وزارة التربية والتعليم

10

أمن وحماية المعلومات

كتاب الطالب

الصف العاشر

نحو ثقافة إلكترونية آمنة

هيئة تنظيم الإتصالات TRA
TELECOMMUNICATIONS REGULATORY AUTHORITY

aeCERT Computer Emergency Response Team

جدول المحتويات

الدرس الاول 5
التشفير 5
تعريفات 5
ماهو التشفير؟ 6
إستخدام التشفير 8
الهاش 11
الدرس الثاني 17
كلمات المرور 17
تعريفات 17
سرقة كلمات المرور 18
..... 20
كشف كلمات المرور 21
إحمي نفسك 24
الدرس الثالث 28
تقنية الشبكات اللاسلكية وتأمينها 28
تعريفات 28
تقنية الشبكات اللاسلكية وتأمينها 29
تأمين الشبكات اللاسلكية 32
حماية شبكات واي – فاي اللاسلكية 34

تمهيد

الإنترنت .. عالم واسع .. شبكة عملاقة .. تلف الكرة الارضية شمالا وجنوبا ، شرقا وغربا.. دخول شبكة الإنترنت أشبه بالجولة في مملكة معظم الموجودين فيها سواحٌ ومسافرون من جميع بقاع العالم، والكل يتجول ويتنقل بحرية تامة دون هويات أو تأشيراتٍ للزيارة، حيث لا حدود ولا مراكز جمركية ولا فواصل طبيعية ، والتنقل والتجول فيها ممتعٌ جدا وشيقٌ وهو لا يعدو أكثر من نبضات الكترونية تربط أطراف ومعالم هذه المملكة العامرة..ودخول الشبكة (المملكة) يمثل مغامرة مثيرة للوهلة الأولى، ورغبة شديدة في التعرف على كل شيء والإطلاع عليه ..

هذا الإتساع المترامي لشبكة الإنترنت، صاحبه بروز ظواهر سلبية بين مرتادي الشبكة، وظهور جوانب تستلزم منا أخذ الحيطة والحذر من بعض التهديدات والمخاطر، ولذلك لحماية أنفسنا من التأثيرات المجهولة عبر هذا العالم الإلكتروني الهائل.

قد تكون البداية مجهولة ومشوشة .. ولكن سرعان ما تبدو جميع الأمور طبيعية ومنتظمة، حين إتباع الإرشادات والتعليمات التي ستأخذك لبر الأمان.

هذا المنهج يمثل أحد المصادر الهامة للتوعية بأمن وحماية المعلومات، وهو مادة مساندة للتعريف بكيفية الحد من المخاطر والإستفادة من فرص الإنترنت. كما يهدف إلى تعزيز قدرات وتغيير سلوك الطلاب في التعامل مع الإنترنت. يسعى هذا المنهج في نهاية المطاف الى نشر ثقافة إلكترونية آمنة عبر المؤسسات التربوية والتعليمية بالدولة.

والله ولي التوفيق ،

المقدمة

يحتوي هذا الكتاب على معلومات وتمارين سوف تغطي عدداً من المواضيع التقنية عن أمن وحماية المعلومات. التي سوف ترشدك الدروس إلى مفهوم التشفير، وتناقش قوة كلمات المرور كيفية مهاجمتها ، وتقودك الى أفضل الطرق التي يمكنك إتباعها للمحافظة على سلامة وأمن شبكاتك اللاسلكية. محتوى المعلومات المعروضة هنا لن تكون معقدة تقنياً ، ولكن ستطرح المواضيع بصورة مبسطة وسهلة لتساعدك في فهم التقنيات والإرشادات المختلفة، كي تتمكن من المحافظة على أجهزتك ومعلوماتك سليمة وأمنة في فضاء الإنترنت والعالم الرقمي.

المخرجات

من خلال دروس هذا الكتاب ، سنتطرق إلى النقاط التالية:

- تعريف مصطلح "التشفير".
- عرض بعض الأمثلة في كيفية إستخدام التشفير بشكل إعتيادي في حياتنا اليومية.
- عرض بعض الأمثلة البسيطة عن التشفير لمساعدتك على فهم كيفية عمله.
- إيضاح ما يمكنك عمله للمحافظة على الأجهزة التي تستخدم التشفير لتكون سليمة وآمنة.
- التذكير بأهمية كلمات المرور.
- سرد بعض الأخطاء التي يرتكبها الأفراد والتي تجعل كلمات المرور الخاصة بهم غير آمنة.
- إيضاح طرق المحافظة على كلمة المرور لتكون سرية وآمنة.
- شرح دور الشبكات اللاسلكية الإعتيادية (واي-فاي) في حياتنا اليومية.
- مناقشة أهمية المحافظة على شبكتنا اللاسلكية لتكون آمنة.

الدرس الاول	التشفير

تعريفات

علم التشفير (التعمية) **Cryptography**– هو علم تحويل البيانات الظاهرة لتكون مخفية، وهو مشتق من الكلمات اليونانية (الكتابة المخفية) - "المخفية Kryptos" و الكتابة graphia".

التشفير Encryption– عملية تغيير شكل البيانات لجعلها غير مقروءة، أو لا يمكن تمييزها من قبل أي شخص لا يمتلك مفتاح فك التشفير وهي عملية معاكسة للتشفير.

الهاش Hash- عملية معالجة البيانات وكتابتها على شكل مجموعة من الرموز التي لها طول ثابت وفريد، لتميز تلك البيانات عن غيرها.

الترميز Code- هو تمثيل البيانات بشكل ليس له علاقة واضحة أو مباشرة بصيغة البيانات الأصلية.

عملية التشفير Cipher– الآلية أو الطريقة المستخدمة في التشفير لجعل البيانات غير مقروءة.

المفتاح Key– جزء من المعلومات يستخدم في عملية التشفير وتتغير مخرجات عملية التشفير بتغير نوع وطول المفتاح.

ماهو التشفير؟

هل مر عليك يوم من الأيام أن كان لديك شيئاً تريد الإحتفاظ به سراً عن الآخرين؟ فمثلاً، فوزك بجائزة ما وتود أن تجعلها مفاجأة لحين الإعلان عنها، أو ترتيب لحفل يوم الميلاد لشخص عزيز عليك، أو أمراً تريد أن يعرفه ولي أمرك فقط وليس أي شخص آخر. إن الرغبة في الإحتفاظ بالأشياء سرية موجودة منذ القدم، منذ أن عاش الإنسان على شكل مجموعات فقد إحتاج إلى الإحتفاظ بالأسرار عن الآخرين.

الأسرار التي يرغب الإنسان بالإحتفاظ بها هي أشياء خاصة مثل سر صناعة معينة والتي من الممكن أن تكون شيئاً فريداً وتدر المال الكثير، ومن الأسرار التي يرغب الأفراد أن يتم الاحتفاظ بها هي ما تتضمن أيضاً الخطط العسكرية ضد الأعداء، كما أن الهدف من الإحتفاظ بالسر هو ضمان عدم معرفة أي شخص غير مخول لمعرفة سر ما.

في الأزمان القديمة، كان معظم الناس لا يستطيعون القراءة أو الكتابة لذلك كان من السهولة الإحتفاظ بسرية المعلومات، وذلك من خلال كتابتها فقط. ذلك لأن أي شخص يرغب في معرفة ما هو مكتوب يجب أن يمتلك مهارة خاصة – (القراءة) - للإطلاع على ماهو مكتوب !

وكل شخص يستطيع القراءة، يمكنه معرفة هذه الأسرار.

على كل حال، كلما ازداد عدد متعلمي القراءة، سيصبح من الصعب الإحتفاظ بالأسرار. وحالما تكون الكتابة خارج يد من كتبها تكون هناك دائماً فرصاً كبيرة لشخص ما لقراءتها.

وجد الأفراد بأن أكثر طريقة موثوقة في الإحتفاظ بسرية المعلومات هي تحويلها بطريقة ما بحيث تصبح صعبة الفهم من قبل الغير.

توجد طريقتان أساسيتان لذلك، وهما: **الترميز** و**التشفير**.

الترميز: هو طريقة لتواصل المعلومات بإستخدام كلمات أو مقاطع غير مترابطة، بحيث أن الأشخاص الغرباء لن يكون بوسعهم فهم أو معرفة المقصود الفعلي منها. على سبيل المثال، تستخدم عبارة "نمط الوحش" لتعني أن تكون حاداً ومركزاً وتنجز شيئاً ما بصورة إحترافية. ما لم يعرف الآخرون معنى عبارة "نمط الوحش"، فأنهم لن يفهموا الرسالة.

لقد تم إستخدام الترميز خلال الحروب من قبل الدول في إرسال الرسائل إلى العديد من الأفراد بطريقة سرية بحيث لا يستطيع العدو كشفها. خلال الحرب العالمية الثانية، تم تمرير رسالة إلى المقاومة الفرنسية بإستخدام الترميز، حيث تم قراءة أبيات شعرية من خلال بث محطة الإذاعة المحلية لتخبر المقاومة الفرنسية بعمل شيء ما. لقد كانت الأبيات بمثابة إشارة لهم للبدء بمهاجمة العدو ولم يكن محتوى الشعر ذا أهمية..

تمرين سريع:

فكّر في مثال لكلمة أو عبارة تستخدمها في المدرسة أو مع زملاءك في الفصل بحيث لا يفهمها سوى عدد قليل من الأصدقاء .

التشفير: آلية معينة لتغيير شكل البيانات والمعلومات بتحويلها إلى شكل يصعب معها قراءتها لتعطي المعنى الاصلي لها إلا من قبل الأشخاص الذين يعرفون كيفية فك تلك الشفرة ويعرفون مفتاح تلك الشفرة . مثال بسيط لعملية التشفير هو التشفير التعويضي المستخدم من قبل القائد يوليوس قيصر قبل ألفي سنة. في عملية تشفير يوليوس قيصر، كل حرف في الرسالة يتم تعويضه بحرف آخر من الحروف الأبجدية. سوف لن تستطيع قراءة الرسالة إلا إذا عرفت الآلية التي أستخدمها القائد يوليوس قيصر لإختيار الحرف الجديد في التشفير التعويضي.

إستخدام التشفير

توجد العديد من الأمثلة عن الترميز وطرق التشفير عبر التاريخ. تتضمن بعض الأمثلة المشهورة (عصا سكايتل اليونانية)، و(شفرة يوليوس قيصر التعويضي)، وكتاب أبو عبد الرحمن الخليل بن احمد الفراهيدي عن التشفير والذي كُتب قبل 1300 سنة، والتشفير متعدد الأبجدية لليون باتيستا الاربرتيز. أن طرق التشفير الحديثة متقدمة جداً وتستخدم صيغاً رياضية معقدة طُورت خلال سنوات وتم إختبارها من أجل التغلب على نقاط ضعفها.

سابقاً، كانت عمليات التشفير مقتصرة على الحكومات، وخاصة الأجهزة العسكرية. من أشهر القصص الحديثة حول التشفير كانت في الحرب العالمية الثانية حيث أُستُخدمت آلة (أنيجما) من قبل الجيش الألماني. تقوم هذه الآلة بعمليات تشفير أثبتت – في ذلك الوقت - صعوبة فكها للوصول لتلك المعلومات المشفرة. وقد عمل علماء الرياضيات البريطانيين والبولنديين لسنوات عدة حتى تمكنوا من فك شفرة تلك الآلة، ومنه تم صنع أول جهاز حاسب آلي يستخدم لفك المعلومات المشفرة.

مع تطور الحاسبات الآلية في قدراتها على تخزين وإرسال المعلومات عبر الشبكات كان من الواضح أن هناك حاجة ماسة للمؤسسات والأفراد ليكون لهم الحق في الإحتفاظ ببياناتهم بصورة سرية وآمنة.

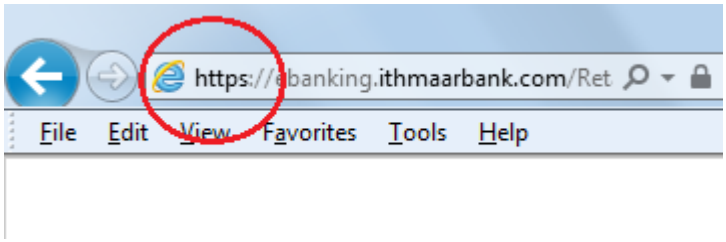
في عام 1991، طوّر (فيل زيمرمان) واحد من أكثر أنظمة التشفير استخداما وهو مايعرف ب "الخصوصية الجيدة جدا- PGP-" بحيث يستطيع كل مستخدم للحاسب الآلي الحصول على صيغة مناسبة لتشفير بياناته.

في عالمنا التقني الجديد، توجد الكثير من البيانات والمعلومات المخزنة على وسائط إلكترونية مختلفة، مثل معلومات حسابك البنكي، وكلمة المرور الخاصة بالبريد الالكتروني، وبعض المراسلات الرسمية والعائلية الخاصة، وحتى التصاميم الجديدة والأفكار التي ترغب بالإحتفاظ بخصوصيتها، هي جميعا أمثلة عن المعلومات التي نرغب بالإحتفاظ بها بصورة سرية.

يُستخدم التشفير في الأمثلة التالية للمحافظة على المعلومات وجعلها سرية.

- يُستخدم التشفير عندما نستخدم بطاقة الدفع الائتمانية في عملية الشراء عبر مواقع الإنترنت.

أنظر إلى سطر العنوان في المتصفح، فإن بدأ **https://** في بداية إسم الموقع الإلكتروني، فإن ذلك يشير إلى أن المعلومات التي يتم إرسالها وإستلامها من الموقع مشفرة.



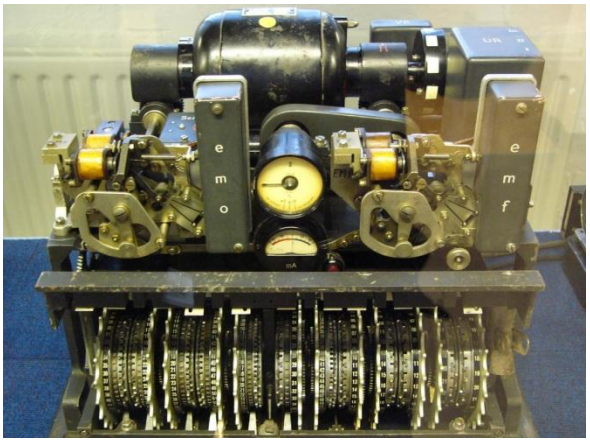
يُستخدم التشفير عند عمليات الدفع بالبطاقات الإئتمانية.

تمتلك العديد من بطاقات الدفع الإئتمانية الحديثة رقاقة حاسب آلي صغيرة تحتوي على بيانات مشفرة تستخدم لتعريف البطاقة. يمكنك رؤية هذه الرقاقة على واجهة بطاقة الدفع الخاصة بك أو بوالديك، حيث يشفر جهاز الدفع أو جهاز قراءة البطاقات بيانات بطاقة الدفع عندما ترسل تلك البيانات إلى البنك.

يتم تخزين كلمة المرور الخاصة بك في الحاسب الآلي، حتى إن تمكن أحدهم من فتح الملفات التي تحتوي على كلمات المرور، فلن يتمكن من قراءتها.

- تستخدم مفاتيح السيارة وأنظمة إنذار المساكن عملية التشفير لحماية كلمات المرور التي تستخدم لفتح الأبواب أو تشغيل جهاز الإنذار.
- تستخدم الإسطوانات المدمجة CD و DVD التشفير لحماية المعلومات المخزونة فيهما من عملية النسخ غير المشروع.
- مكالمات الهواتف النقالة، ومراسلات البلوتوث، والشبكات اللاسلكية تستطيع أيضا إستخدام التشفير إذا تم إعدادها لها الغرض.

آلة لورنز Lorenz ونشأة الحوسبة الحديثة.



تحدثنا عن آلة (أنيجما) التي استُخدمت خلال الحرب العالمية الثانية في تشفير المراسلات السرية. إن الشفرة الأخرى التي تم فكها في تلك الحرب كانت تعتبر اكبر إنتصار لكاسري التشفير. هذه الشفرة كانت تسمى بشفرة (لورنز) والتي استُخدمت في آلة لورنز.

في هذا الواجب المنزلي- ستقوم بالبحث عن تشفير لورنز، وآلة لورنز، وولادة الحاسبات الآلية.

بإستخدام الإنترنت في بحثك، أجب عن الأسئلة التالية:

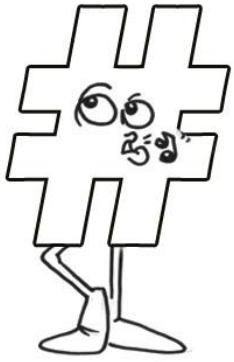
1. ما هي آلة لورنز؟

2. من استخدم تلك الآلة وأي نوع من المعلومات تم إرسالها ؟

3. مانوع عملية التشفير التي تم استخدامها في آلة لورنز؟

4. وجب على العلماء البريطانيين بناء شيء ما لتسريع عملياتهم في فك شفرة لورنز. ماذا كان إسم ذلك الشيء؟ (مساعدة: هي آله ما)

الهاش Hash



يوجد نوع آخر مهم من التشفير ويستخدم بشكل فعّال حالياً، يسمى "دالة الهاش". دالة **الهاش** هي عملية معالجة البيانات وجعلها على شكل مجموعة من الرموز التي لها طول ثابت وفريد.

إذا تم استخدام بيانات مختلفة مدخلة في دالة الهاش، سيكون الناتج عبارة عن مجموعة مختلفة من الرموز، أي أن النتيجة ستكون مختلفة بإختلاف البيانات المدخلة.

تتميز دالة الهاش بخاصية عدم إمكانية إعادة البيانات المدخلة الى صيغتها الأصلية "Unhash"، إذ لاتوجد دالة يمكنها تحويل الرموز الناتجة من عملية الهاش إلى الرموز أو النص الأصلي. الطريقة الوحيدة لمعرفة البيانات الأصلية المستخدمة في تكوين رموز دالة الهاش هي محاولة معالجة أنواع مختلفة من البيانات بنفس دالة الهاش وملاحظة إذا كانت الرموز الناتجة من تلك المحاولات متطابقة.

نتيجة عمليات دالة الهاش لا تعد طريقة صحيحة في إرسال المعلومات السرية أو الرسائل إلى الأفراد، لكنها طريقة مثالية لتخزين كلمات المرور في الحاسب الآلي أو التحقق من عدم إجراء إية تعديلات على ملفات معينة، إذ بتغير أي كلمة أو حرف في الملف، فإن نتيجة دالة الهاش ستكون مختلفة تماماً عن نتيجة دالة الهاش للملف قبل التعديل عليه.

إن الحاسب الآلي لايحتاج إلى معرفة حروف ورموز كلمة المرور المستخدمة، حتى وإن اختُرق الجهاز فلن يتمكن المخترق من معرفة كلمات المرور المخزنة بالجهاز حيث أن نظم التشغيل الحديثة تستخدم دالة هاش لتخزين كلمات المرور بدلاً من كلمات المرور الأصلية.

حين تكتب كلمة المرور للدخول على حاسبك الشخصي، فان النظام يقوم بتمرير الكلمة المدخلة لنفس دالة الهاش التي إستخدمها النظام وقت إنشاء كلمة المرور لأول مرة. يقارن نظام الحاسب الآلي نتيجة دالة الهاش من كلمة المرور المدخلة مع نتيجة دالة الهاش الأصلية التي استخدمت حين أنشئت كلمة المرور لأول مرة، فإذا تطابقتا في النتيجة فأن النظام يتأكد من إدخال كلمة المرور الصحيحة.

لنجرب بعض أنواع التشفير البسيط

من أوائل أمثلة التشفير في التاريخ مايعرف ب "التشفير التعويضي". يأخذ التشفير التعويضي كل حرف من الحروف الأبجدية ويستبدلها بحرف آخر يبعد بمقدار ثابت من الحروف عن الحرف الأصلي في الترتيب الأبجدي.

نعرض هنا مثال عن الشفرة التعويضية التي تزيح الحروف الأولى من الأبجدية ثلاثة مواقع.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	

لإستخدام التشفير التعويضي، يجب أولاً أن تختار كلمة لكي يتم تشفيرها. دعنا نستخدم الكلمة "Hello". خذ الحرف الاول، "H". إبحث عنه في الجدول العلوي واستبدله بالحرف المطابق في الجدول السفلي – والذي هو "K". في التشفير التعويضي فأن الحرف "H" يتم تعويضه بالحرف "K". ثم نعوّض الحرف الثاني في "HELLO" وهو "E". إذا نظرت إلى الحرف "E" في الجدول العلوي فسوف تجد الحرف المطابق في الجدول السفلي وهو "H". أعمل هذا التعويض لكل حروف كلمة "HELLO". ماهي النتيجة؟

"HELLO" تصبح "KHOOR"

لقد إستخدمت آلية بسيطة من التشفير. عملية التشفير المستخدمة هنا صيغة بسيطة من التشفير التعويضي، وهي أن تعوّض الحروف في الكلمة الأصلية بالحروف الأبجدية المزاحة. آلية التشفير المستخدمة في العملية هي عدد الحروف المزاحة وفي إتجاه محدد. يسمى هذا الجزء من عملية التشفير ب "المفتاح Key". يشير المفتاح لمقدار الحروف التي يجب إزاحتها وإتجاه الإزاحة . في مثالنا، كان المفتاح هو" إزاحة بمقدار 3 نحو

اليسار" والذي يعني أننا أزحنا الحروف الأبجدية التعويضية بمقدار ثلاثة حروف إلى اليسار. لفك الشفرة، فأنك تزيح الحروف الأبجدية ثلاثة حروف إلى اليمين.

إن هذا هو شكل بسيط جداً من التشفيرعبر مفتاح بسيطاً جداً. إذا كان شخصاً قادراً على تخمين إزاحة الحروف بثلاثة مواقع، فأنه يستطيع فك تشفير الرسالة بسرعة. بمجرد مطابقة الأبجدية الأصلية والأبجدية المزاحة سيتمكن من معرفة الرسالة الأصلية. إن معظم الخبراء في علم التشفير يستطيعون فتح شفرة التعويض البسيطة بسرعة كبيرة.

لنحاول أن نجعل التشفير أكثر صعوبة. ماذا سيحصل لو قمنا بعمليات تشفير تعويضي ولكن وفق إزاحة متغيرة لكل حرف؟ في المثال السابق كنا دائماً نزيح الحروف بمقدار ثلاثة مواقع نحو اليسار. ماذا يحصل إذا قمنا بإزاحة الحروف بعدد مختلف من المواقع؟

تذكر باننا سمينا العدد المستخدم للدلالة على الإزاحة بالمفتاح، وفي المثال الأول كان المفتاح هو "3". لنجرب مفتاحاً آخر، وليكن مثلاً "359 يسار". تتم مطابقة كل حرف بالحرف الموجود في جدول الإزاحة ووفق الرقم الذي يحدد مقدار الإزاحة.

جرب هذا

هذه المرة سوف تستخدم كلمة قصيرة CAR

المفتاح هو 359

بالنسبة الى الحرف الاول، "C" سوف نزيح حروفنا الابجدية ثلاثة مواقع.

الحروف الأصلية	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
الحروف المعوضة	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

يصبح الحرف "C" هو "F".

بالنسبة الى الحرف الثاني، "A" سوف نزيح حروفنا الابجدية خمسة مواقع.

الحروف الأصلية	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
الحروف المعوضة	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E

الحرف "A" يصبح "F".

بالنسبة للحرف الاول ، "R" سوف نزيح حروفنا الابجدية تسعة مواقع.

الحروف الأصلية	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
الحروف المعوضة	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H

يصبح الحرف "R" هو الحرف "A".

كلمة "CAR" تصبح "FFA".

سيكون هذا أكثر صعوبة عند فك التشفير. إذا كنت لا تعرف مفتاح التشفير وهو 359، فيجب عليك تخمين مقدار الحروف التي يجب إزاحتها لكل حرف في الكلمة المراد تشفيرها، أما إذا كنت تعرف مفتاح التشفير وهو 359 فأنه يصبح من السهل فك تشفير الكلمة.

التشفير الحديث يكون مشابه جداً لهذا المثال حيث يستخدم معادلات رياضية أكثر تعقيداً في عملية التشفير ومفاتيح أكثر طولاً.

يستخدم التشفير ثلاثة أجزاء من المعلومات:

1. **البيانات** – وهي المعلومات المراد الحفاظ على سريتها.
2. **آلية التشفير** – طريقة دمج البيانات والمفتاح لتكوين بيانات مشفرة. يعتمد معظمها على المعادلات الرياضية المعقدة.
3. **المفتاح** –مجموعة من الرموز تستخدم في تحديد كيفية تشفير أو فك شفرة كل جزء من البيانات.

بمعرفة مفتاح التشفير، والطريقة المستخدمة في تشفير البيانات، يكون من السهل فك تشفير المعلومات. في المثال السابق، لفك التشفير يتوجب معرفة المفتاح وطريقة التشفير المستخدمة وهي التشفير التعويضي عبر الإزاحة.

في عمليات التشفير المعقدة تستخدم أساليب معقدة جداً ومفاتيح طويلة جداً ويلزم وقت طويل لفك تلك الشفرات.

إن البيانات المشفرة من قبل آلة أنيجما تم فك شفرتها بواسطة العثور على نقاط ضعف في عملية التشفير تلك، وقد تم تكوين شفرات جديدة في محاولة لجعلها أكثر صعوبة عند محاولة فك شفرتها واكتشاف المفتاح المستخدم. من المهم إستخدام طرق التشفير الحديثة مثل AES، Twofish و IDEA والتي تم إختبارها بصورة جيدة.

تذكر، إذا حصل الأشخاص على مفتاح التشفير فسوف يتمكنون من فك تشفير بياناتك. حين تستخدم التشفير، إحتفظ دائماً بسرية مفتاحك. إن مفتاح التشفير يشبه كلمة المرور ويؤمن الوصول إلى المعلومات المشفرة.

نصائح سريعة للتشفير	

- إستخدم التشفير حين ترغب في حفظ البيانات والمعلومات بصورة سرية وآمنة.
- إحتفظ بمفتاح التشفير بصورة سرية ولا تشرك به أحد.
- إستخدم طرق التشفير المعروفة والحديثة والتي تم إعتمادها من الجهات المتخصصة.

إختبار قصير : التشفير	

1. ماهو علم التشفير؟
2. ماهي عملية التشفير؟
3. ماهو مفتاح التشفير وكيف يستخدم؟
4. ماهي دالة الهاش؟
5. وضح كيف تعمل الشفرة التعويضية؟
6. لماذا من المهم الإحتفاظ بمفتاح التشفير بشكل محمي وسري؟

الدرس الثاني	كلمات المرور

تعريفات

كلمة المرور Password – جزء من المعلومات التي تستخدم لإثبات بانك مخول بالوصول الى شيء ما.

كاشف كلمة المرور Password Cracker– برنامج يحاول إيجاد كلمات المرور للمستخدم من خلال فحص نظام الحاسب الآلي والملفات التي تخزن كلمات مرور المستخدم.

الهاش Hash- عملية معالجة البيانات وجعلها على شكل مجموعة من الرموز التي لها طول ثابت وفريد، لتميز تلك البيانات عن غيرها.

البحث عبر المحاولة والخطأ Brute Force– محاولة البحث عن شيء ما (عادة كلمة مرور) من خلال تكرار المحاولات لحين الحصول على النتيجة المطلوبة

التخمين عبر القاموس Dictionary Guessing –محاولة تخمين كلمة المرور أو مقطع من كلمة المرور باستخدام قائمة من الكلمات المبنية مسبقا.

جداول قوس قزح Rainbow Tables– قائمة من نتائج الهاشات مبنية مسبقاً لكلمات محددة أو مجموعات من الكلمات والحروف والرموز الخاصة. تستخدم عادة في توقع كلمات المرور من خلال مقارنة نتيجة الهاش لملفات كلمات المرور المخزنة في أجهزة الحاسب الآلي مع القائمة بجدول قوس قزح.

سرقة كلمات المرور

كلمات المرور هي جزء مهم من أمن المعلومات لأنها تُستخدم لضمان الوصول للمعلومات من قبل الأشخاص المخولين فقط، وتأمين المعلومات السرية. حين تستخدم كلمة المرور لفتح برنامج البريد الإلكتروني، فإنك تحاول إثبات بانك مخوّل للوصول إلى رسائل ذلك البريد. إذا حصل أشخاص آخرون على كلمة المرور الخاصة بك، فسيتمكنون أيضاً على قراءة بريدك الالكتروني.

نحن نستخدم كلمات المرور لحماية الوصول إلى أشياء أخرى غير البريد الإلكتروني. نستخدم كلمات المرور للوصول لمواقع التسوق في الإنترنت ومواقع الشبكات الإجتماعية، والحاسبات الخاصة بنا، أو الحسابات البنكية، وحتى الهواتف. من دون كلمات المرور سيتمكن الآخرون أيضاً من الوصول إلى هذه الأشياء وإستخدامها بنفس الطريقة التي نتعامل بها. وهذا مالا يرغب فيه أي شخص .

أسئلة:

1. **كم عدد الأجهزة المختلفة ومواقع الإنترنت التي تستخدمها والتي تسألك عن كلمات المرور؟**

2. **كم عدد كلمات المرور المختلفة التي تستخدمها بين جميع هذه الأجهزة ومواقع الإنترنت؟**

قد يرغب شخص في قراءة بريدك الإلكتروني، أو يحاول إنتحال شخصيتك في موقع التواصل الاجتماعي، أو الوصول إلى هاتفك النقال، بل قد يحاول البعض الوصول إلى حسابك البنكي! فإنه يحتاج لمعرفة كلمة المرور الخاصة بك، لذلك فإن كلمات المرور هي جزء مهم من المعلومات ويجب المحافظة على سريتها.

يمكن زيادة حماية كلمة المرور من خلال فهم حيّل وأساليب القرصنة المستخدمة للحصول على كلمات المرور. أسهل طريقة يستطيع فيها المهاجم الحصول على كلمة المرور الخاصة بك هي ببساطة سؤالك عنها!

لن يكون ذلك بإسلوب مباشر حتماً، ولكن عبر طرق إحتيالية. فقد يتصل بك أو يُرسل لك بريداً الكترونياً يطلب فيه إرسال كلمة المرور الخاصة بك منتحلاً صفة موظف خدمة العملاء بالبنك، ونظراً لوجود عمليات مصرفية مشبوهة بحسابك فإن البنك يود التحقق منها لحمايتك! أو يتم توجيهك إلى موقع بشبكة الإنترنت (موقع وهمي طبعاً) ويُطلب منك إدخال معلومات لإعادة تنشيط حسابك للخدمات البنكية الإلكترونية، أو خدمات شبكات التواصل الإجتماعي. تكمن الحيلة في خداع الضحية من خلال تلك الرسائل البريدية التي تبدو وكأنها مرسلة حقاً من البنك. في ظاهر الأمر ستبدو كأنها رسائل رسمية من حيث الشكل والمحتوى وتطلب إرسال معلومات كالرقم الشخصي، وكلمة المرور، ورقم الحساب، والإسم والعنوان، سواء من خلال الرد على الرسالة أو من خلال الضغط على رابط في سيحيلك لصفحة تشبه تماماً صفحة الموقع الرسمي للبنك. لاتستجيب أبداً لأية طلبات من هذا القبيل وقم بالإتصال بالبنك حالاً وإخبارهم بالحادثة.

يحاول بعض القراصنة الحصول على كلمة المرور بصورة مباشرة من موقع الإنترنت أو الحاسب الآلي من خلال مايعرف ب**"كاشف كلمة المرور"**. تقوم هذه الأداة بالبحث عن الملفات التي تخزن كلمات المرور سواء بمواقع الإنترنت أو أجهزة الحاسب الآلي ثم القيام بعمليات سريعة باستخدام قاموس من الكلمات يحتوي أنماط معينة من الرموز مثل "abcd" أو "1234" ، أو كلمات اعتيادية تستخدم غالباً في كلمات المرور مثل كلمة "password".

تستخدم بعض تلك الأدوات ما يعرف بالقاموس المرافق بحيث يتم إختبار كل الكلمات الأكثر شيوعاً والواردة بالقاموس، وعليه فإن إستخدام الكلمات البسيطة أو المعروفة أو المباشرة ككلمة للمرور، سيجعل كشفها في غاية السهولة والسرعة.

أكثر كلمات المرور شيوعاً	Case study

في عام 2011، أجرى استشاري أمن المعلومات يدعى مارك بيرنيت دراسة عن كلمات المرور التي جمعها من قوائم لكلمات المرور المسروقة وتم نشرها في شبكة الإنترنت.وخلص من خلال الدراسة لأكثر كلمات المرور شيوعاً وإستخداماً من قبل المستخدمين.

لقد وجد أن 91% من جميع كلمات المرور المستخدمة حول العالم جاءت ضمن أعلى 1000 كلمة مرور في قائمته. أي أنه يمكن تخمين كلمة المرور لكثير من الناس من خلال الإطلاع على القائمة التي نشرتها الدراسة! ولكن لايعني بالضرورة إمكانية الدخول على حساباتهم.

فيما يلي أكثر6 كلمات للمرور شيوعاً :

1. password
2. 123456
3. 1234578
4. 1234
5. Qwerty
6. 12345

أسئلة:

1. لماذا تعتقد بأن الناس يستخدمون كلمات المرور تلك؟
2. ماهي كلمة المرور التي يجربها القراصنة أولاً للوصول إلى البريد الإلكتروني أو الحساب البنكي للأشخاص؟

كشف كلمات المرور

هل يمكن الدخول على العديد من حسابات مواقع البريد الإلكتروني ومواقع شبكات التواصل الإلكتروني عبر تخمين كلمة السر بإستخدام قائمة دراسة السيد **مارك بيرنيت**، أي 91% من حسابات الآخرين؟ لحسن الحظ، تمتلك معظم المواقع الإلكترونية المشهورة آلية للحماية ضد الأشخاص الذين يحاولون تخمين كلمات المرور للآخرين لعدة مرات، وتعرف ب "تعطيل الدخول على الحساب". فإذا أخطأت في كتابة كلمة المرور الصحيحة عدد محدد من المرات فأنه سوف يتم تعطيل حسابك، وسيتم التحقق من هويتك بطرق أخرى، وقد يُطلب منك إعادة تهيئة كلمة المرور الخاصة بك. إن هذا الإجراء سوف يحميك من محاولات تخمين كلمة المرور.

طريقة أخرى لمحاولة الكشف عن كلمات المرور يكمن في محاولة سرقة الملفات التي تخزن كلمات المرور بالمواقع الإلكترونية أو أجهزة الحاسب الآلي من خلال طرق وأدوات تقنية متخصصة. تلك الطرق والأدوات تتطلب قدراً من المعرفة والخبرة، والبحث عن الثغرات الأمنية الموجودة في أنظمة الحاسب الآلي والشبكات الإلكترونية.

إن الكثير من المواقع الإلكترونية تستخدم تقنيات التشفير لاسيما بالنسبة لبيانات المشتركين وكلمات المرور. تخزن تلك المواقع تلك المعلومات المختلفة في ملفات مشفرة حتى لاتستغل من قبل قراصنة الشبكات الإلكترونية عند تعرض الموقع للإختراق، كما أنها تستخدم دالة الهاش لتخزين كلمات المرور، وعليه فإن الملف الذي يحتوي على كلمات المرور سيكون قائمة من الرموز غير المفهومة ولايمكن بأي حال إعادة البيانات المخزنة لصيغتها الأصلية إذا ماتمت سرقتها.

سيحاول القراصنة تخمين كلمات المرور، ولكن العملية ستكون صعبة وطويلة لو تمت بصورة يدوية عبر المحاولات المتكررة، وعليه يستخدم القراصنة أدوات وبرامج تقنية تسمى "كاشفات كلمات المرور" التي ستحاول الكشف بطريقة أسرع. هناك طرق عدة لهذه العملية ومن ضمنها:

البحث عبر المحاولة والخطأ

تقوم هذه الطريقة عبر إجراء كافة الإحتمالات الممكنة لتشكيل كلمة مرور تتكون من حروف وأرقام ورموز خاصة على أمل أن يكون ضمن الإحتمالات المجربة إحدى كلمات المرور المطابقة لكلمة المرور المخزنة بالملف، أو تطابق نتيجة دالة الهاش لإحدى المحاولات بنتيجة دالة الهاش المخزنة بالملف.

قد تستغرق هذه العملية وقتاً طويلاً لأنها تعتمد مبدأ المحاولة والخطأ لحين الحصول على المحاولة الصحيحة. كلما كانت كلمة المرور طويلة واحتوت على المزيج من الحروف والأرقام والرموز الخاصة، كلما كانت أصعب في الكشف وتحتاج الوقت الطويل حتى يمكن الوصول للنتيجة الصحيحة بعد المحاولات الكثيرة. للتذكير، فإن العملية تتم بواسطة أدوات وبرامج في الحاسب الآلي الذي يمكنه العمل المتواصل لساعات وأيام بل وشهور دون ملل أو كلل.

التخمين عبر القاموس

طريقة التخمين عبر القاموس تعتمد على محاولة تخمين كلمة المرور من خلال مقارنتها بكلمات القاموس. إن العديد من الناس يستخدم كلمات المرور التي تتكون من كلمات مباشرة مثل إسم المدينة، أو إسم الفريق الرياضي المفضل، أو أسماء الأشخاص أو مجرد تسلسل لأرقام. تقوم الأداة المستخدمة لكشف كلمات المرور عبر هذه الطريقة بمقارنة كلمات المرور المخزنة بالملف المخترق بكلمات المرور الأكثر شيوعاً وتلك الواردة بالقاموس المرافق لهذه الأداة على أمل أن تكون إحدى كلمات القاموس مطابقة لكلمة السر المخزنة في الملف المخترق.

جداول قوس قزح

في كثير من الأحيان تعتمد المواقع الإلكترونية على تخزين قوائم نتائج دالة الهاش للدلالة على كلمات المرور ولايتم تخزين كلمة المرور نفسها. يزيد هذا الأسلوب من الجوانب الأمنية بحيث لايمكن معرفة كلمات المرور حتى وإن تم اختراق ملف تخزين كلمات المرور إذ لايمكن إعادة البيانات المدخلة إلى صيغتها الأصلية.

جداول قوس قزح هي تلك الجداول التي تحتوي على قوائم نتائج دالة الهاش لعدد كبير من كلمات المرور والتي تم الحصول عليها من خلال إختراق المواقع الإلكترونية.

تعمل أداة كشف كلمة مرور عبر جداول قوس قزح بصورة جيدة جداً حين تُعرف دالة الهاش المستخدمة، ولكن تكون صعبة جداً حين تستخدم تلك المواقع دالة هاش خاصة بحيث تكون مصممة وفق خوارزميات ومعادلات رياضية معقدة لايمكن معرفتها، وبالتالي يكون ملف تخزين قوائم مخرجات دالة الهاش كلغز رياضي يصعب فهمه.

إحمي نفسك

إن حماية كلمة المرور قد تكون أسهل مما تعتقد! القاعدة الأساسية تقول: كلمة المرور يجب أن تكون سهلة التذكر بالنسبة لك.. صعبة التخمين بالنسبة للغير. إليك بعض المفاهيم الهامة بهذا الشأن:

1) إجعل كلمة المرور طويلة: تستغرق أجهزة الحاسب الآلي وقتاً أطول لقرصنة كلمة المرور حين تكون تلك الكلمة أطول. يبحث عادة قراصنة الشبكات الإلكترونية عن الطرق الأسرع لتحقيق أهدافهم، مما يجعلهم يفضلون إستهداف كلمات المرور القصيرة والمباشرة.

2) إجعل المرور معقدة: إن إستخدام مزيج من الحروف الصغيرة والكبيرة والأرقام والرموز الخاصة، يجعل كلمة السر أكثر تعقيداً من حيث إمكانية تخمينها أو كشفها بواسطة الأدوات التقنية حيث أنها تستغرق وقتاً طويلاً سواء من خلال طرق المحاولة والخطأ أو عبر قواميس التخمين.

3) إستخدم كلمات مرور مختلفة للحسابات الإلكترونية المختلفة: بإستخدامك كلمة مرور موحدة لكل حساباتك في المواقع الإلكترونية المختلفة، فإن ذلك يعني إختراقها جميعاً عند كشف تلك الكلمة. تستخدم بعض المواقع عنوان بريدك الإلكتروني للدلالة على هوية المستخدم وعليه مثلاً، لو تم إختراق كلمة المرور الخاصة ببريدك الإلكتروني، فإن القراصنة سيتمكنون من معرفة كلمة المرورالخاصة بك لكل المواقع الأخرى التي تستخدم بريدك الإلكتروني للدلالة على هوية المستخدم أو إسمه.

4) غيّر كلمة مرورك دائماً: قد لا تعرف بأن كلمة المرور الخاصة بك قد تمت سرقتها، لكن إذا غيرتها بصورة منتظمة، فإن ذلك سيقلص من فرص إمكانية إختراقها بواسطة الأدوات التقنية المختلفة.
حين تغيّر كلمة المرور بصورة دورية (90 يوماً مثلاً) فلن يستفيد القراصنة من الملف المخترق الذي يحتوي على كلمات المرور حتى وإن تمكنوا من كشف كلمة المرور الخاصة بك أثناء محاولاتهم لاسيما أن العملية قد تستغرق وقتاً طويلاً. لن يفرح القراصنة كثيراً، إذ ستكون كلمة المرور قد غُيرت في الوقت الذي تم كشفها في ملف كلمات المرور المخترق.

5) إحمِ كلمة المرور: لاتكتبها في الورق، ولا تحتفظ بها في الملفات الإلكترونية غير المتخصصة بهذا الشأن، كأن تُكتب في ملف مايكروسوفت وورد، أو ملف في برنامج مايكروسوفت إكسل..الخ.
توجد العديد من برامج تخزين كلمات المرور المتخصصة والتي تحتفظ بكلمات المرور بصورة آمنة في حاسبك الآلي، أو هاتفك النقال. إبحث عن أحد تلك البرامج الموصي بها جيدًا، وتأكد بأنها تستخدم تشفير متقدم في تخزين كلمات المرور.

نصائح سريعة لكلمات المرور	

1. إستخدم كلمات المرور الطويلة بحيث تتضمن خليطاً من الحروف والأرقام والرموزوالحروف والارقام .
2. لا تستخدم نفس كلمة المرور لحساباتك بالمواقع الإلكترونية المختلفة.
3. إحتفظ بكلمة المرور الخاصة بك بصورة آمنة ولا تبيح بها لأي شخص.
4. غيّر كلمة المرور بصورة دورية ومنتظمة.

إختبار قصير ـ كلمات المرور	

1. لماذا تكون أجهزة الحاسب الآلي أفضل من الإنسان في هجوم "البحث بالمحاولة والخطأ"؟

2. لماذا يكون من الأفضل أن تكون كلمة المرور مكونة من 9 رموز بدلاً من 5 رموز؟

3. هل أسماء الأشخاص في كلمات المرور آمنة إذا تم إستخدام "التخمين بالقاموس"؟

4. لماذا يجب عليك إستخدام كلمات مرور مختلفة للمواقع المختلفة؟

5. كيف تعمل "جداول قوس قزح"؟

الدرس الثالث	تقنية الشبكات اللاسلكية وتأمينها

تعريفات

واي- فاي Wi-Fi – تكنولوجيا لاسلكية تسمح بالإتصال وتبادل البيانات بين الأجهزة الإلكترونية.

ل اللاسلكي النقال Mobile Wireless - تكنولوجيا لاسلكية تسمح بالتواصل الصوتي وعبر تناقلالبيانات بين الأجهزة النقالة اللاسلكية. تستخدم عادة مع الهواتف النقالة وأجهزة الحاسب الآلي والأجهزة الإلكترونية الأخرى. توجد العديد من التقنيات الخاصة مثل LTE ,GSM, EDGE, 3G, 4G, وتعد جميعاً جزءً من هذا النوع من الشبكات اللاسلكية.

WPA2 – مجموعة من المعايير التي توفر الأمن لشبكات واي - فاي والتي تتضمن التحقق من الإرتباط بشبكة واي-فاي وكذلك تشفير البيانات المرسلة خلال شبكة واي – فاي.

WPA2-PSK – طريقة تحقق في شبكة واي – فاي عبر مفتاح مفرد مشترك- محدد مسبقاً لجميع الأجهزة التي ترتبط بشبكة واي – فاي. تسمى في بعض الأحيان WPA2 – الشخصية.

WPA2 – يعد هذا المشروع كطريقة للتحقق من الإرتباط بشبكة واي –فاي عبر كلمات مرور، أو الشهادات الرقمية، أو طرق فريدة أخرى لكل مستخدم مرتبط في شبكة واي – فاي بصورة منفردة. تتطلب هذه الطريقة مزودات لتوفِر التحقق من المستخدمين.

تقنية الشبكات اللاسلكية وتأمينها

فكّر في جميع الأماكن التي ترغب بالعمل فيها من خلال جهاز الحاسب الآلي الخاص بك :

- في المقهى
- في الفندق
- في المطار
- عند الأصدقاء
- في المتنزهات والحدائق
- في شرفة المنزل أو أي غرفة فيه

سابقاً، كانت الطريقة الأكثر إستخداماً وتوافراً هي ربط جهاز الحاسب الآلي بالشبكة عبر الأسلاك. سوف تحتاج إلى سلك طويل جداً حتى يمكنك العمل في المقهى! أو حتى بين غرف المنزل المختلفة إذا لم تتوفر فيها مقابس الربط السلكية. أما اليوم، فالشبكات اللاسلكية في كل مكان من حولنا. وباتت كل الأجهزة التي نستخدمها تتوفر فيها خدمة الإتصال اللاسلكي، كالأجهزة المحمولة، وهواتفنا النقالة، والطابعات، وحتى أجهزة التلفاز! كما أصبحت المجمعات والأماكن العامة توفر وصولاً سهلاً لمستخدمي شبكة الإنترنت من خلال نقاط الإتصال اللاسلكي المنتشرة.

أكثر أنواع الشبكات اللاسلكية شهرة يسمى واي – فاي wi-fi. لقد تم إختيار الإسم ليعني الإتصال اللاسلكي عالي الجودة "فيديليتي اللاسلكيWireless Fidelity" إشتقاقاً من مصطلح عالم تسجيل الموسيقى عالي الجودة "Hi-fi". تمتلك معظم الحاسبات الحديثة خيار لاسلكي واي – فاي ضمن الخصائص الأساسية فيها، وتشير عادة على أنها 802.11a/b/g/n يشير 802.11 إلى مواصفات شبكة "واي – فاي" اللاسلكية، وتشير a, b, g, n إلى السرعات والترددات المختلفة. تستطيع شبكة "واي – فاي" المثالية الإتصال في نطاق دائري لمسافة 100 متر من نقطة توزيع الإشارات اللاسلكية.

تمتلك بعض الهواتف النقالة أيضاً قدرات "واي – فاي"، لكنها تمتاز بخصائص الشبكات اللاسلكية للمسافات البعيدة. يشار لها غالباً بإستخدام مصطلحات مثل UMTS, EDGE, GSM, CDMA, HSPA, 2G, 3G, 4G, WiMAX واخيرا LTE. إن مدى هذه الشبكات اللاسلكية يمتدعادة لعدة كيلومترات، ولكنه أبطأ من شبكات الواي فاي بصورة عامة.

اللاسلكي في البيت

توجد العديد من الأجهزة في البيت والتي تستخدم الشبكات اللاسلكية. حاسبك الآلي هو فقط أحد تلك الأجهزة. أنظر حولك بالمنزل. كم جهاز يمكنك تحديده والذي يستخدم شبكات "واي – فاي" اللاسلكية.

1. أدرج جميع أجهزة "واي – فاي" اللاسلكية التي يمكنك إيجادها في منزلك.
2. أكتب ماهو الإرتباط اللاسلكي المستخدم لكل جهاز منها.
3. إبحث في شبكة الإنترنت وانظر إذا كان بإمكانك إيجاد ستة أجهزة أخرى تعمل بواسطة إرتباط "واي – فاي" اللاسلكي، ويمكن إستخدامها بالمنزل.

التقنية اللاسلكية

إن وجود الشبكات اللاسلكية في مكاتب الشركة تعني بأن المستخدمين يمكنهم العمل في اي مكان، حيث لا يوجد أي أسلاك للشبكة، ويمكن بسهولة إنتقال الموظفين من مكتب إلى آخر، حيث يمكن نقل الأجهزة داخل المكاتب وإعادة تهيئتها وتركيبها بأقل الجهود والتكلفة.

بعض دول العالم بدأت في إنشاء مايعرف ب "البيوت الذكية" كما في دولة الإمارات العربية المتحدة حيث توجد مشاريع عدة لإنشاء هذه البيوت. ترتبط البيوت الذكية بمنظومة إلكترونية متقدمة تشتمل على تقنيات الإتصال اللاسلكي، بحيث يتم التحكم بالعديد من الأدوات والأجهزة من خلال أجهزة الحاسب الآلي اللوحية والهواتف الذكيةبواسطة تقنيات الإتصال اللاسلكي، يمكن مثلاً من خلال أجهزة الهاتف الذكية تفعيل أو تعطيل نظام الإنذار بالمنزل، ومشاهدة كاميرا المراقبة المثبتة بالمنزل بينما أنت في مقر عملك، كما يمكن أن تتحكم في حفظ أو رفع درجة حرارة المكيف وضبط درجة حرارة حوض السباحة ليكون جاهزاً بينما أنت في طريق العودة.

إستخدمت الشركات مثل بانوسونيك هذه التقنية أيضاً لجعل أماكن عمل موظفيها أفضل، فقد إستخدموا أجهزة لقياس حرارة المكتب بواسطة حواسيبهم المكتبية والتحكم بدرجة تكييف المكتب على ضوء حرارة المكان الذي يعمل فيه.

كما أن مطار تورنتو الدولي بكندا يستخدم التقنيات الذكية بنظام معلومات رحلات الطيران الواصلة والمغادرة وربطها مع الحرارة والاضاءة ونظام التبريد في كل بوابة من أجل السيطرة على إستهلاك الطاقة حين لا تستخدم تلك البوابات.**أسئلة:**

1. صف فوائد المبانى الذكية الحديثة.
2. ماهي المخاطر الأمنية للمباني الذكية؟

تأمين الشبكات اللاسلكية

تستخدم جميع الشبكات اللاسلكية الإشارات الراديوية في إرسال البيانات. ترسل هذه الإشارات الراديوية عبر الهواء. حين تُرسل البيانات من خلال الشبكات السلكية، فإنه يمكنك التقاط تلك البيانات إذا إستطعت الإرتباط سلكياً بتلك الشبكة. مع الشبكات اللاسلكية، يمكن للإشارات الراديوية الذهاب إلى أي مكان، وقد يتمكن شخص ما من إلتقاط تلك البيانات المرسلة وكشفها مالم تكن مؤمنة بشكل صحيح.

تصور إصغائك إلى المذياع – يمكنك سماع المحطات الإذاعية بوضوح – كل شيء يذاع بالإمكان التقاطه والإستماع اليه، مثل نشرات الأخبار، وبرامج النقاش المباشرة، وسماع الموسيقى وغيرها. تعمل الشبكات اللاسلكية بنفس الطريقة، بحيث يستطيع أي حاسب مجهز بتقنية الربط اللاسلكي من التقاط إشارات الشبكات اللاسلكية، وعليه تم وضع معايير تقنية عالمية من شأنها تأمين الدخول على الشبكات اللاسلكية وحمايتها من الإختراق.

فكّر في البيانات بالشبكات اللاسلكية

تصور مراقبة الإشارات الراديوية من الشبكة اللاسلكية متدفقة في وسط الهواء.

1. إذا كنت تريد إرسال ملف خاص لوالديك، أو إرسال رسالة إلكترونية لصديق مقرب. قد لا ترغب أن يطلع أي شخص آخر على ذلك البريد الالكتروني؟
2. عندما ترتبط بشبكة واي – فاي، فأنت ترتبط عبر الهواء! حين تذهب إلى المقهى، أو مكان عام تتوافر فيه خدمة واي – فاي، فإنه يمكنك إختيار شبكة واي – فاي للإرتباط معها لتتصل بشبكة الإنترنت. من حيث المبدأ، لا يوجد ما يعيق عملية الإرتباط تلك. تصور إذا كانت شبكة الواي – فاي الخاصة بك في المنزل تعمل بنفس الطريقة. ماذا يستطيع جيرانك عمله؟
3. ماهو الضرر الذي قد يحدث إذا دخل أناس آخرون لشبكة الإنترنت عبرشبكة واي فاي الخاصة بمنزلك ؟
4. ما هي الحلول لحماية شبكتك من أي مستخدم غريب من شأنه أن يستهلك موارد الشبكة ويجعلها بطيئة أو يستخدمها لمهاجمة جهازك ؟
5. ماذا تعلمت لمساعدتك في جعل البيانات المرسلة خلال إشارات اللاسلكي آمنة وسليمة.

حماية شبكات واي – فاي اللاسلكية

ترسل شبكات "واي– فاي" إشاراتها خلال الهواء، ويمكن لأي جهاز يحتوي على التقنيات اللاسلكية إلتقاط تلك الإشارات، وقد يتمكن من التجسس على البيانات المرسلة بواسطتها.

لحسن الحظ، هناك العديد من التقنيات الأمنية التي تحمي شبكة واي – فاي والبيانات المرسلة بواسطتها. من المهم أن تعرف ماهي تلك التقنيات وبعض أنواعها.

تمتلك شبكات واي – فاي تقنية تسمى WPA2 والتي تعني "وصول واي – فاي المحمي الجيل 2" . تعمل WPA2 بأمرين:

اولاً: من خلال طلب كلمة المرور أو مايعرف بالمفتاح المشترك لأي شخص يحاول الإرتباط بشبكة واي – فاي. يجب إدخال كلمة المرور تلك أو المفتاح المشترك المعرّف مسبقاً قبل أن ترتبط مع شبكة واي – فاي. إذا لم يكن لديك مفتاح مشترك معرّف مسبقاً، فلا يمكنك إستخدام الشبكة. إن ذلك يساعدك في صد الغرباء من إستخدام شبكة الواي – فاي التابعة لك، وكذلك إبعاد جيرانك من إستخدام شبكة الواي فاي لتنزيل الأفلام وجعل الإنترنت بطيئاً عندك. من جانب آخر، فإن معظم الشركات تستخدم كلمات المرور وتعرف ب – WPA حيث تستخدم نفس كلمة المرور للدخول على الجهاز والإتصال بالشبكة معاً. تتطلب هذه الطريقة تقنيات أخرى تتوفر عادة في قطاع المؤسسات والأعمال.

ثانيا، يؤمن WPA2 عملية تشفير لكافة البيانات المرسلة من جهازك عبر شبكة واي – فاي. بمعنى أن المعلومات، والصوّر، أو البريد الإلكتروني الذي ترسله عبر شبكة الواي – فاي سيكون محمياً من الأشخاص المتطفلين الذين يراقبون الموجات اللاسلكية.

ولكن ماذا عن رغبتك بإستخدام الشبكات اللاسلكية حين تكون مسافراً أو في المقهى؟

كن حذراً بمعرفة ماهي شبكات الواي – فاي التي ترتبط بها، فليست كل شبكات واي – فاي آمنة وتحمي معلوماتك. معظمها تسمح لأي شخص بالإرتباط بالشبكة (إنها واي – فاي عامة، أليس كذلك؟) والعديد منها لا تقوم بتشفير المعلومات التي ترسلها خلال شبكة واي – فاي. إذا إرتبطت بشبكة واي – فاي عامة، فينبغي الإفتراض بأنها غير آمنة. إفترض بأن أي شخص يمكنه رؤية ما ترسله خلال الشبكة. لا تستخدمها في الدخول على مواقع البنوك، أو إجراء المعاملات المالية، أو إرسال المعلومات السرية والخاصة، إذ يمكن للقراصنة كشف تلك المراسلات طالما كانت في شبكة واي – فاي عامة.

يقوم بعض القراصنة بتأسيس شبكات واي – فاي مزيفة ونقاط وصول لخداعك بالإرتباط بشبكة الواي – فاي مجانية تابعة لهم! ثم يقوموا بتصميم مواقع وهمية شبيهة جداً بتلك الحقيقية لتدخل عليها مثل تأسيس موقع وهمي لبريد جي ميل المشهور، أو موقع بريد ياهو أو موقع لبنك ما يقدم خدمات مصرفية إلكترونية. تحقق دائماً من إسم نقطة وصول الواي – فاي قبل الإرتباط بها. تأكد من أنها نقطة وصول بشبكة واي – فاي آمنة وموثوقة قبل عملية الإرتباط، وإذا كنت لا تعرف نقطة الوصول تلك فلا ترتبط بها.

نصائح سريعة للواي – فاي	

1. إضبط الشبكات اللاسلكية التابعة لك لإستخدام WPA2
2. اختار كلمة مرور آمنة للمفتاح المشترك المعرّف مسبقاً ل WPA2-PSK التابعة لك
3. لا تقم بأعمال حساسة كالمعاملات البنكية وإرسال الرسائل السرية حين تستخدم شبكات واي – فاي عامة.

الشبكات اللاسلكية	

1. ماذا تعني واي – فاي؟
2. ماهي التقنية التي تجعل البيانات المرسلة خلال شبكات واي – فاي بصورة آمنة؟
3. كيف ترسل الشبكات اللاسلكية البيانات؟
4. ماهي فوائد الشبكات اللاسلكية؟
5. ماهي الأجهزة التي تستخدم الشبكات اللاسلكية؟

التقييم	

1. أكتب تعريفاً للتشفير بأسلوبك.
2. متي يستخدم التشفير؟ إختر جميع الإجابات الصحيحة.
   أ. عندما يقوم الحاسوب بحفظ كلمة المرور الخاصة بك
   ب. عند إستخدام بطاقة الإئتمان أو بطاقة الشراء في المحلات أو أجهزة سحب النقود
   ج. عندما تزور موقع إلكتروني يستخدم HTTP
3. ما هي الشفرة؟ أكتب التعريف بأسلوبك.
4. لماذا يجب حماية المفاتيح المستخدمة في التشفير؟
   أ. يمكن بسهولة فكها وإتلافها
   ب. إذا حصل أحد على مفتاح التشفير فإنه سيتمكن من فك الشفرة
   ج. هي طريقة تستخدم للتشفير
   د. لا يهم حماية مفاتيح التشفير
5. ما هي طرق حماية كلمة المرور؟ إختر جميع الإجابات الصحيحة.
   أ. إجعل كلمة المرور صعبة التذكر
   ب. الحفاظ على سرية كلمات المرور
   ج. لا تستخدم كلمات مرور سهلة التخمين
6. استناداً للدراسة المذكورة في هذا الكتاب، ما هي كلمات المرور الأكثر شيوعاً؟ اختر أفضل إجابة.
   أ. Ferrari
   ب. password
   ج. a1b2c3d4e5
   د. Tim2012bP+iT
7. أي من التالي يمكن إستخدامه لكشف كلمة المرور؟ إختر جميع الإجابات الصحيحة.

أ. القوة الغاشمةBrute Force
ب. قاموس التخمينDictionary guessing
ج. جداول قوس قزحRainbow Tables
د. التشفير

8. عند إختيار كلمة مرور، ماذا يمكنك أن تفعل لتكون سهلة التذكر بالنسبة لك وصعبة التخمين للغير؟ إختر جميع الإجابات الصحيحة.

أ. إختيار أول حرف من كل كلمة في جملة معينة
ب. إختيار بعض الكلمات التي ليس لها معنى وتكوين صورة لتذكرك بها
ج. إختيار أرقام وحروف ورموز عشوائية لتكوين كلمة طولها 30 حرف

9. أي من الجُمل التالية صحيح بخصوص الإتصال اللاسلكيWi-Fi ؟ إختر جميع الإجابات الصحيحة.

أ. شبكات الإتصال اللاسلكي تستخدم إشارات الراديو التي يمكن تتبعها بسهولة
ب. يمكن الإرتباط بشبكات الإتصال اللاسلكي حتى وإن لم تكن آمنة
ج. يمكن أن تتعثر في أسلاك شبكة الإتصال اللاسلكي
د. يجب أن تحمل معك سلك لترتبط بشبكة الإتصال اللاسلكي

10. أي من الطرق التالية جيدة لحماية نفسك عند إستخدام شبكة الإتصال اللاسلكي؟. إختر جميع الإجابات الصحيحة.

أ. قم بإعداد شبكة الإتصال اللاسلكي في المنزل عبر تقنية WPA2
ب. قم بإعداد شبكة الإتصال اللاسلكي بالمنزل ليتحتم إستخدام كلمة مرور للإرتباط بها
ج. إرتبط دائماً بشبكات الإتصال اللاسلكي في الأماكن العامة
د. إفترض دائماً بأن الإرتباط بشبكات الإتصال اللاسلكي العامة غير آمن
ه. لاتستخدم شبكات الإتصال اللاسلكي العامة لإجراء العمليات البنكية أو إرسال المعلومات الخاصة والسرية.