پروژه پایانی برنامه نویسی درس طراحی الگوریتم پیشرفته – نیمسال اول ۱۴۰۳-۱۴۰۲ – دانشگاه کردستان

مدرس: آمانج خرّمیان

عنوان	طراحی و پیاده‌سازی یک الگوریتم برای کدگذاری و رمزگذاری یک فایل متنی با استفاده از الگوریتم‌های هافمن و AES
اهداف	• آشنایی با مفاهیم کدگذاری هافمن، رمزگذاری فایل و الگوریتم AES • پیاده سازی الگوریتم های کدگذاری هافمن، رمزگذاری فایل و الگوریتم AES • ارزیابی کارایی و قابلیت استفاده از برنامه های پیاده سازی شده
توضیح	ابتدا یک فایل متنی حاوی حروف انگلیسی و فاصله از ورودی دریافت می‌شود. سپس با استفاده از الگوریتم کدگذاری هافمن، فایل متنی فشرده شده ذخیره و جدول کدگذاری مربوطه نمایش داده می‌شود. در مرحله بعدی، از شماره دانشجویی به عنوان کلید رمزگذاری برای الگوریتم AES استفاده می‌شود. فایل فشرده شده فوق با استفاده از الگوریتم AES رمزگذاری شده و در یک فایل جدید ذخیره می‌شود. برنامه نوشته شده به کاربر امکان رمزگشایی از فایل رمز شده با استفاده از همان کلید دانشجویی و سپس بازیابی فایل اصلی از طریق فایل کدگذاری شده هافمن را فراهم می‌کند. این فرآیند تضمین می‌کند که اطلاعات اصلی با دقت بازیابی شوند و همچنین امانت اطلاعات با استفاده از رمزگذاری AES حفظ گردد.
ورودی‌ها	• یک فایل متنی از روی دیسک با اسم input.txt صرفاً شامل حروف انگلیسی و کاراکتر فاصله • شماره دانشجویی به عنوان کلید رمزگذاری
خروجی‌ها	• یک فایل جدید، با اسم huffman.txt کدگذاری شده فایل ورودی با الگوریتم هافمن • نمایش جدول کدگذاری مربوطه و ذخیره آن با اسم huffman_table.txt داخل یک فایل برای مراجعات بعدی • فایل cipher.txt حاوی رمزگذاری شده فایل huffman.txt با الگوریتم AES و کلید ورودی (شماره دانشجویی) • همچنین برنامه باید قابلیت رمزگشایی فایل رمزگذاری شده با استفاده از همان کلید و نمایش فایل اصلی با استفاده از فایل کدگذاری شده هافمن را داشته باشد
بخش اول (کدگذاری هافمن)	یک فایل متنی شامل صرفاً کاراکترهای انگلیسی a تا z و کاراکتر فاصله از ورودی گرفته می شود. این فایل حاوی هیچ کاراکتر دیگری نیست. یعنی کاراکترهای نقطه، کاما، حروف بزرگ و سایر کاراکترها نیست. سپس، با استفاده از الگوریتم کدگذاری هافمن، برای هر کاراکتر یک کد دودویی اختصاص داده می شود. سپس، جدول کدگذاری نمایش داده می شود. در نهایت فایل کدگذاری شده روی دیسک ذخیره می‌شود. برای این کار میتوانید مثلاً هر هشت بیت را بصورت یک کاراکتر ذخیره کنید.
بخش دوم (رمزگذاری فایل)	فایل کدگذاری شده هافمن با استفاده از شماره دانشجویی بعنوان کلید و الگوریتم AES رمزگذاری می شود. در نهایت، فایل رمزگذاری شده بصورت یک فایل جدید ذخیره می شود.
یادآوری	• الگوریتم هافمن: یک الگوریتم برای کدگذاری متغیر طولی که بر اساس تکرار هر کاراکتر در یک متن، کدهای کوتاه‌تری به کاراکترهای پرتکرار و کدهای بلندتری به کاراکترهای کم‌تکرار اختصاص می‌دهد. این الگوریتم باعث می‌شود که حجم فایل متنی کاهش یابد و ذخیره‌سازی آن بهینه‌تر شود. • الگوریتم AES: یک الگوریتم برای رمزگذاری متقارن است که با استفاده از یک کلید مشترک بین فرستنده و گیرنده، یک متن را به چندین بلوک ۱۲۸ بیتی تقسیم می‌کند و با اعمال چندین گردش روی هر بلوک، متن را رمزگذاری می‌کند. این الگوریتم یکی از معروف‌ترین و مطمئن‌ترین الگوریتم‌های رمزگذاری است. برای یافتن الگوریتم AES جستجو کنید.
نکته	تمام الگوریتم‌ها (منجمله الگوریتم هافمن و AES) می‌بایست توسط دانشجو پیاده‌سازی شوند.
زبان‌برنامه‌نویسی	C یا C++
ارزشیابی	پروژه بر اساس موارد زیر ارزیابی خواهد شد • صحت پیاده سازی الگوریتم ها • کارایی برنامه • قابلیت استفاده از برنامه
تحویل	آخرین مهلت تحویل پروژه و نحوه تحویل آن متعاقباً از طریق گروه تلگرامی مربوطه اعلام خواهد شد

موفق باشید