النص الكامل لدرس "الصورة السّحريّة"

المقطع الأول:

كان يا ما كان في قديم الزمان

أتت امرأة إلى الحاكم و قالت له

أشكو إليك قلة الفئران في بيتي.

فتعجب الجالسون حول الحاكم

فيما هو فهم كلامها، و أصدر أمره فقال:

املؤوا لها بيتها خبزاً و لحماً و سمناً و تمراً.

السلام عليكم و رحمة الله و بركاته

أهلاً و مرحباً بكم في هذا الدرس

أنا عبد الله صالح صدّيق، مبرمج حاسب آلي، أعمل هنا في مركز سلطان بن عبد العزيز للعلوم و التقنية (سايتك)، في مدينة الخبر، في المملكة العربية السعودية.

سنتحدث اليوم عن التشفير، و هو تحويل البيانات من الشكل المفهوم لكل شخص، إلى شكل آخر يتعذر على من لا يعرف خبرة محددة أن يعرف محتوى البيانات.

لقد استُخدم التشفير منذ أقدم العصور في المراسلات الحربية و الدبلوماسية، و في التجسس.

و يُعتبر العالم العربي المسلم يعقوب بن إسحاق الكندي، الذي عاش في بغداد أيام الخليفة المأمون، أول من وضع طريقة لفك التشفير و دوّن ذلك.

و هو صاحب كتاب علم استخراج المُعَمّى.

سنتحدث اليوم عن التشفير و الإخفاء، و لكن باستخدام الحاسب الآلي أحد أهم أدوات عصرنا الحديث.

ما رأيكم، لو أردت إرسال ملف حاسوبي إلى شخص آخر، هل من الممكن أن أشفره و أخفيه داخل صورة رقمية، دون أن يبدو عليها تغيير في شكلها، و دون تغيير في حجمها؟ هل ذلك ممكن؟ و لماذا؟

فكروا في ذلك جيداً، و تناقشوا حوله، و سأعود إليكم بعد دقيقتين إن شاء الله.

المقطع الثاني:

السلام عليكم. لعل الكثيرين منكم قالوا إنه من غير الممكن وضع ملف داخل صورة.

لكن دعوني أقول لكم إن هذا ممكن باستخدام التشفير و الإخفاء.

و لنتذكر بداية أن الحاسوب هو جهاز يعتمد كلياً على التشفير، لكنه تشفير غير سرّي، و هو معروف لدى جميع المبرمجين، فالحاسوب جهاز إلكتروني، لا يميز سوى حالتين فقط هما أساس النظام الثنائي:

وجود جهد محدد من الكهرباء، و هو ما اصطلح على تسميته بالواحد المنطقي. وجود جهد ضئيل من الكهرباء، و هو ما اصطلح على تسميته بالصفر المنطقي.

لقد تم ترميز الحروف و الأرقام و الرموز الأخرى الأساسية التي يفهمها البشر و يتعاملون بها يومياً باستخدام ثمانيات من الأصفار و الواحدات، و تم تسمية تلك الثمانية بالبايت، و هي واحدة قياس حجوم البيانات على الحواسيب كما تعلمون، و البت هو الجزء الواحد من هذه الثمانية، تم اعتماد جدول الترميز الأمريكي المعياري لتبادل البيانات ASCII، و الذي يحوي جميع هذه المحارف و عددها ٢٥٦ محرفاً.

لاحظوا أن حرف (A الكبير) هو المحرف رقم ٦٥ في الجدول بينما الحرف (a الصغير) هو المحرف رقم ٩٧ من الجدول، و أما الرقم (0) فهو المحرف رقم ٤٨، و [المسافة] التي نستخدمها للفصل بين الكلمات هي المحرف رقم ٣٢، و أن هناك مجموعة من رموز العمليات الحسابية و الرموز الأخرى.

مثال: كلمة "Salaam" يتم ترميزها كما يلي:

"S": (83) = [01010011]

دعونا نستذكر معاً كيفية التحويل من النظام العشري إلى الثنائي

إن لكل بت قيمة موضحة تحته في هذا الشكل

كل ما علينا هو اختيار مجموعة من الأرقام مجموعها ٨٣ و وضع ١ في البت الذي تشير إليه كل منها، و وضع صفر في باقي الخانات كما يلي:

١ ١ ١ ١ و البقية أصفار

و بالمثل "a": (97) = [01100001]

"l": (108) = [01101100]

"m": (109) = [01101101]

و الآن لنقم بالبحث عن طريقة نقوم فيها بتشفير جملة من عدة كلمات، باستخدام أساليبنا الخاصة، سنقسمكم إلى مجموعات:

المجموعة (أ) تقوم بكتابة جملة بطريقة مشفرة و تعطيها إلى المجموعة (ب)

المجموعة (ب) ستحاول فك التشفير من خلال التخمين و التجربة و المحاولة، فإن لم تستطع سنعطيها للمجموعة الثالثة (ج)، حيث سيقومون بفك التشفير اعتماداً على الطريقة التي سيزودهم بها زملاؤهم في المجموعة (أ)

قوموا بهذا النشاط بالتعاون مع مدرسكم، و سأعود إليكم بعد دقائق إن شاء الله.

المقطع الثالث:

أهلاً بكم ثانية، لقد سررت بمحاولاتكم، و أعجبني أولئك الذين تمكنوا من فك التشفير، و كما لاحظتم أنه من أبسط الطرق، أن نستبدل بالحرفِ الحرفَ الذي بعده في الأبجدية، أو الحرف الذي قبله، أو أن نستخدم جدولاً خاصاً بنا نقوم فيه بتبديل الأحرف.

و قد وجدتم أنه من الممكن فك التشفير من خلال تخمين ما قام به المشفر، أو من خلال ملاحظة

تكرار حروف معينة، و هي الطريقة التي كان العالم الكندي أول من استخدمها. (تحليل التواتر)

حسناً، لكن ألا تشاطرونني الرأي أن التشفير وحده غير كافٍ، فلعله يثير فضول بعض الأشخاص، و يدفعهم إلى منع وصول الرسالة، أو محاولة اكتشاف ما بداخلها، أليس من المناسب أن نقوم بالإخفاء؟! دعونا نجرب هذا الشيء، لدينا هنا كيس.

لدينا هنا شيء داخل الكيس، هل تستطيعون معرفته؟ إنه كرة، دون أن نراها نستطيع أن نعرف أنه كرة، هذا ليس مناسباً، هذا إخفاء غير مناسب.

دعونا نجرب شيئاً أفضل، لدينا هنا كأسان من الشاي اللذيذ، سأضع سكراً في أحدهما و أحركهما كليهما.

و سأسأل صديقي عبد الكريم هذا السؤال: لو سمحت يا عبد الكريم، أياً من الكأسين فيه سكر؟ هل تستطيع بمجرد النظر أن تعرف أيهما فيه سكر؟

لا أستطيع.

شكراً لك.

دعونا نبحث عن شيء يشبه هذا، إذا دعونا نتعرف على طريقة برنامج الرسام في نظام ويندوز و كيفية تخزين الصور الرقمية النقطية ٢٤ بت. إنها تشبه هذه اللوحة.

لدينا هنا صورة مكونة من ٤ بكسلات، ٤ خلايا، لقد كبرناها ٢٥٠٠ مرة حتى تروها بهذا الشكل، سأخزن هذه الصورة، و أفتحها بمحرر ست عشري، يعرفه المبرمجون.

كما ترون لقد تم تخزين الصورة بهذه الرموز، لدينا هنا ملف BMP، لاحظوا أن هناك رأساً للملف مكون من ٥٤ بايت، و أن البايتات من ٣٥ و حتى ٣٨ تحدد حجم البيانات، بعد الرأس

تأتي البيانات، و ما هي إلا رموز الألوان المستخدمة في تلوين كل خلية، حيث يتم تخصيص ثلاثة بايتات لأجل لون كل خلية ابتداءاً من الخلية التي في أقصى يسار السطر الأخير من الصورة و انتهاءاً بالخلية التي في أقصى يمين السطر الأول من الصورة حيث:

البايت الأول لكمية اللون الأزرق في الخلية

البايت الثاني لكمية اللون الأخضر

البايت الثالث لكمية اللون الأحمر

و كل منهم يأخذ إحدى القيم من ٠ إلى ٢٥٥

و من هنا كان بإمكاننا أن نختار لون الخلية لوناً واحداً من حوالي ١٦ مليون لون، لأن

٢٥٦ × ٢٥٦ × ٢٥٦ = ١٦٧٧٧٢١٦ لون، هي احتمالات لون الخلية

كما نلاحظ أن هناك بايتات إضافية تحمل القيمة ٠ تستخدم لإتمام عدد بايتات سطر واحد من الصورة، إلى رقم من مضاعفات العدد ٤، و هذا من تصميم واضعي هذا النوع من الملفات الحاسوبية.

و لعلكم تتساءلون عن الأنواع الأخرى من الصور مثل jpg، نعم يمكن استخدامها، غير أن الطريقة صعبة بعض الشيء.

و الآن ريثما أشرب هذا الكأس من الشاي، حاولوا –كل مجموعة على حدة- محاولة البحث عن طريقة (لتذويب)، عفواً، لتشفير الملفات في الصور، ألقاكم بعد قليل.

المقطع الرابع:

حسناً هل تمكنتم من إيجاد طريقة، ربما لاحظتم أن عيوننا غير قادرة على تمييز ١٦ مليون لون تماماً كما الحاسوب، يمكننا الاستفادة من هذه النقطة، تخيلوا أن لدينا ٢٥٦ لوناً متدرجة من الأبيض إلى الأحمر القاني، أبيض، أحمر، أكثر، أكثر، أكثر، الأحمر القاني. هل تستطيعون التمييز بين اللون الأحمر ٢٥٥ و الأحمر ٢٥٤، لا أعتقد ذلك.

الآن صرنا أقرب إلى تحقيق هدفنا، و هو تشفير ملف داخل صورة دون أن يبدو عليها تغيير في شكلها و دون تغيير في حجمها.

ابحثوا عن مكان لتخزين الملفات داخل الصورة النقطية.

المقطع الخامس

أشكركم على إجاباتكم، بالطبع يمكننا الاستفادة من البت الأدنى لأجل تخزين بت من الملف المراد تشفيره، و هكذا يتم توزيع بتات الملف كبديل للبتات الدنيا في بايتات ألوان خلايا الصورة، و التي لا تشكل كبير أهمية للصورة. تذكروا أن جميع الملفات سواء النصية أو الرسومية أو غيرها ما هي إلا مجموعة من البايتات المتتالية.

كما يمكننا أن نستخدم ٢ بت، أو ٣ بت، أو حتى ٤ بت، طبعاً البتات الدنيا لأجل التشفير، حيث سيحصل تغيير بنسبة ٢٥٥/١٥، أي ما لا يتجاوز نسبة ٦% من جودة ألوان الصورة، و بعد قليل ستَرَون أن هذه النسبة أحياناً لا يمكن للعين البشرية تمييزها بسهولة في الصور ذات الجودة العالية المفعمة بالتدرجات اللونية.

الآن أريدكم أن تحاولوا الإجابة على الأسئلة التالية أثناء الفاصل:

١ -قوموا بحساب الحجم الذي تستوعبه الصورة من البيانات المخفية في كل من الحالات التالية:
أ - استخدام ١ بت
ب - استخدام ٢ بت
ت - استخدام ٤ بت
٢ -ماذا يحصل لو استخدمنا ٨ بت؟

المقطع السادس:

لنقم بحساب الحجم، مع الانتباه إلى أننا سنحتاج بايتات إضافية لنحدد أن الملف المشفّر المخبّأ داخل الصورة قد انتهى، و هذا سنحتاجه أثناء عملية فك التشفير لمعرفة أننا انتهينا، إذ لا مانع من أن تكون الصورة أكبر من الحجم اللازم لتخزين الملف المشفر.

مثلاً كلمة (فسنستنبكتك#) كلمة غير ذات معنى! و بفرض أننا لا نتوقع وجودها في أي ملف نريد تشفيره، يمكننا استخدامها كإشارة إلى انتهاء التشفير، عدد حروفها ١١ و بالتالي نحتاج ٨٨ بت إضافية.

إذا كان حجم الملف المراد تشفيره

١ ميغا بايت، أي ١٠٢٤ كيلو بايت، أي ١٠٤٨٥٧٦ بايت، أي ٨٣٨٨٦٠٨ بتات

أضفنا إليها ٨٨ فتصبح:

٨٣٨٨٦٩٦

و باستخدام ١ بت فقط من كل بايت من بايتات ألوان خلايا الصورة، سنحتاج إلى

٨٣٨٨٦٩٦ بايت

و لأن كل ٣ بايت تكون خلية سنحتاج ٢٧٩٦٢٣٢ خلية

بالجذر التربيعي للرقم السابق نجد أننا بحاجة إلى

صورة مربعة من ١٦٧٣ × ١٦٧٣ خلية

لكن يفضل استخدام ١٦٧٦ × ١٦٧٦

لأنه إذا كان لدينا ١٦٧٦ خلية في السطر، و كل خلية تخزن في ٣ بايت، فإنه سيكون لدينا ٥٠٢٨ بايت

و هو رقم يقبل القسمة على ٤ دون باقٍ، ما يمنع وجود بتات إضافية في سطور الصورة، تفضحنا إذا استخدمناها في التشفير، و هي ينبغي أن تكون قيمتها صفراً فقط.

إذاً لتشفير ملف ما، نصاً كان أو جدولاً أو عرضاً تقديمياً، أو أي نوع آخر حجمه ١ ميغا بايت، يمكننا استخدام صورة bmp عرضها ١٦٧٦ خلية و ارتفاعها مثل ذلك، و هو ما يقارب ١٥×١٥سم، و هي صورة شبيهة بتلك التي تلتقطها الهواتف المحمولة، و آلات التصوير الرقمية ذات الدقة ٣ ملايين خلية. (3 Mega Pixel)

مما سبق نجد أنه يمكن أن نلخص ذلك بالعلاقة التالية:

س>= ٨×(ح+ن)/(٣×ع)

حيث:

س عدد صحيح يمثل عدد خلايا الصورة (عرضها × ارتفاعها)

ح حجم الملف المراد تشفيره مقدراً بالبايت

ن عدد بايتات كلمة الإشارة إلى النهاية

ع عدد البتات الدنيا التي نريد استخدامها من كل بايت من بايتات ألوان خلايا الصورة

و باستخدام العلاقة السابقة نجد أنه

باستخدام ٢ بت من كل بايت من بايتات ألوان خلايا الصورة، سنحتاج إلى

١٣٩٨١١٦ خلية

أما باستخدام ٤ بت من كل بايت من بايتات ألوان خلايا الصورة، سنحتاج إلى

٦٩٩٠٥٨ خلية (و هي صورة حجمها ٧×٧سم بدقة ٣٠٠نقطة/بوصة)

و ذلك لتشفير ملف حجمه ١ ميغا بايت كما أسلفنا، و هذا حجم يمكن أن يستوعب نص كتاب ضخم من أكثر من ٨٠٠ صفحة.

أما إذا استخدمنا ٨ بت فسيتم تغيير الصورة بنسبة ١٠٠% و ستتشوه كلياً، و بالتالي سيتم معرفة أنها تحوي بيانات مشفرة بسهولة.

و الآن أعزائي، سأترككم بضعة دقائق لتفكروا في السؤال التالي:

ما هي متطلبات برمجة برنامج حاسوب يقوم بعملية التشفير و الإخفاء هذه؟

المقطع السابع:

السلام عليكم، في الحقيقة أنا متأكد أن معظم من لديه إلمام بالبرمجة، و طريقة كتابة الجمل الشرطية و الحلقات التكرارية، قادر على كتابة برنامج يقوم بهذا العمل، كل ما عليه أن يعرف كيف يقوم بالأشياء التالية:

١ -فتح و قراءة بايت من ملف ثنائي (الصورة + الملف المراد تشفيره)
٢ -تجزئة البايت إلى بتات و وضعها في بايتات ملف الصورة
٣ -إضافة كلمة النهاية، و حفظ الملف الثنائي الناتج (الصورة السحرية)

بالنسبة لي لقد اخترت أن أقوم بكتابة برنامج حاسوبي باستخدام لغة Visual Basic ليقوم بعملية التشفير و فك التشفير.

يمكنكم تنزيل نسخة منه من موقع بلوسومز.

سأقوم بتشفير هذا الملف النصي البسيط الصغير داخل صورتي الشخصية هذه

انظروا كم هو سهل الاستخدام، نشغل البرنامج و نختار تشفير

نختار الصورة، و الملف النصي، و نحدد اسماً للملف الناتج و مكان تخزينه، ثم نضغط ابدأ

ننتظر هنيهة، و سيكون الأمر قد انتهى.

الآن انظروا إلى الصورة السحرية الناتجة، إنها تبدو مماثلة لصورتي الشخصية

و حجمها مطابق لحجم صورتي الشخصية، يا له من شيء جميل.

تعالوا نشفر هذه الصورة الشخصية السحرية في صورة سايتك.

نكرر نفس الخطوات، و نقارن، و نجد أن كل شيء على ما يرام.

تعالوا الآن نحذف الملفات هذه التي استخدمناها، عدا صورة سايتك السحرية (آخر صورة)

دعونا نشغل البرنامج ثانية، و نطلب فك تشفيرها (احصل)

انظروا، ها، لقد عادت الصورة الشخصية (و هي سحرية أيضاً)

تعالوا نطلب فك تشفيرها (احصل)

ياه، لقد عاد الملف النصي، دعونا نفتحه و نتأكد من محتواه

حقاً إنه برنامج جميل، أليس كذلك؟

قوموا أنتم أيضاً بتجربة تشفير ملفات لديكم داخل صور من هواتفكم المحمولة، بعد أن تقوموا بتحويلها إلى صور ذات النوع 24-bit Bmp باستخدام برنامج "الرسام" من البرامج الملحقة بنظام Windows.

البرمجة ممتعة أدعوكم إلى بذل قصارى جهدكم في تعلمها و كتابة برامج خاصة بكم

أستودعكم الله و السلام عليكم و رحمة الله و بركاته.

المقطع الثامن (دليل المعلم)

أعزائي المدرسين السلام عليكم و رحمة الله و بركاته

كما تابعتم فإن هذا الدرس يهدف إلى ربط عدد من المواضيع في علوم الحاسب الآلي للوصول إلى بناء تطبيق ذو فائدة في الحياة العملية

إذ يتعرف الطالب على مفهومي التشفير و الإخفاء

و يطّلع على جدول الترميز الأمريكي المعياري لتبادل البيانات ASCII

و على بنية ملف الصورة النقطية و كيفية تخزين الألوان

كما يتعلم الطالب إجراء العمليات على مستوى البت و البايت و التعامل مع الملفات الثنائية Binary Files

ليصل في النهاية إلى استخدام تطبيق حاسوبي بلغة Visual Basic أو غيرها من لغات البرمجة يقوم بتشفير و إخفاء ملف داخل صورة دون أن يبدو عليها تغيير في الشكل أو تغير في الحجم.

يفضل أن يكون الطالب قبل هذا الدرس قد تعرف على:

١- النظام الثنائي Binary System

٢- واحدة التخزين الحاسوبية البايت، و مضاعفاتها: الكيلو و الميجا و الجيجا.

٣- المحرر الست عشري Hexadecimal Editor

٤- مبادئ البرمجة و التعامل مع الملفات الثنائية Binary Files

في نهاية المقطع الثاني من الدرس يمكنكم أعزائي المدرسين مساعدة الطلاب بأن تقترحوا عليهم طرقاً للتشفير مثل تغيير ترتيب الحروف أو أن يستبدلوا بالحرف حرفاً آخر حسب جدول يضعونه هم، أو أن يستخدموا الحرف الذي قبله أو بعده في الأبجدية.

كذلك في الأسئلة الأخرى تتعاونون معهم من واقع خبرتكم في مجال الحاسب الآلي.

أخيراً، هناك العديد من النقاط التي يمكنكم طرحها على الطلاب خصوصاً المتفوقين منهم، أو أولئك الذين أعجبهم موضوع الدرس، مثل:

- هل يمكنك تشفير و إخفاء الملف في أكثر من صورة (توزيعه على أكثر من صورة)
- ما رأيك بكتابة برنامج بإحدى لغات البرمجة، و أن تجعل البرنامج مموهاً لا يبدو عليه أنه يقوم بالإخفاء و التشفير، و إنما يبدو و كأن له هدفاً آخر؟
- كيف يمكنك إدخال تعديلات على البرنامج، و جعله مناسباً لعدة مجموعات من المستخدمين، و بحيث لا تستطيع مجموعة فك تشفير الصور السحرية للمجموعات الأخرى؟ (مثلاً باستخدام خيار للإزاحة أو جداول تشفير مختلفة)
- إتاحة الخيار للمستخدم في أن يختار عدد البتات الدنيا التي يريد استخدامها من الصورة في عملية التشفير (و بالتالي التحكم بمقدار التشويه الضئيل غير الملحوظ الذي يلحق بالصورة)
- هل من طرق لكشف محتوى الصور السحرية دون استخدام نفس البرنامج؟ و كم سيلزم من زمن لتجربة الاحتمالات في حال وجودها؟

أخيراً أرجو أن أكون قد وفقت و القائمين على هذا المشروع إلى تقديم إضافة للمكتبة العلمية العربية، و السلام عليكم و رحمة الله و بركاته.