

**دانشگاه صنعتی امیرکبیر (پلی تکنیک تهران)**

**دانشکده‌ی مهندسی کامپیوتر و فن‌آوری اطلاعات**

**روش تحقیق و گزارش نویسی**

**تکلیف دهم**

**سید محمد مهدی موسوی**

**(9231053)**

**استاد :**

**جناب آقای دکتر صفابخش**

اردیبهشت 95

**\*\*\*مکث کوتاه\*\*\***

**شروع بحث با مطرح کردن موضوع و اینکه چه هدفی قرار است دنبال شود .**

**موضوع اصلی : امنیت بخشیدن به پروتکل HTTP از طریق SSL و TLS**

**هدف خاص : آشنا کردن مخاطبین با نحوه ی برقراری امنیت در پروتکل HTTPS**

**\*\*\*مکث کوتاه\*\*\***

**مقدمه**

1. **ما امروزه برای ارتباط داشتن با دیگران و اطلاع رسانی و برای سادگی کار خودمون از اینترنت استفاده می کنیم** 
   1. همه ی ما اطلاعات شخصی و محرمانه بسیاری با هم ردو و بدل می کنیم .
   2. آیا تا به حال به این فکر کردیم که این اطلاعاتی دیگران آیا می تونند این اطلاعاتی که رد و بدل میشه دسترسی پیدا کنند .
   3. حال فرض کنیم این اطلاعات، جزء محرمانه ترین اطلاعات ما باشه مثل اطلاعات حساب های مالی، یا اطلاعات کاربری رایانامه، یا عکس های خانوادگی و ...
   4. اگه ندانیم که این کانال ارتباطی امن هست، آیا باز هم حاضر هستیم محرمانه ترین اطلاعات خود را از این طریق با دیگران مبادله کنیم .
2. **HTTP چیست ؟**
   1. بیشتر شما با این پروتکل آشنائی کافی دارید و بطور مختصری آن را شرح می دهم
   2. بحث مختصری در رابطه با TCP و UDP مطرح شود .
   3. حال بحث اینکه این پروتکل امینیت ندارد را مطرح کرده
   4. و اشاره می کنیم که در طول این ارائه ما با نحوه ی امنیت بخشیدن به این پروتکل آشنا می شویم
3. **چگونه ممکن است که اطلاعات رد و بدل شده میان Server ها و Client ها در دسترسی دیگران قرار بگیرد .**
   1. مطرح کردن و بررسی ISP
   2. مطرح کردن و بررسی Proxy Server ها
   3. مطرح کردن و بررسی Cache Server ها

**\*\*\*مکث کوتاه\*\*\***

**متن**

1. تبدیل HTTP به HTTPS
2. رمزنگاری دیجیتالی [[1]](#footnote-1)
3. رمزنگاری کلید متقارن [[2]](#footnote-2)
4. رمزنگاری کلید عمومی [[3]](#footnote-3)
5. امضای دیجیتالی [[4]](#footnote-4)
6. گواهی نامه دیجیتالی [[5]](#footnote-5)
7. HTTPS جزئیات [[6]](#footnote-6)
8. یک کاربری حقیقی HTTPS [[7]](#footnote-7)

**\*\*\*مکث کوتاه\*\*\***

**جمع بندی**

1. خب ما می خواستیم که نحوه امنیت بخشیدن به پروتکل HTTP رو بررسی کنیم .
2. مراحلی که برای امنیت بخشیدن به این پروتکل ذکر شد رو بصورت خلاصه با هم مرور می کنیم (در حد یک دقیقه)
3. اگه سؤالی دارید مطرح کنید .
4. مراجع تحقیق رو مشاهده می کنید (توضیح مختصری برای هر کدام از مراجع می دهم )
5. امیدوارم مطالب امروز براتون مفید واقع بوده باشه و ازش لذت برده باشید .
6. مرسی از همگی

1. Digital Cryptography [↑](#footnote-ref-1)
2. Symmetric-Key Cryptography [↑](#footnote-ref-2)
3. Public-Key Cryptography [↑](#footnote-ref-3)
4. Digital Signatures [↑](#footnote-ref-4)
5. Digital Certificate [↑](#footnote-ref-5)
6. HTTPS : The Details [↑](#footnote-ref-6)
7. A Real HTTPS Client [↑](#footnote-ref-7)