دانشگاه صنعتی امیرکبیر (پلی تکنیک تهران)
دانشکده‌ی مهندسی کامپیوتر و فن‌آوری اطلاعات

روش تحقیق و گزارش نویسی

تکلیف نهم

سید محمد مهدی موسوی

(9231053)

استاد :

جناب آقای دکتر صفابخش

فروردین 95

موضوع پروژه

در این مقاله پروتکل HTTPS[1] بررسی شده و مزایا و معایب آن نسبت به پروتوکل HTTP[2] شرح داده می شود این پروتکل امنیت صد در صد را در تبادلات اطلاعاتی از طریق اینترنت برای ما مهیا می کند . کاربرد های استفاده از این پروتکل را می توان در سیستم های مالی، سیستم های اطلاعاتی، و یا هر سیستمی که بر مبنای تبادل اطلاعات کار می کند و نیاز به امنیت دارد، دید .

این پروتکل بسیار محبوب است زیرا پیام هائی که میان فرستنده و گیرنده اطلاعات جابجا می شود **کد گذاری**[1] می شود و این مهم از طریق استفاده ی پروتکل HTTP از SSL[3] یا TLS[4] است که باعث می شود جلوی حمله ی مردان میانی[5] را بگیرد .

برای کد گذاری اطلاعات از الگوریتم های نظریه ی اعداد استفاده می شود مانند یافتن اعداد اول بزرگ، بررسی اول بودن عدد، رمز نگاری کلید عمومی[6] ، و سیستم رمزنگاری RSA[7] .

موفقیت سیستم رمزنگاری RSA بر اساس این حقیقت است که می توانیم اعداد اول بزرگی را بیابیم، ولی روش موثری برای تجزیه اعداد بزرگ وجود ندارد . پیدا کردن عدد اول بزرگ الگوریتمی دارد که دارای پیچیدگی زمانی چند جمله ای است اما تاکنون هیچ کسی، الگوریتمی برای تجزیه ی عدد اول نداده است که دارای پیچیدگی زمانی چند جمله ی باشد

[1] Hypertext Transfer Protocol Secure
[2] Hypertext Transfer Protocol
[3] Secure Sockets Layer
[4] Transport Layer Security
[5] Man In The Middle Attacks
[6] Encryption Public key
[7] Crypto System

بررسی پیشینه ی موضوع

- **پروتکل HTTP :**

یکی از پروتکل های لایه کاربرد (Application) است و برای انتقال اطلاعات شبکه ی جهانی وب از این پروتکل استفاده می شود .

- **SSL و TLS :**

این دو پروتکل امنیت تبادل اطلاعات را در شبکه های کامپیوتری فراهم می آورند . در این دو پروتکل کاربر با سرور بر سر اینکه از چه الگوریتمی برای کد گذاری اطلاعات استفاده کنند به توافق می رسند سپس شروع به کد گذاری اطلاعات می کنند، سپس تبادل اطلاعات آغاز می شود .

- **Cryptography**

Cryptography شامل تکنیک هائی است که به مخفی کردن اطلاعات کمک می کند مثل microdots ترکیب لغات و جایگزنی آنها به عکس. در دنیای کامپیوتر Cryptography روی اطلاعات که به فرم متن هستند صورت می گیرد

Cryptography انواعی دارد که شامل موارد زیر است :

  - Confidentiality
  - Integrity
  - Non-repudiation
  - Authentication

طرح پیشنهادی

با توجه به کاربرد گسترده ی این پروتکل در شبکه ی جهانی اینترنت، و همچنین اهمیت آن، موضوع حمله ی مردان میانی به پروتکل HTTPS[8] را بررسی می کنم .

زمان بندی

ID	Task Name	Start	Finish	Duration
1	شناسایی و تهیه منابع	5/3/2016	5/10/2016	6d
2	تنظیم ساختار اولیه	5/11/2016	5/13/2016	3d
3	مطالع و یادداشت برداری	5/16/2016	5/17/2016	2d
4	اجرای علمی پژوهش	5/18/2016	5/20/2016	3d
5	اماده سازی ارایه نهایی	5/23/2016	5/27/2016	5d

[8] Man In The Middle Attack To The HTTPS Protocol