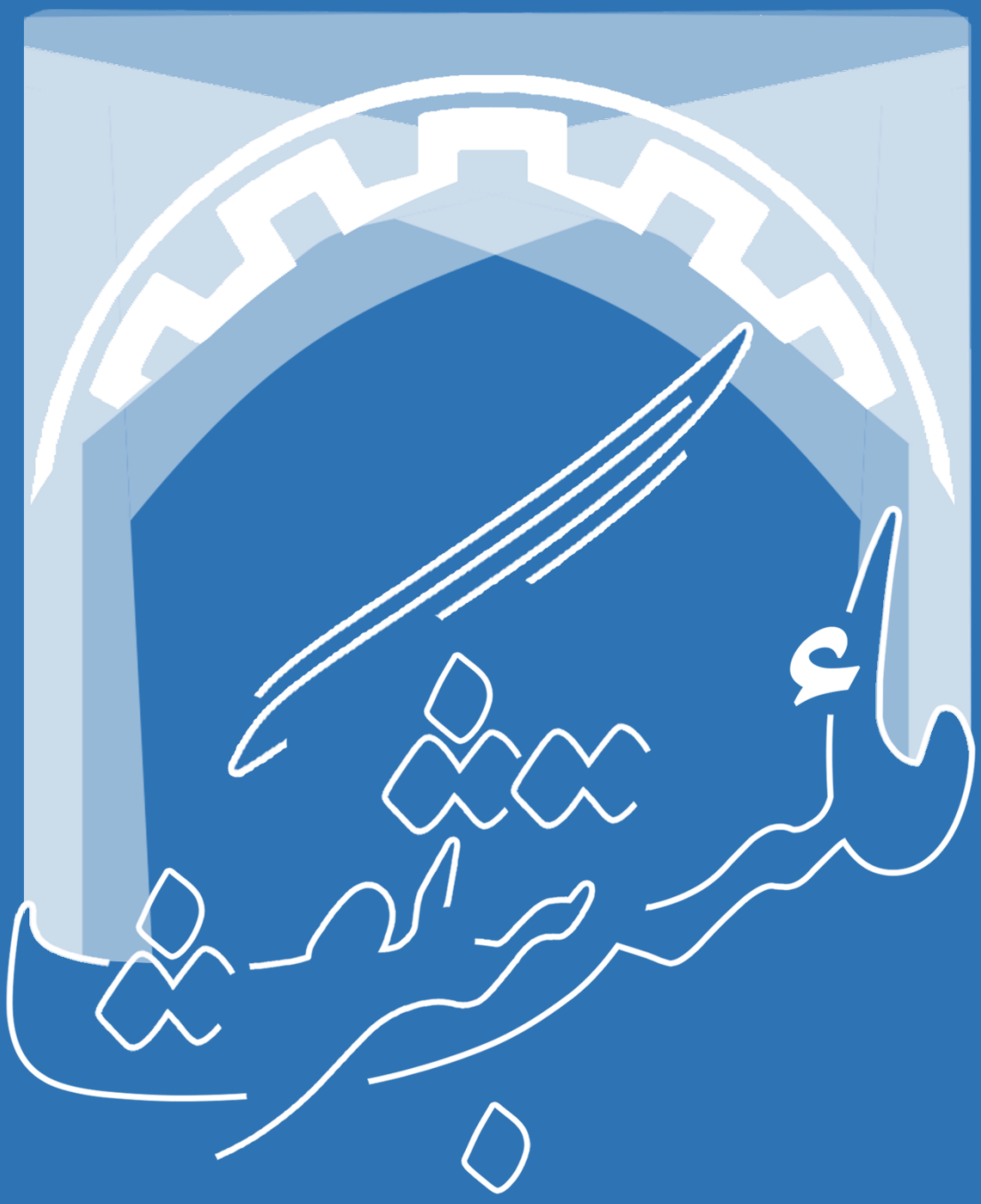
به نام خدا



بهار و تابستان ۱۴۰۰

دوره : PHP 54

نام و نام خانوادگی کار آموز : امیرحسین نجفی زاده

ایمیل : najafizadeh21@gmail.com

عنوان : تمرین اول

مباحث : سوالات پایه از مباحث وب و HTML و PHP

سوال : چند الگو ریتم رمزنگاری در وب را توضیح دهید.

DES که از قدیمی‌ترین استانداردها محسوب می‌شود، در دسته‌ی متقارن قرار می‌گیرد و اصول آن، پایه‌های توسعه‌ی استانداردهای بعدی را شکل داد DES .از کلیدی ۵۶ بیتی (یا هفت بایتی) برای رمزنگاری استفاده می‌کند و ساختار آن براساس ساختار فایستل (دستاورد رمزنگاری مشهور، هورست فارستل) توسعه یافته است.

در الگوریتمDES ، داده‌های شامل متن ساده با طول ۶۴ بیتی در یک بلوک رمزنگاری می‌شوند. ابتدا داده به دو بخش ۳۲ بیتی تقسیم شده و سپس فرایند رمزنگاری روی هریک از آن‌ها به‌صورت مجزا اجرا می‌شود. فرایند مذکور شامل ۱۶ مرحله است که در آن‌ها، انواع عملیات ریاضی روی داده صورت می‌گیرد. درنهایت داده‌های ۶۴ بیتی رمزنگاری‌شده به‌عنوان خروجی از الگوریتم به دست می‌آیند. از نقط ضعف اصلی DES که منجر به منسوخ شدن آن شد، می‌توان به کوتاه بودن کلید رمزنگاری اشاره کرد. بسیاری از متخصصان امنیت موفق به شکستن رمز DES شدند که درنهایت منسوخ شدن آن را در سال ۲۰۰۵ به‌همراه داشت.

نسخه‌ی بهبودیافته‌ی DES به‌نام DES 3معرفی شد. این الگوریتم از دهه‌ی ۱۹۹۰ به شهرت رسید و به‌نوعی برخی از ساختارهای DES را بهینه می‌کرد. همان‌طور که از نام الگوریتم DES 3بر می‌آید، در فرایندهای رمزنگاری آن، سه بار الگوریتم DESرا در هر بلوک داده اجرا می‌کنند .درنتیجه شکستن رمز، دشوارتر خواهد بود. الگوریتم DES 3پس از مدتی به‌عنوان استاندارد محبوب در سیستم‌های پرداخت و استانداردها و فناوری‌های حوزه‌ی مالی استفاده شد. از همین الگوریتم در بسیاری از پروتکل‌های رمزنگاری همچون TLS, SSH, IPsecو OpenVPN استفاده شد.

الگوریتم AES براساس اصول جابه‌جایی و تعویض کار می‌کند. ابتدا داده به‌صورت متن ساده به بلوک‌های متعدد تقسیم می‌شود. سپس با استفاده از کلید رمزنگاری، فرایند رمزنگاری روی بلوک‌ها اعمال می‌شود. خود فرایند رمزنگاری دارای چندین زیر فرایند است که فعالیت‌های گوناگونی را روی داده‌ها انجام می‌دهند. بسته به طول کلید رمزنگاری، ۱۰ یا ۱۲ یا ۱۴ مرحله از زیرفرایندها روی داده اعمال می‌شود.

از مزیت‌های الگوریتم پیشرفته‌ی AES می‌توان به سرعت و امنیت و انعطاف‌پذیری آن اشاره کرد. الگوریتم جدید، سرعتی بسیار بیشتر از DES دارد و تفاوت در طول کلیدها، بهترین مزیت امنیتی آن محسوب می‌شود. فراموش نکنید که هرچه طول کلیدها بیشتر باشد، رمزگشایی دشوارتر خواهد بود.

الگوریتم RSA حاصل همکاری سه متخصص به‌نام‌های Ron Rivest, Adi Shami و Leonard Adlemanبود که از ابتدای نام خانوادگی خود برای نام الگوریتم استفاده کرده و آن را در سال ۱۹۷۷ معرفی کردند. امروزه RSA به‌عنوان پرکاربردترین الگوریتم رمزنگاری نامتقارن شناخته می‌شود. قدرت اصلی الگوریتم مذکور را می‌توان در روش موسوم به Prime Factorizationدید که به‌عنوان پایه‌های آن استفاده می‌شود. در این روش، از دو عدد بسیار بزرگ تصادفی استفاده می‌شود که برای ساختن یک عدد عظیم تصادفی، در هم ضرب می‌شوند. برای شکستن رمزهای RSA باید دو عددی که کلید نهایی و عظیم را ساخته‌اند، شناسایی کنید.

Hash چیست و چه تفاوتی با رمزنگاری دارد ؟ چند الگوریتم Hash را نام ببرید با نمونه مثال.

در این روش یک محاسبه روی پیام انجام می شود و آنرا به یک مقدار عددی تبدیل می کند که به آن Hash Value گفته می شود. بطور مثال هر کاراکتر را در 3 ضرب و با هم جمع و حاصل را بر 10 تقسیم کن. این الگوریتم یک طرفه است و نمی توان از مقدار Hash به متن رسید.

یک الگوریتم آن باقی مانده گیری برای ذخیره سازی داده های عددی است. به طوری که به یک مقدار ثابت از داده عددی باقی مانده میگیریم و عدد را به باقی مانده اش Hash می کنیم.

$$12 \gg 12 \bmod 24 = 12\ ,952863 \gg\ 952863 \bmod 24 = 15$$

برای داده های رشته ایی یک الگوریتم Hash کردن تبدیل آن ها به کد اسکی (ASCII) می باشد و سپس آن را به عنوان Hash Value ذخیره کرد.

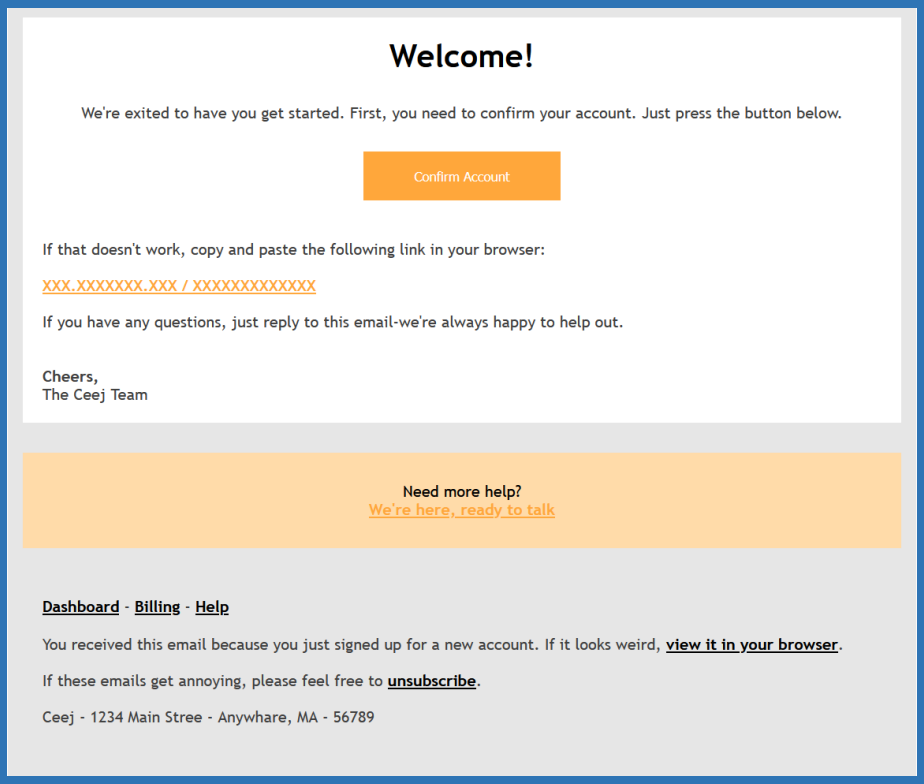
$$amir \gg 97109105114\ (\ a = 97, m = 109, i = 105, r = 114\ )$$

چه تفاوتی بین GET و POST در HTTP است ؟

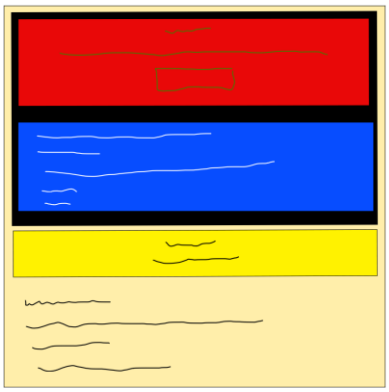
متود Post	متود Get
پارامترهای POST در بدنه گنجانده شده است. پس امنیت بالاتری دارد	پارامترهای GET در URL موجود است
از متد POST اغلب برای بروزرسانی داده‌ها برای تغییر در سرور یا داده‌های ذخیره شده در سرور استفاده می‌شود	از متد GET اغلب برای واکشی اسناد استفاده می‌شود و از پارامترهای GET برای توصیف اینکه به دنبال کدام سند هستید، در چه صفحه‌ای هستید و... استفاده می‌شود
هیچ محدودیتی در طول URL ندارد	از آنجا که پارامترها در URL می‌آیند، حداکثر طول URL دارای محدودیت است
با فراخوانی متدPOST ، اطلاعات ذخیره شده تغییر می‌کنند، پس تراکنش بین سیستمی پیچیده‌تر می‌شود	در اغلب موارد، هنگامی که شما یک درخواست ساده را با استفاده از متد GET ارسال می‌کنید، تراکنش بین ماشین‌ها و سیستم‌ها کمتر است
داده‌های موجود در سرور را تغییر می‌دهد	با فراخوانی پی در پی یک متد GET اطلاعات بازگشتی از سمت متد GET نباید تغییر کنند

مباحث HTML

از ما خواسته شد تا به صورت کد HTML یک صفحه ایی طراحی کنیم که خروجی آن مشابه تصویر زیر باشد.



در ابتدا یک شماتیک کلی حاصل برداشت خودم از عکس را رسم کردم.



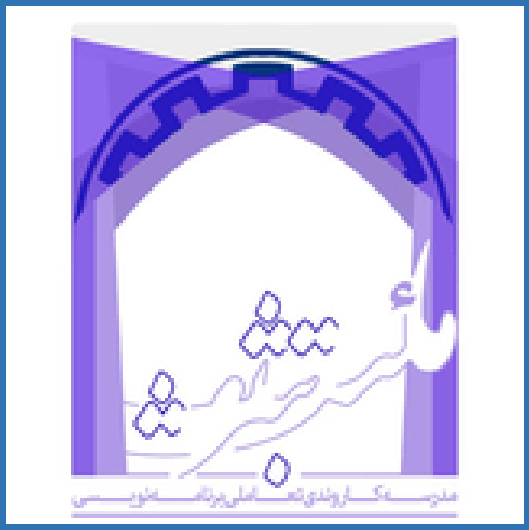
سپس با استفاده از تگ div و دیگر تگ های لازم صفحه را درست کردم.

کد ها در فایل index.html قرار دارند.

مباحث PHP

از من خواسته شد تا ده درخواست را در زبان PHP انجام دهم که مباحث ابتدایی PHP مانند if-else , حلقه ها , رشته ها, عبارات Boolean شامل آن ها می شد.

فایل کدها در index.php قرار دارد.



با تشکر از توجه شما

امیرحسین نجفی زاده

دوره 54 ام PHP مکتب شریف