عنوان سند: PGP (Pretty Good Privacy)

ارائه دهنده: شـهرزاد اميني

تاريخ ارائه: ۸۳/۱۰/۲۱

گروه کاری : امنيت

گروه مطالعاتی : امنيت

اصلاح کننده : شـهرزاد اميني

تاريخ اصلاح: ۸۳/۱۱/۲

منابع: مقالات اينترنت و www.pgp.com

بنام خدا

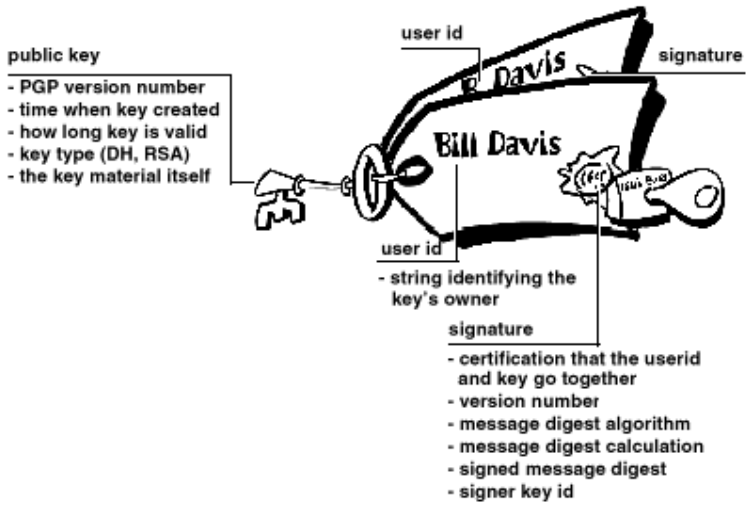
PGP
PRETTY GOOD PRIVACY

تاريخچه PGP:

مولف و سازنده اوليه **PGP** ، **Philip (R) Zimmerman** است .آقاي زايمرمن نوشتن برنامه PGP را در سال ۱۹۹۱ آغاز كرد و تقريباً به پايان رساند .
PGP ، سرويس محرمانگي واحراز هويت براي پست الكترونيكي و برنامه هاي ذخيره فايل است .
نسخه تجاري اين محصول را مي توان از شركت Viacrypt تهيه كرد. مدت سه سال آقاي زايمرمن براي صدور نرم افزار با دولت آمريكا درگير بود. درپايان سال ۱۹۹۹ بخش Network Associatesشركت Viacrypt اعلام كرد كه مجوز صدور محصول را دريافت كرده است .

PGP
Pretty Good Privacy

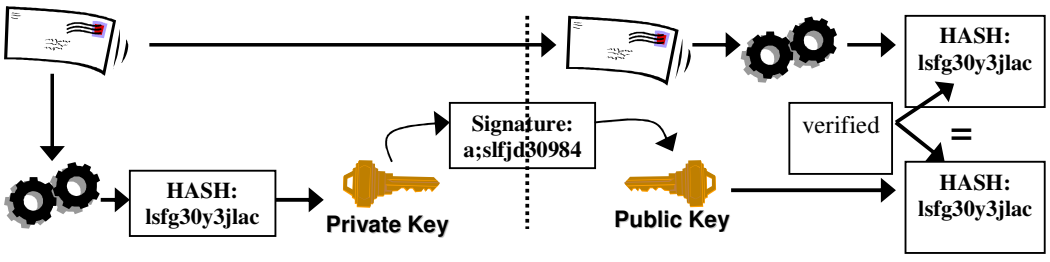
PGPيك برنامه كامپيوتري براي خصوصي سازي شخصي است .بدين شكل افراد ديگر نمي توانند به اطلاعات و Email هاي شخص مذكور دسترسي يابند .
بدين منظور از روشهاي Cryptographic استفاده مي شود (مز نگاري و امضاي ديجيتال) براي ساده سازي درك ساختار پسورد از (Public P K I key infrastructure) استفاده مي شود.
PGP مي تواند يك جفت كليد عمومي و خصوصي را توليد كند .كليد عمومي PGP توسط يك شبكه غير رسمي بانام The Web of trust تاييد مي شود .



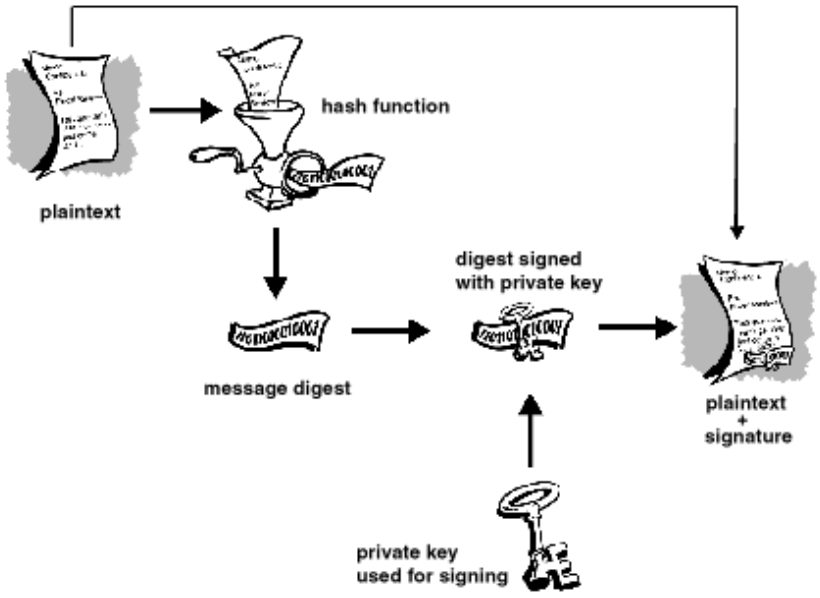
شكل ١ : روش رمز نگاري در PGP را نشان مي دهد.

درصورت استفاده صحيح از PGP امنيت بالايي را مي توان فراهم كرد. PGP از الگوريتم هاي Diffie –Hellmanو. DSS .و RSA براي رمز نگاري نامتقارن استفاده مي كند .
PGP از الگوريتم هاي CAST.125 ,IDEA ,3DESبراي رمز نگاري متقارن استفاده مي كند.

روش درهم ريختگي (hash algoritm) آن SHA-1مي باشد .



شكل ٢: شمايي از الگوريتم Hash Function را نشان مي دهد.



شكل ٣: شمايي از الگوريتم PGP را نشان مي دهد.

كاربرد PGP بقرار زير است :

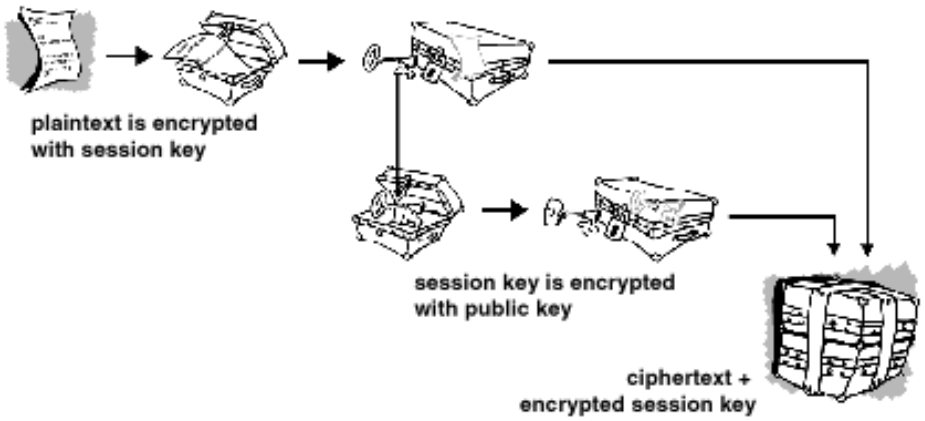
- ❖ رمز گذاري و علامت گذاري اطلاعات
- ❖ رمز گشايي ، شناسايي فايلها و امضاها
- ❖ مديريت و جمع آوري كليد هاي PGP شامل (TESTكردن Property ها،Import يا Export ،معتبر سازي و غيره)

پس از اينكه PGP را نصب كرديم يك جفت كليد براي خودمان استخراج مي كنيم. كليد عمومي Public Key را براي دوستان Export مي كنيم . حالا وقت رمز كردن فايلها است . شما نام اشخاصي از دوستان را كه اجازه دارند پيغامها را بخوانند انتخاب مي كنيد .حال PGP يك فايل رمز شده ايجاد مي كندكه فقط اعضاي ليست فوق قادر به رمز گشايي آن هستند.

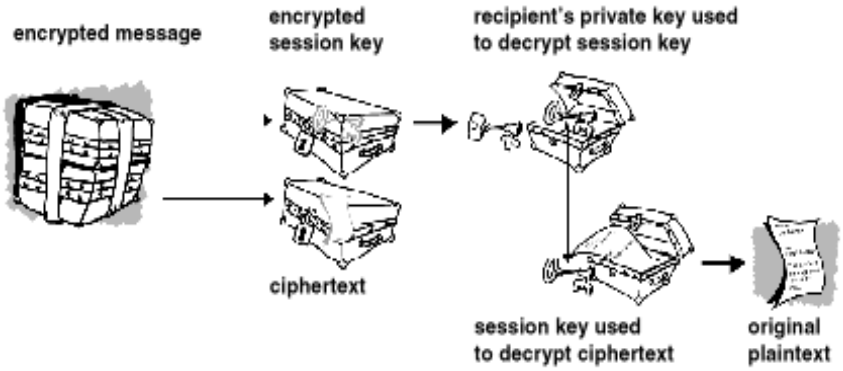
شما مي توانيد فايلها را امضا ءنيزكنيد .باانتخاب يك كليد خصوصي Private Key و دادن فاز قبول كليد PGP يك فايل با اطلاعات امضاء شده با امضاء عمومي يا امضاء مخصوصي ايجاد مي شود .

مي شود ايندو مرحله را با هم ادغام كرد و رمز نگاري و امضاء فايل را توامان انجام داد . در اينصورت تنها وقتي فايل رمز گشايي شود امضاء قابل تشخيص مي شود . اگر شما يك فايل امضاء شده دريافت كرديد يا Double Cilic كردن روي آن PGP تشخيص مي دهد كه امضاء درست است يا نه و اگر فايل رمز شده دريافت كنيد مي توانيد بازش كند و PGP از شما كليد خصوصي Private Key مي خواهد تا آن را رمز گشايي كند .

مورد دیگر اینکه کلید ها را امضاء کنید تا ببینید آیا آنها معتبر هستند و مقادیر کلیدهاي عمومي Public Key بگونه اي SET (تنظیم)کنید تا قابل اطمینان باشند .



شكل ٤: شمايي از رمز نگاري با كليد عمومي و كليد خصوصي را نشان مي دهد.



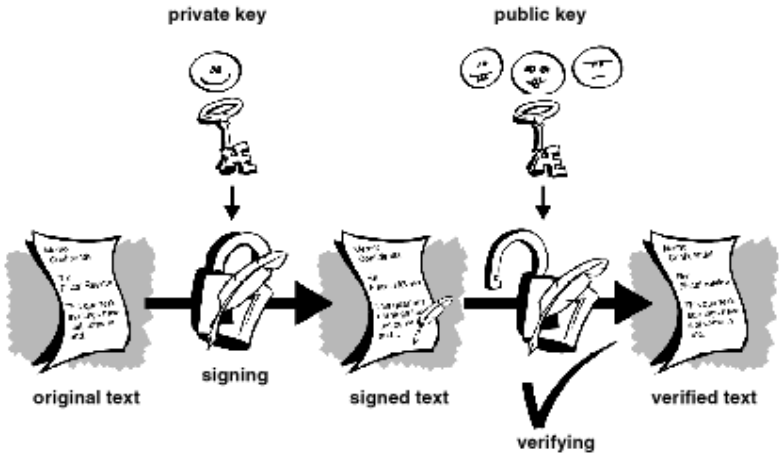
شكل ٥: شمايي از رمز گشايي با كليد عمومي و كليد خصوصي را نشان مي دهد.

مزایای PGP

- مجاني بودن و قابليت اجرا بر روي سيستم هايDOS، WINDOWS، Unix، Macintosh،.....
- نسخه تجاري آن ضمانت و خدمات پس از فروش دارد .
- استفاده از الگوريتم هاي قوي و مورد تاييد
- روش معين و استاندارد براي رمز كردن اطلاعات چه Email و چه فايل
- ايجاد يك ارتباط امن در اينترنت براي كاربران
- عدم تكيه به كشور خاص

امضای رقمی :

- ❖ براي احراز هويت از آن استفاده مي شود .
- ❖ خلاصه 160 بيتي پيام توسط SHA-1 محاسبه و سپس توسط RSA يا PSS امضاء مي شود.
- ❖ فشرده سازي اطلاعات قبل از رمز نگاري و بعد از امضاء انجام مي شود .
- ❖ با توجه به محدوديت در بعضي از سرويسها ي پست الكترونيكي PGP پيام رمز شده را از حالت باينري به متن ASCII تبديل مي كند (توسط الگوريتم radix64) ولي متاسفانه حجم پيام 33%بزرگتر مي شود .



شكل ٦ : شمايي از امضاي ديجيتال را نشان مي دهد.

سرویس های PGP:

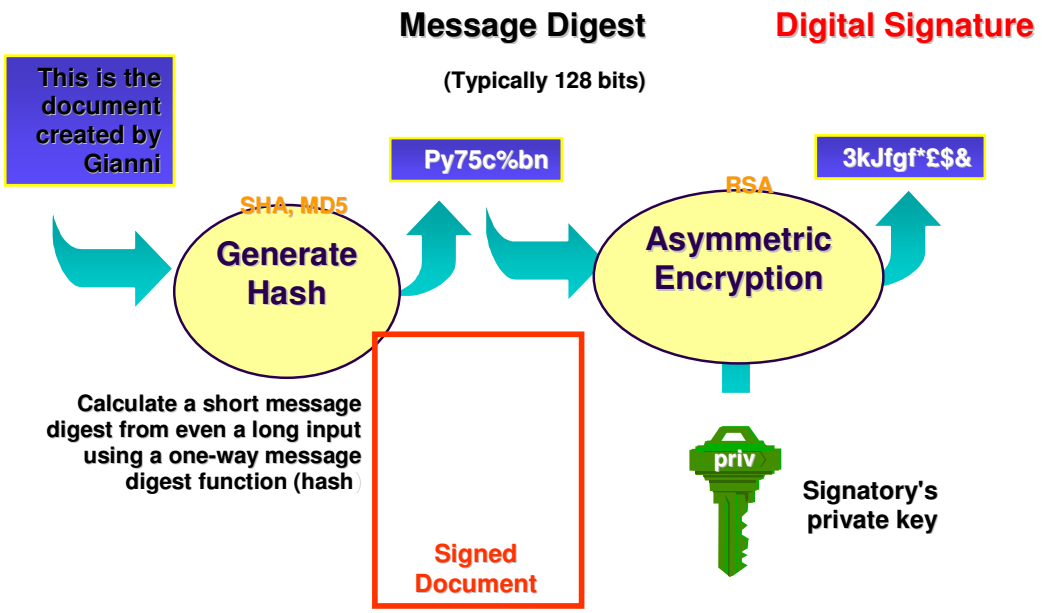
١. امضاي رقمي Digital Signature
٢. احراز هويت Authentication
٣. محرمانگي Confidentiality
٤. فشرده سازي Compression
٥. سازگاري با پست الكترونيكي Email Compatibility
٦. تقسيم و تركيب Segmentation

حال به توضيح سرويس هاي فوق مي پردازيم :

امضای دیجیتال :

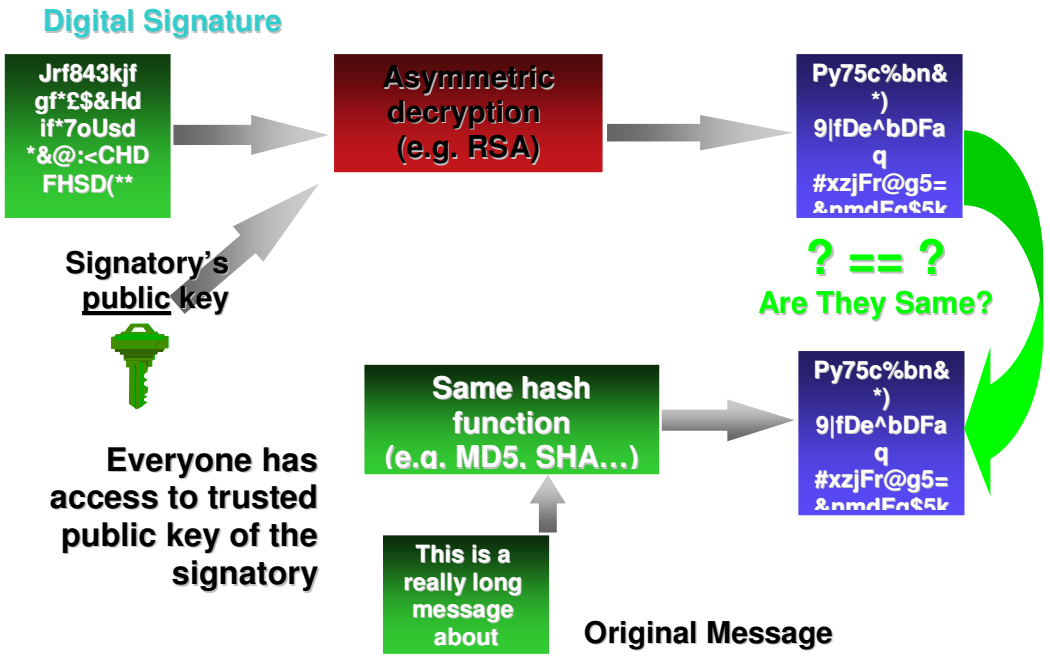
از امضاي رقمي براي احراز هويت استفاده مي شود . بدينصورت كه ابتدا چكيده 160 بيتي پيام توسط SHA-1 محاسبه و سپس توسط RSA يا DSS امضاء مي شود . PGP اجازه مي دهد امضاء همراه

پيغام يا مستقل از آن ارسال شود .ارسال امضاء مستقل از پيغام زماني لازم مي شود كه يك امضاء براي چند پيغام نياز است يا لازم است چند نفر يك پيغام را امضاء كنند .

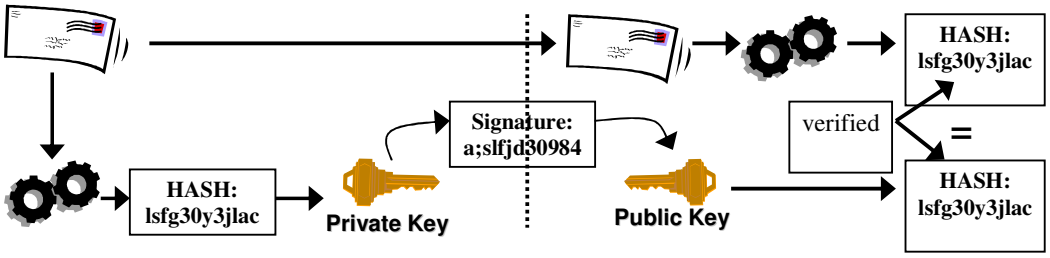


شكل٧ : امضاي ديجيتال را نشان مي دهد.

پيغام همراه با يك نسخه از hash امضا شده پيغام ويك كپي از digital certificate فرستنده ارسال مي گردد.
پروسه hash function توسط نرم افزار PGP روي certificate data انجام داده و آنگاه PGP، نتيجه آن را باmessage مقايسه كرده و اگر يكسان بودند نشان مي دهد كه پيغام معتبر مي باشد.



شكل٨ : مقايسه امضاي ديجيتال با مقدار Hash پيغام اوليه



شكل ٩ : اثبات درستي پيغام ارسال شده را نشان مي دهد .

محرمانگی :

محرمانگي با استفاده از رمز نگاري متقارن انجام مي شود . كليدمتقارن بصورت تصادفي ساخته مي شود و توسط الگوريتم نامتقارن رمز و به همراه پيغام رمز شده به گيرنده ارسال مي شود .كليد تصادفي را كليد Session Key يا كليد يكبار مصرف نيز مي نامند كه نياز به همزمان كردن سيستم ها ندارد كه براي Email سودمند است.

فشرده سازی Compression :

فشرده سازي قبل از رمز و بعد از امضاء انجام مي شود فشرده سازي قبل از رمز نگاري ساختار آماري پيغام را از بين مي برد و قدرت رمز نگاري را افزايش مي دهد .
فشرده سازي بعد از امضاء اين حسن را دارد كه مي توان پيام و امضاء را براي تاييد بعدي و بدون نياز به فشرده سازي ذخيره كرد .

سازگاری با پست الکترونیکی

PGPتوسط الگوريتم radix64 پيام رمز شده را از حالت briary به ASCLL تبديل ميكند كه پيام را 33% بزرگ مي كند .تبديل به ASCLL امضاي نامه (نه متن)در صورتيكه گيرنده PGPباشد مشكلي پيش نمي آيد .

تقسیم و ترکیب Segmentation

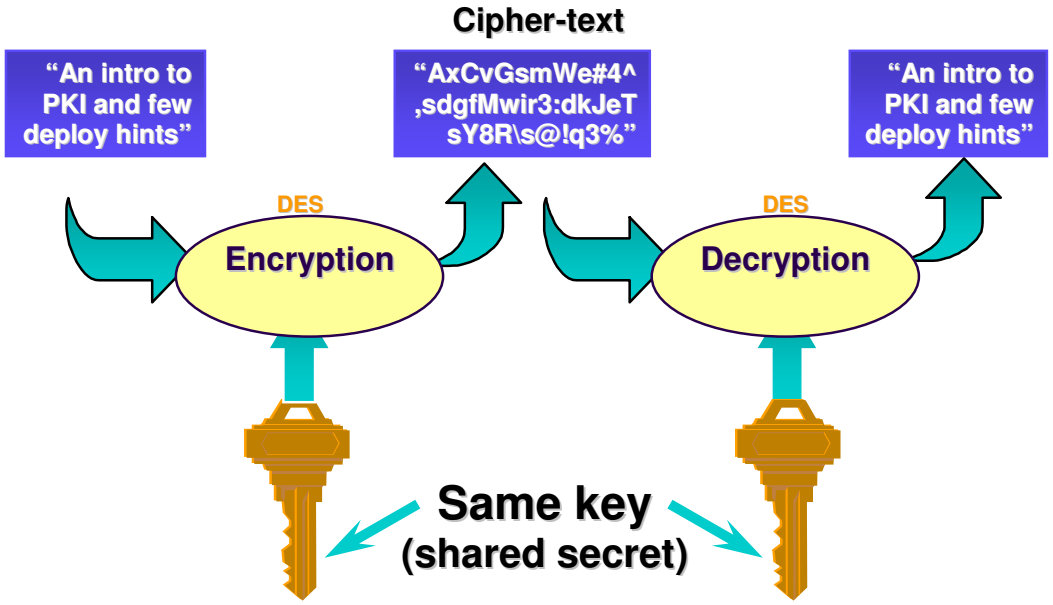
جهت سازگاري با پست الكترونيكي تقسيم به قطعات كوچكتر كردن پيام وارسال مجزاي هر كدام از قطعات اما در طرف مقابل پيام ها دوباره تركيب شده تا پيام اوليه تشكيل گردد.كه عمل تقسيم با استفاده از radix64 انجام مي شود .

کلیدهای رمز نگاری در PGP:

كليد متقارن مناسب كرده وكليد هاي عمومي و خصوصي ذخيره ميكند. ميتواند چندين كليد نامتقارن (تركيب Public Key و Private Key) براي ارتباط با گروههاي مختلف داشته باشد (براي زماني است كه كليد عوض شود و پيامي با كليد قديمي رمز شده باشد .)

رمزنگاری با استفاده از کلید عمومی

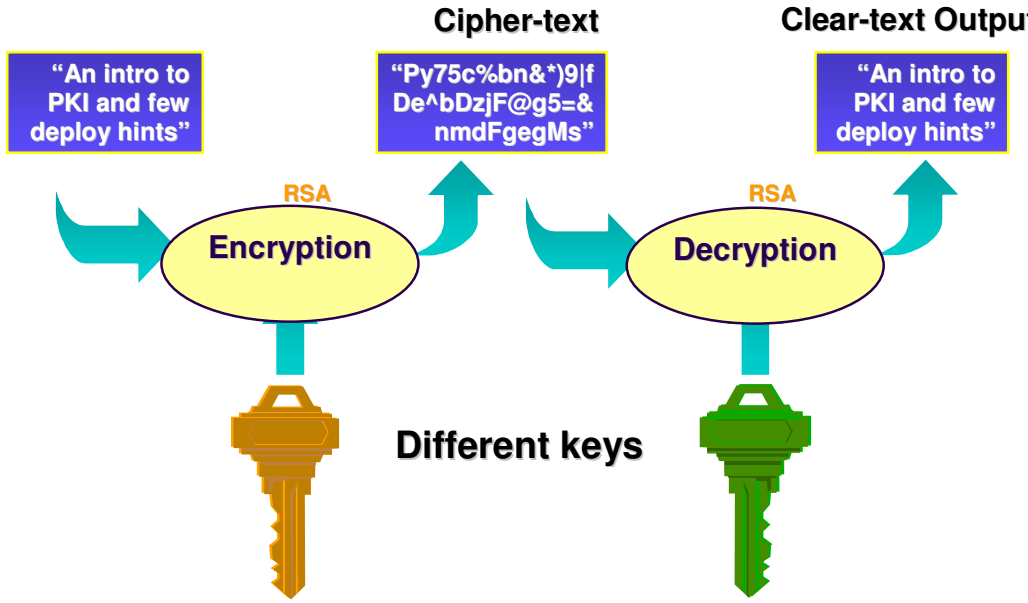
در اين نوع هم براي رمزگذاري و هم رمزگشايي از يك كليد استفاده مي شود.با حفظ تبديلات رمزگذاري و رمزگشايي مي توان امنيت و اعتبار اطلاعات را فراهم كرد.



شكل ١٠ : رمزنگاري با استفاده از كليد عمومي را نشان مي دهد.

رمزنگاری با استفاده از کلید خصوصی

در اين نوع سيستمهاي كليدهاي رمزگذاري و رمزگشايي مختلف مي باشند و بدست آوردن يك كليد از ديگري غير ممكن مي باشد. تبديل رمزگشايي حفاظت و امنيت،و تبديل رمزگذاري اعتبار و صحت را فراهم مي كند.



شكل ١١ : رمزنگاري با استفاده از كليد خصوصي را نشان مي دهد.

نحوه توليد كليد Session

كليد بصورت تصادفي و يكبار مصرف توليد مي شود و الگوريتم توليد كننده عدد تصادفي CAST-128است . اين الگوريتم توسط تايپ مقدار اوليه بر مي گردد.كليد متقارن Symmetric توسط كليد عمومي گيرنده رمز و براي گيرنده ارسال مي شود.و اين كليد عمومي براي افراد مختلف بايد نگهداري شود .فرستنده بايد توسط Key IDكليد استفاده شده را معين كند .

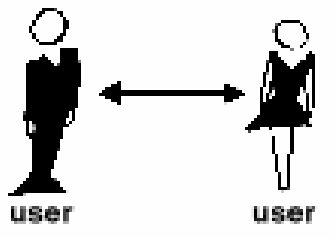
در PGPبراي هر Public Key مقدار (Kua mode 264)بعنوان Key IDدر نظر گرفته مي شود . Time Stamp آن از حمله جلوگيري مي كند .

يك Time Stamp مربوط به فايل حاوي پيام و يكي مربوط به امضاي پيام است . با حذف time stamp و نام فايل مي توان امضاي مستقل براي يك پيام ايجاد كرد . دو بايت ا زچكيده قبل از امضاء در قسمت signature درج مي شود تا خطاهاي احتمالي مانند Public Key غلط يا noise بررسي شود .

مديريت Public Key در PGP:

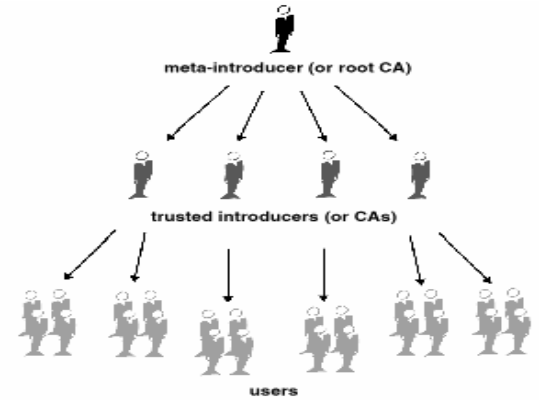
ارسال كليد Public Key با تشخيص هويت صورت مي گيرد كه انتقال بطور فيزيكي در شبكه غير ممكن است .گاهي از طريق الكترونيكي يا تاييد توسط تلفن انتقال مي يابد.

روش ديگر اين است كه انتقال توسط يك فرد(مورد اطمينان) trusted كه كليد Public key را دارد انجام شود. بدين شكل كه مثلاً كليد Public key كاربر A توسط يك كاربر شناخته شده و مورد اطمينان بنام B امضاء و به كاربر C ارسال گردد.

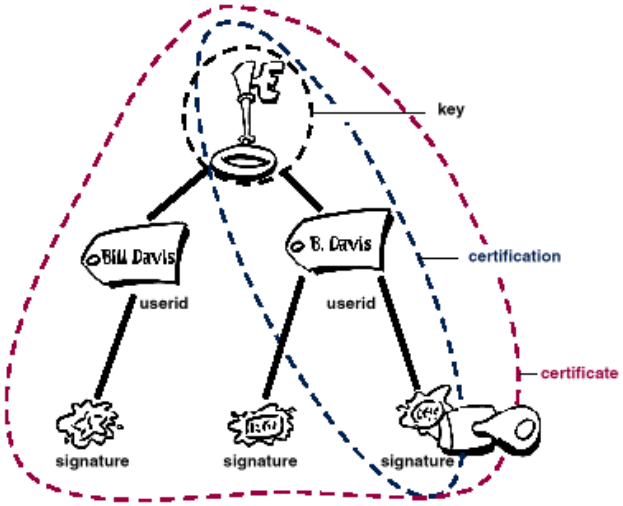


شكل١٢ : انتقال توسط يك فرد(مورد اطمينان) trusted صورت مي گيرد.

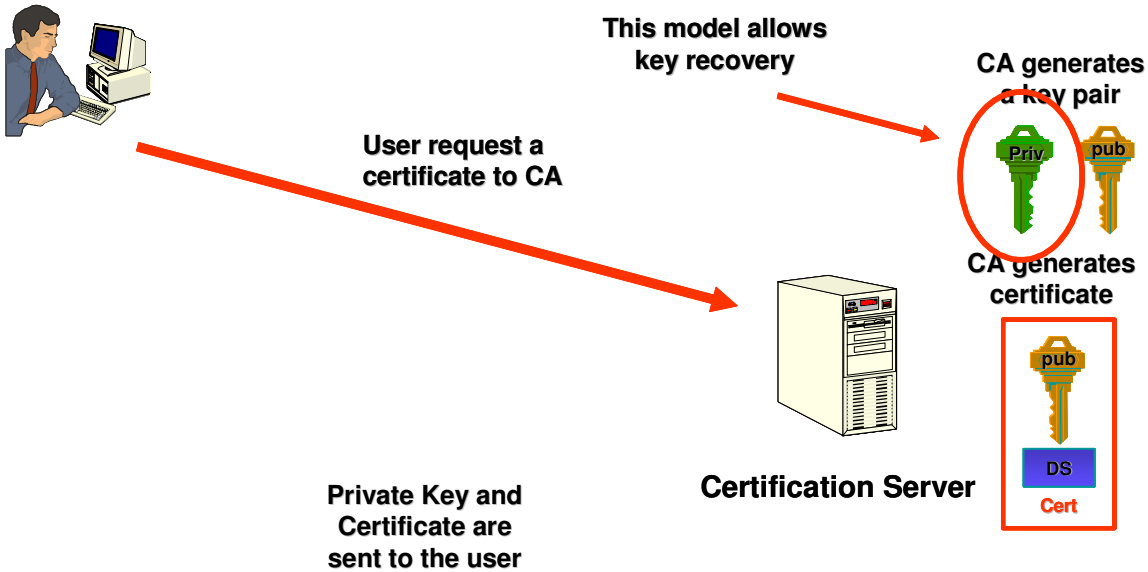
يا اينكه انتقال توسط CA(Certificate Authority) انجام شود.



شكل ١٣ : انتقال توسط CA(Certificate Authority) را نشان مي دهد.



شكل١٤ : شمايي از روش كار گواهي Certificate Authority را نشان مي دهد.



شكل ١٥: شمايي از روش كار گواهي Certificate Authority را نشان مي دهد.

تعيين اعتبار Public key:

فيلد Owner Trust:

تعيين اعتبار كليد عمومي Public key براي امضاي كليدهاي عمومي ديگر كه اين توسط user تعيين شده و اعتماد userبه صاحب Public key را نشان مي دهد. به ازاي هر Public keyيك يا چند signature بعنوان تأييد كننده اين key وجود دارد.

فيلد Signature Trust**:**

براي امضاهاي انجام شده براي Public key است.

فيلد key Legitimacy**:**

اعتماد PGP به اعتبارPublic key را بيان مي كند و از فيلد قبلي بدست مي آيد.
متناظر با هر Public keyيك Private key از جدول وجود دارد.
كليد خصوصي Private key متناظر ندارد.
كليد عمومي توسط كليدهاي ديگر signature مي شود.
ميزان قابل اطمينان بودن Public key از فيلد owner trust محاسبه مي شود.