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

روش تحقیق و گزارش نویسی

تکلیف ششم

سید محمد مهدی موسوی
(9231053)

استاد
جناب آقای دکتر صفابخش

فروردین 95

1. ابتدا سعی می کنیم با جستجو در موتور جستجو گر **گوگل** اطلاعات کلی در مورد پروژه به دست آوریم پس عبارات زیر را تایپ می کنیم :

_ “what is a HTTPS ? ”
_ “ Every thing about HTTPS .PDF ”
_”HTTPS over SSL or TLS ”

سپس عبارات فوق را در موتور جستجو گر **بینگ** تایپ می کنیم تا اطمینان پیدا کنیم که اکثر مطالب موجود در اینترنت را مشاهده کرده ایم .

وقتی که اطلاعاتی کلی در مورد موضوع به دست آوردیم حال سعی می کنیم کتابی مرجع در رابطه با موضوع پیدا کنیم برای این منظور در هر دو موتور جستجو گر گوگل و بینگ در رابطه با موضوع جستجو می کنیم تا کتاب مرجعی پیدا کنیم
در ضمن از وب سایت هائی نظیر http://it-ebooks-search.info/ نیز می توان استفاده کرد .
پس از جستجو کتاب زیر را که به صورت رایگان قرار داده شده است می یابیم :

_ “ HTTP - The Definitive Guide”
_ “SSL & TLS Essentials , Securing the Web , Stephan Thomas ”

در این کتاب اول در یک فصل جدا گانه به نحوه ی امنیت بخشیده به پروتوکل HTTP و ایجاد پروتوکل HTTPS پرداخته است که منبع خوبی برای این پژوهش است .

2. حال سعی می کنیم مقالاتی که به صورت جامع در رابطه با یک موضوع تحقیق انجام داده اند پیدا کنیم این مقالات را “survey” می نامند .

به این منظور عبارات زیر را در پایگاه **Google Scholar** و **Academia** تایپ می کنیم .

“HTTPS”
“Survey HTTPS”

کلید واژه هائی که در این جستجو نقش داشته اند : **"HTTPS" و "Survey"**

3. حال سعی می کنیم جستجو را کمی خاص تر کنیم تا در رابطه با موضوعات جزئی تر نیز مقالات مربوطه را پیدا کنیم برای این امر عبارت زیر را در هر دو پایگاه جستجو می کنیم :

“HTTPS over SSL and TLS”
“Implementing SSL and TLS using Cryptography”
“Mathematical Algorithm for cryptography”

کلید واژه هائی که در این جستجو نقش داشته اند عبارت اند از :

“SSL and TLS” و “Cryptography”و “Mathematical” و “Algorithm”

4. حال منابعی را که در گام دوم و سوم پیدا کرده ایم را به ترتیب اهمیت پالایش می کنیم برای این امر از نکاتی که در کتاب درسی و نکاتی که در کلاس درس مطرح شده است بهره می بریم :

1. Analysis of the HTTPS Certificate Ecosystem

   Zakir Durumeric, James Kasten, Michael Bailey, J. Alex Halderman
   Department of Electrical Engineering and Computer Science University of Michigan, Ann Arbor, MI 48109, USA

2. A COMPARISON OF HTTP AND HTTPS PERFORMANCE

   Arthur Goldberg, Robert Buff, Andrew Schmitt ,
   Computer Science Department Courant Institute of Mathematical Science New York University

3. SSL and HTTPS:
   Revisiting past challenges and evaluating certificate trust model enhancements

   Jeremy Clark and Paul C. van Oorschot
   School of Computer Science Carleton University, Canada

4. Man_ In _ The _ Middle Attack To The HTTPS Protocol

   Franco Collegati , Walter Cerroni , Marco Ramilli , Univercity Of Bologna

5. The Cost of the "S" in HTTPS

   David Naylor ; Alessandro Finamore;Ilias Leontiadis;Yan Grunenberger;MarcMellia;Maurizio , Politecnico di Torino Porto Institutional Repository , Carnegie Mellon University

6. HTTPS Hacking Protection

   Thawatchai Chomsiri , Faculty of Informatics, Mahasarakham University, Mahasarakham 44150, Thailand.

7. AN ALGEBRAIC METHOD FOR PUBLIC-KEY CRYPTOGRAPHY

   Iris Anshel, Michael Anshel, and Dorian Goldfeld

8. Digging into HTTPS: FlowBased Classification of Webmail Traffic

   Dominik Schatzmann , Wolfgang Mühlbauer , Thrasyvoulos Spyropoulos , XenofontasDimitropoulos