گزارش‌کار پروژه مخابرات دیجیتال. بخش ۳

««««یک افسانه دیجیتال»»»»

قسمت سوم: تشکیل امپراتوری

طرح ریزی برای این بخش

تلاش برای کامل کردن بخش کدینگ و افزودن منبع

تلاش من در روند پروژه تا اینجا این بود که به بلوک‌دیاگرام اولیه وفادار بمانم. در بلوک‌دیاگرام من یک بخش برای رمزنگاری داده‌ها تعبیه کرده بودم. احتمالا اکنون زمان مناسبی برای پیاده‌سازی این بخش باشد.

هم‌چنین هنوز منبع ندارم. طبق تصمیم اولیه منبع را متن در نظر خواهم گرفت.

کار دیگر من پیاده‌سازی تمام الگوریتم‌ها بصورت پیش‌فرض در حالت کلی است. سازگار با تمام مدولاسیون‌هایی که می‌شناسم.

در نهایت تلاش من این است که به سیستمی برسم که کار اصلی خودش را شروع کند. یک سیستم که بالاخره کار می‌کند!

بلوک‌دیاگرام

بلوک‌دیاگرام من بدین شکل بود:

منبع: ورودی داده ← **کدینگ منبع ← رمزنگاری ← کدینگ کانال ← ترکیب سیگنال ← کانال ←**

تفکیک سیگنال ← کدگشایی کانال ← رمزگشایی ← کدگشایی منبع ← خروجی سیستم

اکنون شکل جزئی‌تر هر بخش آن به این شکل است:

منبع : متن. احتمالا با استاندارد اسکی

کدینگ منبع ← تبدیل متن ورودی به اعداد

رمزنگاری : رمزنگاری به روشی شبیه به One Time Pad ← اضافه کردن یک سری اندیس به داده برای کمک به رمزگشایی.

کدینگ کانال: ← اضافه کردن بیت‌های تشخیص خطا ← اضافه کردن فلگ برای مشخص کردن ابتدای بلوک‌ها ← کدینگ دیفرانسیلی (مربوط به مدولاسیون)

مدولاسیون: مدولاسیون PSK . مدولاسیون در حالت باینری است اما برای M تایی هم کار می‌کند.

کانال: اعمال یک فیلتر میانگذر در سمت فرستنده ← اعمال یک شیفت زمانی ← اضافه کردن نویز ← اعمال یک فیلتر میان گذر در سمت گیرنده

دیمدولاسیون ← محاسبه انتگرال قطعات سیگنال ضرب شده در ۲ عامل سینوسی و کسینوسی و به دست آوردن فیزورها ← تبدیل فیزورها به اعداد دیمدوله شده به روش دیفرانسیلی

کدگشایی کانال: حذف فلگ‌های اضافه شده و تشخیص بلوک‌های داده ← چک کردن خطاها با استفاده از کدهای parity اضافه شده

رمزگشایی ← کمک گرفتن از اندیس‌های موجود و رمزگشایی داده. هم‌چنین حذف اندیس‌ها از داده

کدگشایی منبع ← تبدیل اعداد دریافت شده به حروف.

هم‌چنین برای سازگار نگهداشتن بلوک‌ها با یک‌دیگر برخی بلوک‌های اضافی هم ساخته‌ام.

کارهایی که کردم

افزودن اندیس به داده‌ها برای کمک به رمزگشایی

برای کمک به رمزگشایی نیاز بود که از یک سری اندیس استفاده کنم. با توجه به این که اگر اندیس‌ها اشتباه شوند، خروجی اصلا قابل تشخیص نخواهد بود. هرچند با کوشش انسانی یافتن اندیس شدنی است، اما سیستم ما نباید نیاز به چنین چیزی داشته باشد.

پس به آغاز هر بلوک، اندیس آن بلوک را نیز افزودم.

پیدا کردن اندیس‌ها و حذف آن‌ها از داده

حال که اندیس‌هایی را به داده افزوده‌ایم، باید در بخش آشکارسازی آن‌ها را از داده پاک کنیم و عوض آن‌ها را جداگانه در کنار داده خام به خروجی ارسال کنیم.

این کار به سادگی صورت می‌پذیرد. چرا که قبلا با کمک بیت‌های راهنما، بلوک‌ها را از هم جدا ساخته‌ایم.

طراحی سیستم رمزنگاری

به احتمال زیاد برای رمزنگاری از روشی شبیه به one time pad استفاده خواهد شد.

در این روش هر بلوک داده با یک بلوک هم‌اندازه خودش xor خواهد شد. البته این عمل xor واقعی نیست! بلکه همان عملگر تعمیم‌یافته است که در بخش قبل طراحی کرده بودم.

اما خود بلوکی که باید با این xor شود چگونه ساخته می‌شود؟

این بلوک از لیستی شامل تعداد زیادی بلوک رندوم از پیش ساخته شده انتخاب می‌شود. بلوک‌ها را به ترتیب از آن لیست خارج می‌کنیم و ۱ بار استفاده می‌کنیم. در سمت گیرنده نیز باید از همان لیست استفاده شود. اگر پاد همان عمل رمزنگاری را انجام دهیم، داده‌ها رمزگشایی خواهند شد.

پس انتخاب بلوک درست از لیست مهم است و برای همین اندیس بلوک به همراه خود بلوک اضافه می‌شود.

البته اندازه بلوک‌های رمزنگاری می‌تواند کوچک‌تر از اندازه بلوک‌های داده‌ای باشد که میخواهند در کانال ارسال شوند. در این صورت برای افزودن اندیس باید فرض شود اندازه بلوک رمزنگاری ما کسری صحیح از بلوک‌های ارسالی است فرض کنیم این عدد برابر k باشد. در این صورت اگر شماره بلوکی که می‌خواهیم رمز کنیم داخل بلوک پرچم دار برابر r باشد، اندیس بلوک رمزنگاری ما نیز با یک رابطه به دست می‌آید:

اندیس بلوک رمز = k * اندیس بلوک پرچم دار + r

نکته اینجاست که هنوز بلوک رمزنگاری را پیاده‌سازی نکرده‌ام! اما این روش منطقی به نظر می‌رسد!

کدگذاری منبع

منبع من متن است. یک فایل شامل متنی را انتخاب کردم و آن‌را باز کردم. هر حرف فایل را به روش اسکی دیکد کردم و بعد با تبدیل اعداد دهدهی به دودویی آن‌را کدگذاری کردم و به عنوان داده ورودی به سیستم دادم.

سیستم من بالاخره شامل یک منبع شد!

کدگشایی منبع

هر علامت از منبع من (هر کاراکتر از متن)، بعد از کدگذاری شامل چند عدد می‌شود. برای این که کدگشایی این اعداد و بعد از آن کدگذاری متن درست انجام شود نیاز است ابتدای هر بلوک را بشناسیم. که این کار به درستی انجام می‌شود.

تلاش برای افزایش سازگاری بلوک‌ها

در تلاش برای افزایش سازگاری بلوک‌ها با یک‌دیگر بلوک‌های مختلف را از سیستم حذف می‌کنم و آن‌ها را دوباره اضافه می‌کنم. در این روش از یک سیستم ساده پایدار شروع می‌کنم و سعی می‌کنم بعد از اضافه کردن هر بلوک، سیستم هم‌چنان پایدار بماند. اگر پایدار نبود، بلوک جدید را ویرایش می‌کنم و به سیستم وفادار می‌مانم. در نهایت یک سیستم بزرگ و پیچیده ایجاد می‌شود که کار می‌کند!

افزودن امکان حذف یا جایگزینی بلوک‌ها به سیستم اصلی

برای تست، برای خطایابی، برای گسترش سیستم یا برای جایگزینی بلوک‌ها، نیاز است سیستم اصلی به شکلی طراحی شود که هر یک از بلوک‌ها را بتوان حذف کرد یا دوباره به سیستم اضافه‌کرد. این‌کار را این دفعه انجام دادم و باعث شد سیستم قوی‌تر به نظر برسد و کار کردن با آن آسان‌تر باشد.

نتیجه گیری

- متلب یک داکیومنت درست ندارد! توابع متلب باهم سازگار نیستند و بعد از آن تبدیل تایپ‌ها در متلب طاقت‌فرساست.

  اندیس‌ها از ۱ شروع می‌شود. همه محاسبات را دوباره انجام بده! این ویژگی متلب غیرقابل تحمل است و گویا هیچ چاره‌ای هم ندارد.

- از اضافه کردن بلوک رمزنگاری به بلوک‌دیاگرام اولیه سیستم احساس پشیمانی می‌کنم! پیاده‌سازی این بخش برای خودش نیاز به صرف زمان و انرژی دارد و کار من را سخت‌تر خواهد کرد. البته هنگام شروع پروژه چیزی مثل کمبود وقت یا سایر عوامل غیرقابل کنترل را در نظر گرفته بودم ولی با این حال امیدوار بودم اتفاق نیفتد! (نیافتد؟)
- به تازگی متوجه شده‌ام بخش‌هایی از سیستم هنوز با تغییر شرایط ناپایدار می‌شوند. باید پارامترهای سیستم را یکی یکی تغییر دهم و تست کنم تا از پایداری کدی که نوشته‌ام در شرایط مختلف مطمئن باشم. یعنی تست‌های بیشتری روی برنامه باید انجام دهم.

- پس از این که سیستم من کار کرد، وقت آن است که مشخصات کیفیت انتقال را با آزمایش استخراج کنم.

  تا سیستم من یک شناسنامه داشته باشد. دارای اطلاعاتی مثل این که سیستم من در چه نویزی چقدر خطا دارد و اضافه کردن یا حذف کردن هر یک از بلوک‌ها چه تاثیری در خطا دارد. یا این که بیشترین نرخ ارسال داده در این پهنای باند برای سیستم من چقدر است.

- در نهایت از پیشرفت خودم در این مرحله، در حد مراحل قبل راضی نبودم. البته برای سیستم تلاش زیادی کردم ولی قصد داشتم بخش رمزنگاری را در این مرحله کامل کنم و مرحله بعد را تنها به بررسی سیستم اختصاص دهم. به هر حال سیستم از مراحل قبل اشکالاتی داشت و مجبور بودم آن‌ها را در این مرحله برطرف کنم. هرچند هم‌چنان بعضی از اشکالات حل نشده‌اند.