**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**
   - 1-1 همه ی ما اطلاعات شخصی و محرمانه بسیاری با هم ردو و بدل می کنیم .
   - 2-1 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 .
   - 3-1 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 ...
   - 4-1 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 ؟**
   - 1-2 بیشتر شما با این پروتکل آشنائی کافی دارید و بطور مختصری آن را شرح می دهم
   - 2-2 بحث مختصری در رابطه با TCP و UDP مطرح شود .
   - 3-2 حال بحث اینکه این پروتکل امینیت ندارد را مطرح کرده
   - 4-2 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 .**
   - 1-3 مطرح کردن و بررسی ISP
   - 2-3 مطرح کردن و بررسی Proxy Server ها
   - 3-3 مطرح کردن و بررسی Cache Server ها

***مکث کوتاه***

## متن

1. اصلاح در پروتکل HTTP، و رسیدن به پروتکل HTTPS
    1.1. مطرح کردن اینکه پروتکل HTTPS همان پروتکل HTTPS است با اصلاحاتی
2. اضافه کردن یک لایه امنیتی به پروتکل HTTP
    2.1. این لایه SSL یا TLS است .
3. لایه ی امنیتی SSL یا TLS
    3.1. آشنائی مختصر با این دو پروتکل
    3.2. تفاوت های این دو پروتکل
4. آشنا شدن با مفاهیم رمز گذاری و رمزگشائی
5. بررسی الگوریتم های رمز گذاری اطلاعات
    5.1. الگوریتم های ساده که قبل از اختراع رایانه ها استفاده می شدند مطرح شود .
    5.2. مشکلات موجود در الگوریتم های ساده
    5.3. مطرح کردن تحول در رمزگذاری اطلاعات
    5.4. اختراع رایانه ها
6. مطرح کردن سیر تکاملی الگوریتم های کد گذاری
    6.1. بررسی مشکلات موجود در هر الگوریتم
    6.2.

***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)

## مراجع

## سؤال

## تشکر