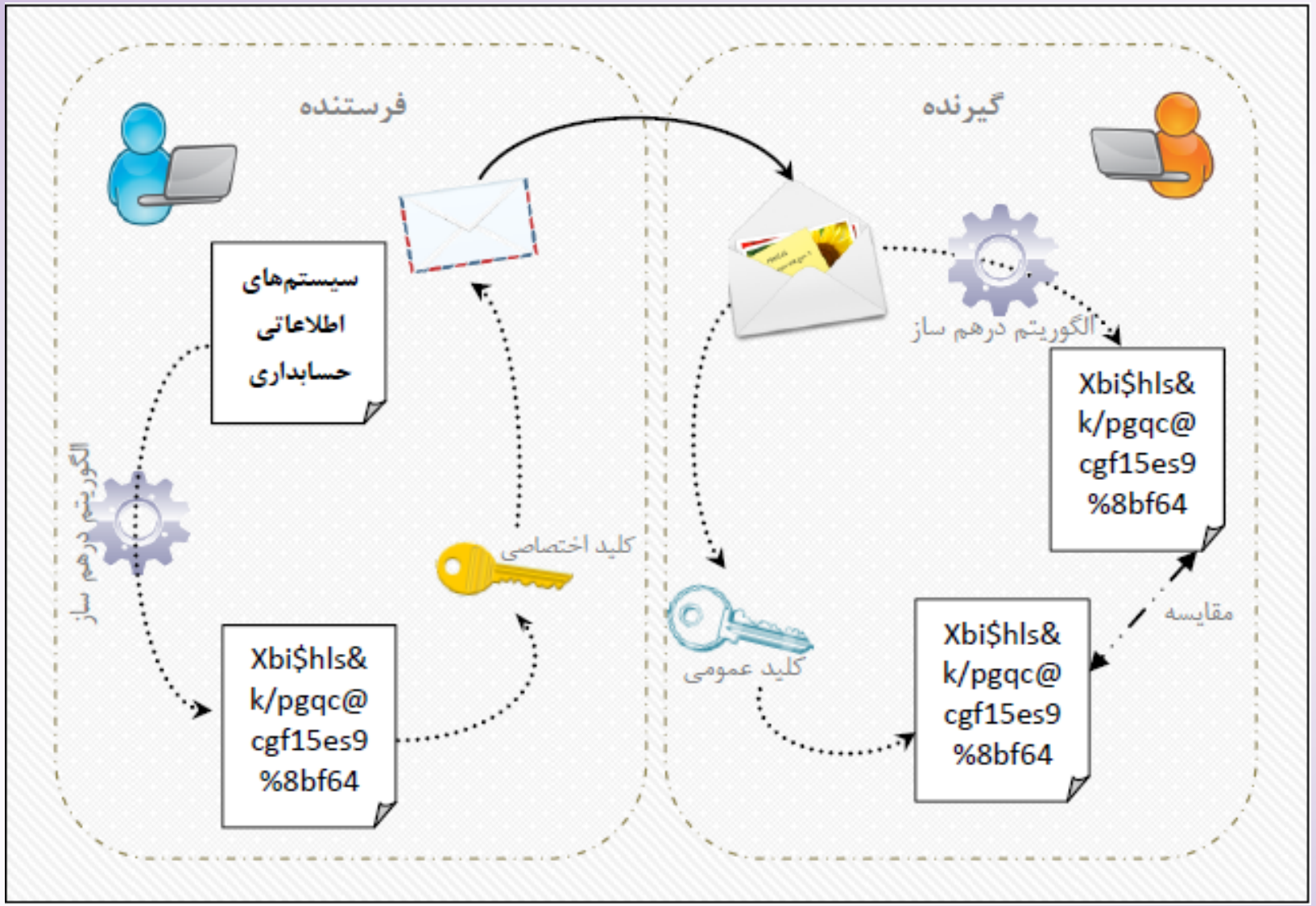
کاربرد توابع درهم ساز

- ✓ تشخیص درستی یک فایل
- ✓ هش کردن کلمات عبور
- ✓ نشانه گذاری اسناد یا امضای دیجیتال

عملکرد توابع درهم ساز مشابه اثر انگشت یک شخص می باشد.

امضا دیجیتال

- امضا الکترونیکی روشی برای حفاظت از سندیت و جامعیت اسناد الکترونیکی است.
- در تولید امضا الکترونیکی از شیوه‌های رمزنگاری مبتنی بر کلید عمومی و توابع درهم ساز استفاده می‌شود.



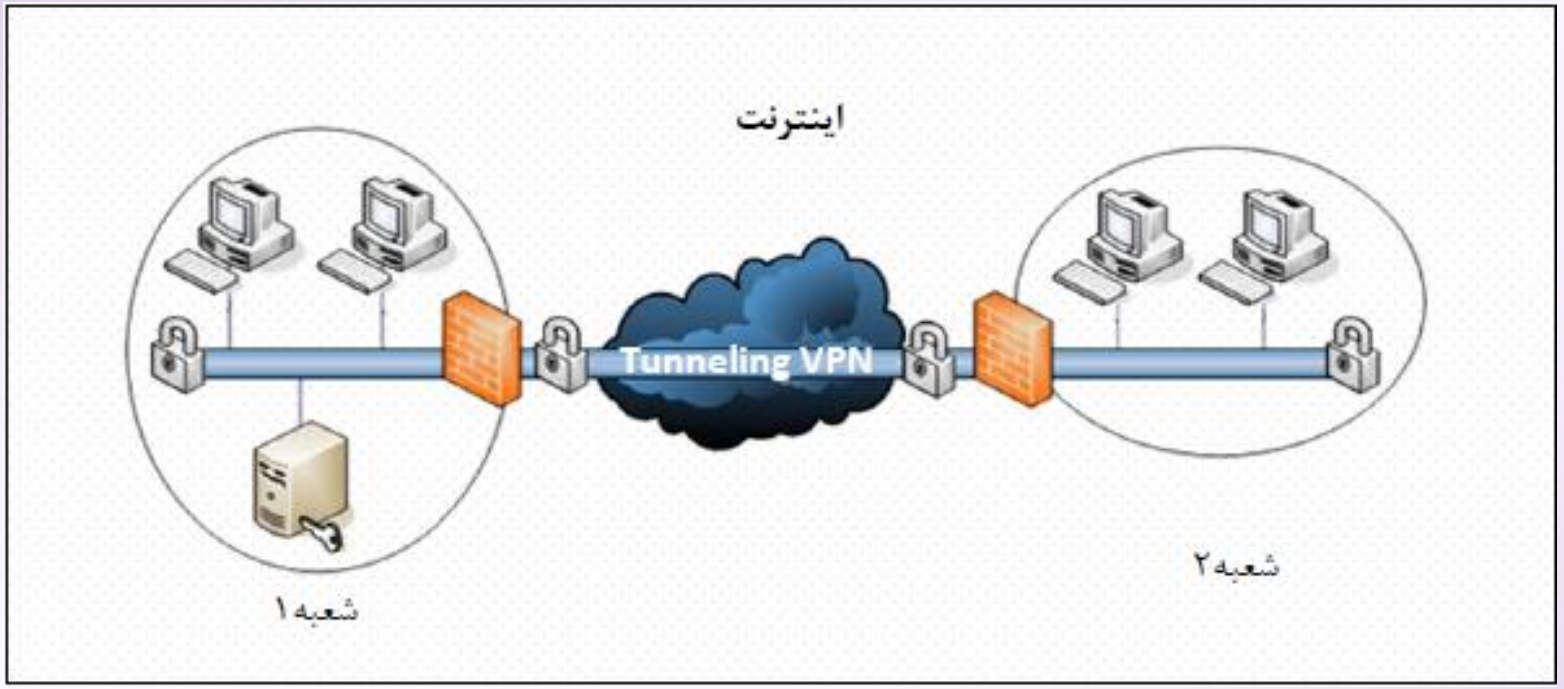
امضای دیجیتال

زیرساخت کلید عمومی و گواهینامه های دیجیتال

- زیر ساخت کلید عمومی چارچوبی است که تولید، توزیع، کنترل، لغو و ردیابی گواهی‌ها و کلیدهای مربوطه را بر عهده دارد.
- به عبارت دیگر، سامانه صدور کلیدهای عمومی و اختصاصی و گواهی‌نامه‌های دیجیتالی، زیرساخت کلید عمومی نامیده می‌شود.

شبکه های خصوصی مجازی

- شبکه خصوصی مجازی در واقع پیاده‌سازی شبکه خصوصی یک شرکت یا سازمان بر روی شبکه عمومی اینترنت است.
- شبکه‌های خصوصی مجازی به منظور تامین امنیت داده‌ها و ارتباطات از روش‌های متعددی مانند رمزنگاری و تونل‌سازی استفاده می‌کنند.



شبکه خصوصی مجازی

کنترل های انتقال داده ها

- روش های بازبینی مسیردهی
- کنترل های توازن
- تکنیک های تایید پیام


اللهم صل علی محمد و آل محمد