آشنایی با GNUPG

مهدی عطائیان
http://www.ataeyan.com

Cryptology

- Cryptography
  - علم استفاده از ریاضیات برای رمزکردن و از رمز خارج کردن دیتا است.
  - روشی برای ارسال امن اطلاعات در یک بستر ناامن است.
- Cryptanalysis علم آنالیز و شکستن ارتباطات امن است.
- Cryptology علم استفاده از دو علم بالاست.

Cryptology چرا

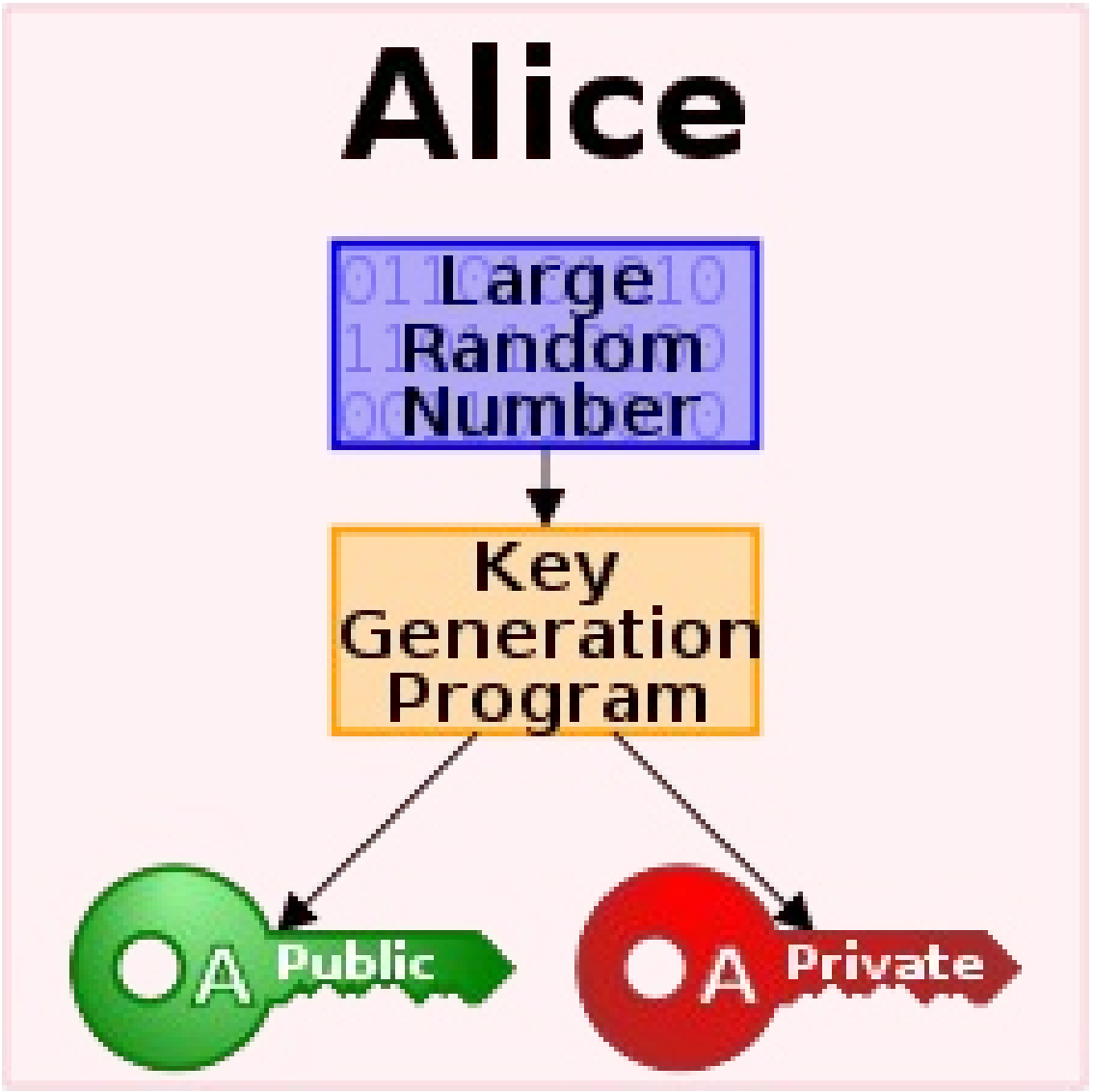
- Privacy
ارتباطات مخفی
- Integrity
ارتباطات امن
- Authentication
با چه کسی ارتباط داریم؟
- Nonrepudiation
دیتای فرستاده شده قابل انکار نیست

انواع رمزنگاری

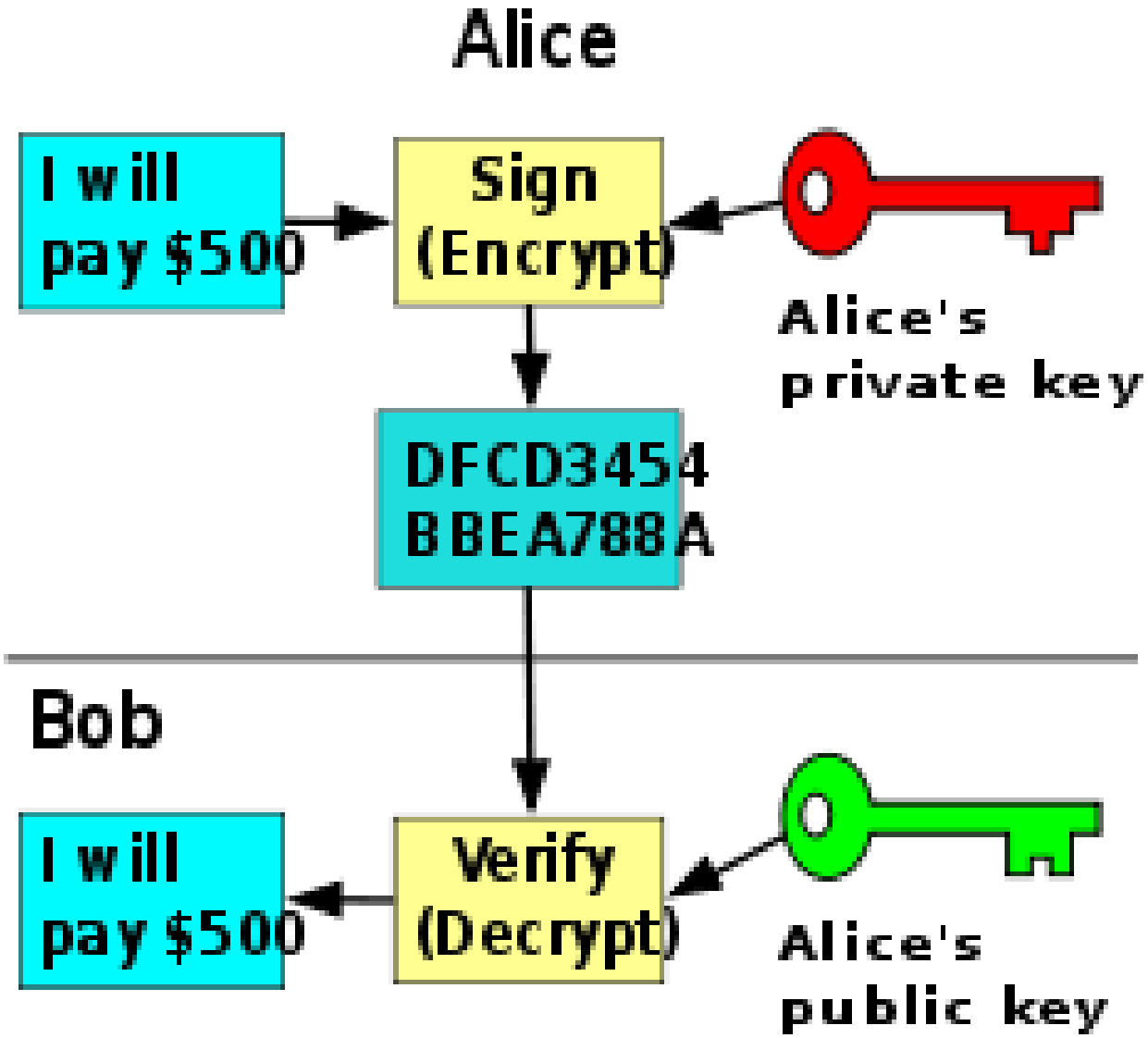
- متقارن

  با کلید ۱۲۸ بیت برای شکستن باید ۲^۱۲۸ حالت ممکن تست شود.
  عمر جهان ۲^۳۴ سال است.
  خورشید در ۲^۳۰ سال آینده به سوپرنوا تبدیل می‌شود.
- نامتقارن یا کلید عمومی

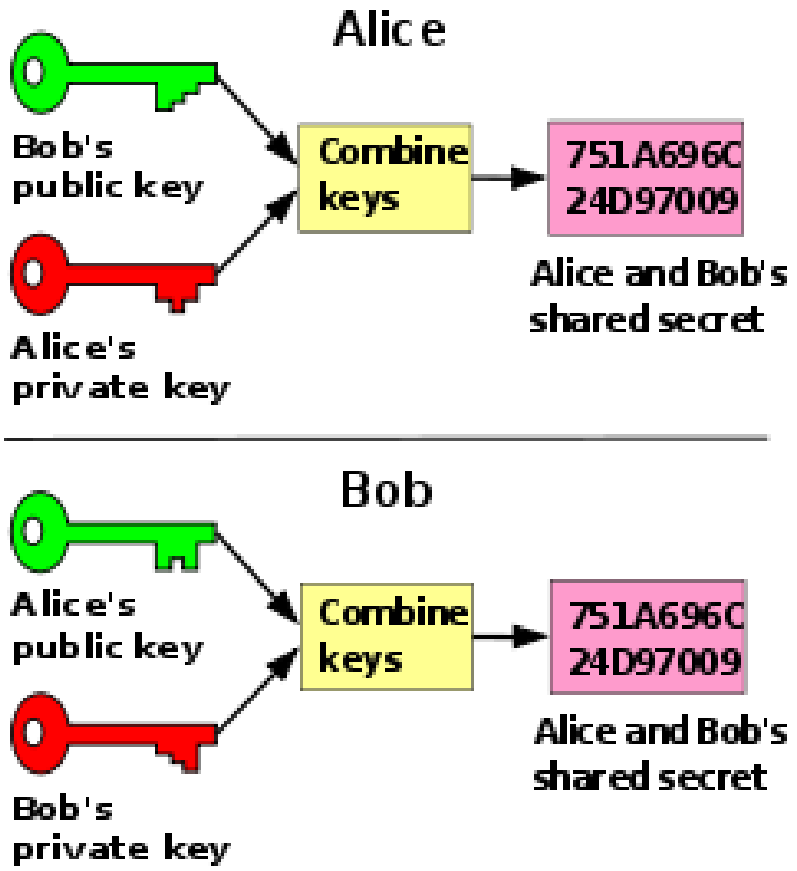
الگوریتم رمزنگاری نامتقارن



الگوریتم رمزنگاری نامتقارن



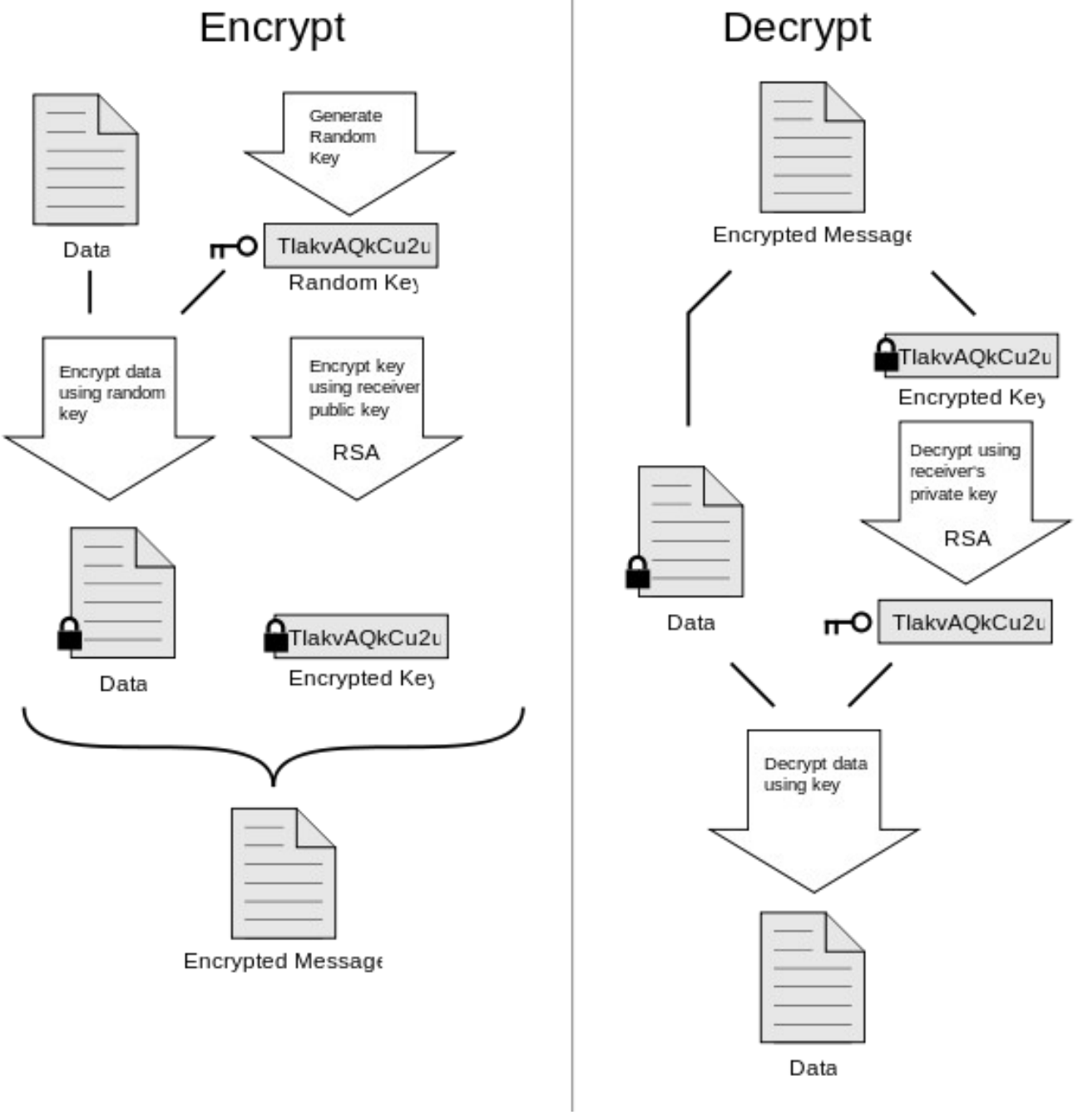
الگوریتم رمزنگاری نامتقارن



PGP

- Pretty Good Privacy (پوشیدگی خیلی خوب- مخفی کردن خوب)
- یک برنامه کامپیوتری برای به رمز کردن یا از رمز خارج کردن اطلاعات

PGP


Encrypt
Data
Generate Random Key
TlakvAQkCu2u
Random Key
Encrypt data using random key
Encrypt key using receiver public key
RSA
Data
TlakvAQkCu2u
Encrypted Key
Encrypted Message
Decrypt
Encrypted Message
TlakvAQkCu2u
Encrypted Key
Decrypt using receiver's private key
RSA
Data
TlakvAQkCu2u
Decrypt data using key
Data

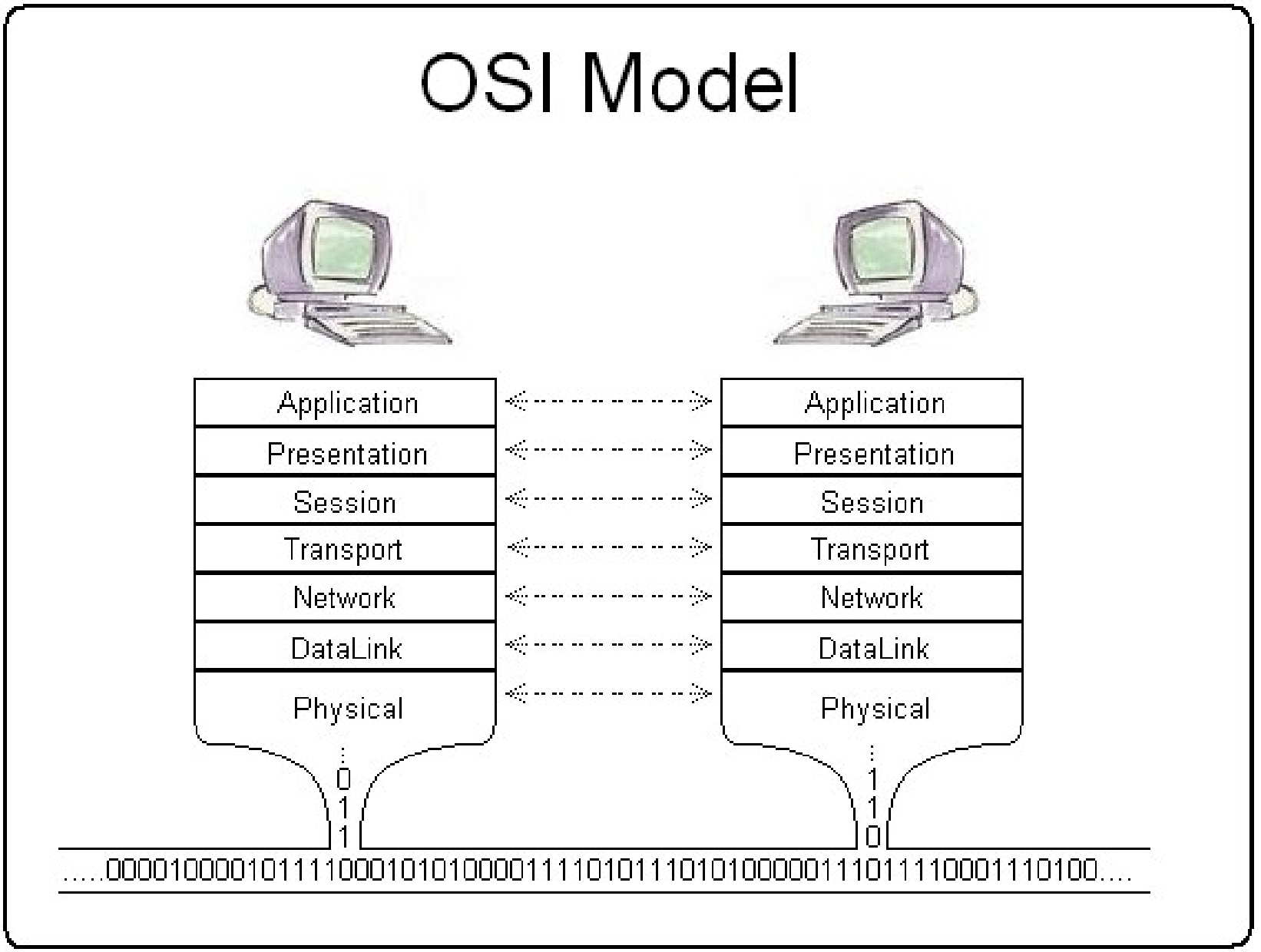
SSL - TLS

- لایهٔ سوکت‌های امن (Secure Sockets Layer) یا اس‌اس‌ال (SSL) پروتکلی است که توسط شرکت Netscape برای ردّ و بدل کردن سندهای خصوصی از طریق اینترنت توسعه یافته است. SSL از یک کلید خصوصی برای به رمز درآوردن اطلاعاتی که بر روی یک ارتباط SSL منتقل می‌شوند استفاده می نماید. طبق آن‌چه در استاندارد آمده است. URLهایی که نیاز به یک ارتباط از نوع SSL دارند با https: به جای http: شروع می‌شوند. SSL یک پروتکل مستقل از لایه برنامه است (Application Independent).بنابراین، پروتکل‌هایی مانند HTTP، FTP و Telnet قابلیت استفاده از آن را دارند. با این وجود SSL برای پروتکل‌های HTTP، FTP و IPSec بهینه شده‌است.

SSL - TLS

- پروتکل امنیتی لایهٔ انتقال (Transport Layer Security)، بر پایه لایهٔ سوکت‌های امن(Secure Sockets Layer) که یکی از پروتکل‌های رمزنگاری است بنا شده‌است. این پروتکل امنیت انتقال داده‌ها را در اینترنت برای مقاصدی چون کار کردن با پایگاه‌های وب، پست الکترونیکی، نمابرهای اینترنتی و پیام‌های فوری اینترنتی به کار می‌رود. اگرچه TLS و SSL با هم تفاوت‌های اندکی دارند ولی قسمت عمده‌ای از این پروتکل کم و بیش یکسان مانده است.

SSL - TLS


OSI Model
Application
Presentation
Session
Transport
Network
DataLink
Physical
Application
Presentation
Session
Transport
Network
DataLink
Physical
0
1
1
1
1
0
.....00001000010111100010101000011110101110101000001110111100011101000....

Gpg

- یک معادل با مجوز گنو برای برنامه PGP است.
- کمک مالی از دولت آلمان
- سازگار با استاندارد OpenPGP

پارامترها

- Gpg --gen-key
- Gpg --list-keys
- Gpg --delete-secret-key A30e9680c
- Gpg --delete-key A30e9680c
- Gpg -c file
- Pgp file.gpg
- Gpg -e -r 'mahdi' file
- Gpg -r -r 'mahdi.ataeyan <at> gmail<dot>com' file

منابع

- ویکی‌پدیا فارسی اس‌اس‌ال
- http://en.wikipedia.org/wiki/Osi_layer
- http://en.wikipedia.org/wiki/Cryptography
- http://en.wikipedia.org/wiki/GNU_Privacy_Guard
- گنوپرایوسی گارد در ویکی‌پدیا فارسی
- مستندات GPG