**1-ва задача: файлът RSA.zip липсва, за да мога да анализирам кода.**

**2-ра задача:**

**За Gpg4win**

Gpg4win (GNU Privacy Guard for Windows) е софтуер за криптиране на файлове и имейли.

**Какво е Gpg4win?**

Gpg4win позволява на потребителите безопасно транспортиране на имейли и файлове с помощта на криптиране и цифрови подписи. Шифроването защитава съдържанието срещу нежелани лица, което искат да го прочетат. Цифровите подписи ни уверяват, че съдържанието не е променено и идва от конкретен подател.

Gpg4win поддържа както съответните криптографски стандарти, OpenPGP, така и S / MIME (X.509) и е официалният дистрибутор на GnuPG за Windows. Поддържа се от разработчиците на GnuPG. Gpg4win и софтуерът, включен в Gpg4win, са безплатни.

**Цел на инициативата Gpg4win**

Инициативата на Gpg4win има за цел да предостави актуален инсталационен пакет за Gpg4win за Windows, включително инструмента за шифроване на GnuPG и свързаните с него приложения.

И OpenPGP, и S / MIME трябва да се поддържат по унифициран начин.

Основно постижение на Gpg4win е, да позволява лесно създаване на актуализирани инсталатори. Най-добре работи в GNU / Linux система. Почти всички софтуерни компоненти се компилират автоматично за интегриране в инсталатора. По този начин Gpg4win не зависи от само от един човек, който да създава инсталатора.

**3-та задача:**

**Мрежова сигурност**: Това е най-очевидното - ако китайските хакери получат идентификационни данни във вътрешните ви системи, те ще потърсят вашия източник (ако няма друга причина освен факта, че изходният код ще им каже къде да продължат напред). Така че основната компютърна сигурност трябва да бъде „дадена“.

**Контрол на достъпа:** Има ли нужда вашия съсед, например, до хранилището на вашия код? Вероятно не. Ограничете достъпа си.

Бъдете избирателни при наемането и поддържането на здравословна работна среда: DLP(**Data Loss Prevention**) мерките като сканиране на изходяща електронна поща са теоретични, но може би вашият инженер е достатъчно умен, за да разбере как да заобиколят вашите DLP мерките. Вашите служители не трябва да имат причината да предоставят вашия код на трети лица. Ако го направят, вие сте направили нещо погрешно.

**Наблюдавайте мрежата си:** Това е разширение на отговора „сигурност на мрежата“, но с акцент върху цифровото предотвратяване на загуби. Ако забележите внезапен скок в DNS трафик, това може да е вашият изходен код, който се атакува от нападател. ОК, сега се запитайте дали дори бихте разбрали дали има внезапен скок в DNS трафика от вашата мрежа. Вероятно не.

**Отнасяйте се по различен начин към мобилните устройства:** Телефоните и лаптопите се губят много често. Никога не трябва да съхранявате чувствителна информация (включително изходния код, клиентски данни и търговски тайни) на мобилни устройства. Никога. Това не означава, че не можете да използвате мобилни устройства за достъп и редактиране на изходния код. Но ако лаптопът ви изчезне, трябва да можете да отмените дистанционно всеки достъп, който лаптопът има до чувствителни данни. Обикновено това означава, че кодът и документите се редактират „в облака“ с подходяща автентификация за всичко това.