رمزنگاری، امضای دیجیتال و نمونه‌ی عملی آن

مهرداد مومنی

گروه کاربران لینوکس مشهد

تعریف و تاریخچه

- رمزنگاری، پنهان‌نگاری، کدگذاری
- جابجا کردن حروف الفبا در تمام متن
- پیچیدن یک نوار کاغذی بر روی استوانه‌ای با قطر مشخص
- در قرن بیستم میلادی از همین روش به همراه موتورهای الکتریکی برای رمزنگاری با سرعت بالا استفاده شد که نمونه‌های آن در ماشین رمز لورنتز و ماشین رمز انیگما دیده می‌شود.

سرویسهای رمزنگاری

- محرمانگی یا امنیت محتوا
- سلامت محتوا
- احراز هویت یا اصالت محتوا
- عدم انکار

برای ارائه کردن هر یک از سرویس‌های رمزنگاری، بسته به نوع کاربرد، از پروتکل‌های مختلف رمزنگاری استفاده می‌شود

الگوریتم رمزنگاری

- تمام امنیت حاصل شده از الگوریتم‌ها و پروتکل‌های رمزنگاری استاندارد، متکی به امنیت و پنهان ماندن کلید رمز است و جزئیات کامل این الگوریتم‌ها و پروتکل‌ها برای عموم منتشر می‌گردد.

انواع الگوریتم رمزنگاری

توابع بدون کلید

توابع مبتنی بر کلید

* الگوریتم‌های کلید متقارن
* الگوریتم‌های کلید نامتقارن
* الگوریتم‌های امضای رقومی

الگوریتم‌های رمزنگاری متقارن خیلی سریع‌تر از الگوریتم‌های رمزنگاری نامتقارن می‌باشند.

امضای دیجیتال

- یک امضای دیجیتال صرفا" به شما نخواهد گفت که «این شخص یک پیام را نوشته است» بلکه در بردارنده این مفهوم مهم است که : «این شخص این پیام را نوشته است»
- برای هر امضای دیجیتال ، یک کلید عمومی و یک کلید خصوصی وجود دارد

Command Line Interface

- gpg –gen-key generate a new key pair
- --import import/merge keys
- --verify verify a signature
- -e, --encrypt encrypt data
- -d, --decrypt decrypt data
- -s, --sign [file] make a signature

GUI Tools

- KGPG
- GnomeGPG