دانشگاه صنعتی امیرکبیر
(پلی تکنیک تهران)

Department of
Computer Engineering

به نام خداوند جان و خرد

تمرین تحویلی چهارم

درس مبانی امنیت اطلاعات

امیرفاضل کوزه گر کالجی

9931099

سوال اول

Connection ارتباط میان یک کلاینت و سرور می‌باشد که با استفاده از پروتوکل هایی مانند TCP اجرایی می‌شود و معمولا کوتاه مدت است. سرور ها پس از مدتی ارتباط را قطع می‌کنند.

Session اما مفهومی از چیزی است که وضعیت و داده یک چیز خاص را در خود نگه می‌دارد حتی پس از قطع شدن ارتباط. در واقع هدف نیز این است که داده ها را بعد از قطع شدن ارتباط نگه داریم تا زمانی که ارتباط جدیدی متصل شود.

سوال دوم

هدف وجود این پروتکل، انتقال record بین سرور و کلاینت بوده که امنیت داده را تضمین میکند. پس دو اصل را برقرار کرده که Confidentiality و Integrity بوده، حتی در محیط های غیر امن و غیر رمزنگاری شده.

سوال سوم

Pgp به لطف سرویس هایی که دارد، یک سری از مشکلات را برایمان حل کرده است.

شرح مشکل:

- فرستادن داده های باینری از طریق سرویس های پست الکترونیکی که تنها برای ارسال متن ascii طراحی شده اند.

راه حل:

- تبدیل داده های خام باینری به متن ascii
- استفاده از الگوریتم radix-64
  - تبدیل 3 بایت به 4 کاراکتر قابل چاپ ascii
  - اضافه کردن CRC به انتهای آن
- توسعه متن به اندازه 33٪ به دلیل استفاده از Radix-64 و فشرده سازی به اندازه -50٪
- در نهایت فشرده سازی به اندازه 1/3 صوت می‌پذیرد.

سوال چهارم

در PGP، عملیات فشرده سازی بعد از امضای دیجیتال و قبل از رمزنگاری انجام می‌شود. فشرده سازی با کمک الگوریتم zip صورت می‌گیرد. این فرایند شامل Integrity و confidentiality می‌باشد.

سوال پنجم

سرویس های ارائه شده توسط pgp در ذیل آمده اند:

- Confidentiality
- Compression
- E-mail compatibility
- Authentication
- segmentation

سوال ششم

در این روش، فرستنده کلید جلسه pgp رمزنگاری شده خود را به گیرنده می‌فرستد و گیرنده با استفاده از کلیدخصوصی خود قادر به رمزگشایی آن است. و این موجب فراهم آمدن محیطی امن برای ارتباط میان طرفین خواهد شد.

سوال هفتم

محدودیت های SMTP : عدم توانایی یا مشکل در انتقال

- فایل های باینری یا اجرایی (مانند jpeg)
- کاراکتر های غیرلاتین
- پیام بزرگتر از یک اندازه خاص
- مشکلات تبدیل در ASCII و EBCDIC
- خطوط بزرگتر از حد خاص