الوحدة الرابعة

أمن المعلومات والتشفير

العلامة الكاملة في علوم الحاسوب

إعداد المعلم: سامر جديع "٢٠١٩

الوحدة الرابعة : أمن المعلومات

(١) وضّح المقصود بمفهوم أمن المعلومات؟

العلم الذي يعمل على حماية المعلومات والمعدات المستخدمة لتخزينها ومعالجتها ونقلها، من السرقة أو التطفل أو من الكوارث الطبيعية أو غيرها من المخاطر ويعمل على إبقائها متاحة للأفراد المصرح لهم باستخدامها.

عناصر (خصائص) أمن المعلومات	
(١) السرية	تعني أن الشخص المخول هو الوحيد القادر على الوصول إلى المعلومات والاطلاع عليها. **مصطلح** مرادف لمفهومي **(الأمن والخصوصية).** **المعلومات الشخصية والمعلومات العسكرية والموقف المالي لشركة ما قبل إعلانه** بيانات يعتمد أمنها على مقدار حفظ سريتها.
(٢) السلامة	**تعني حماية الرسائل أو المعلومات التي تم تداولها والتأكد بأنها لم تتعرض لأي عملية تعديل** بالإضافة أم الاستبدال أم الحذف. عند **نشر نتائج طلبة الثانوية العامة** يجب الحفاظ على هذه النتائج من أي تعديلات. عند **صدور قوائم القبول الموحد للجامعات الأردنية والتخصصات** التي قُبل الطلبة فيها.
(٣) توافر المعلومات	تكون المعلومات رغم الحفاظ على سلامتها وسريتها بلا فائدة في حالتين : **(١) لم تكن متاحة للأشخاص المصرح لهم بالتعامل معها.** **(٢) الوصول إليها يحتاج إلى وقت كبير.** **من الوسائل التي يقوم بها المخترقون جعل هذه المعلومات غير متاحة :** إما بحذفها أو الاعتداء على الأجهزة التي تخزنها.

تقسم المخاطر التي تهدد أمن المعلومات إلى نوعين :	(١) التهديدات. (٢) الثغرات.

التهديدات	أسباب طبيعية	حدوث حريق. انقطاع التيار الكهربائي.
	أسباب بشرية غير متعمدة	**تحدث نتيجة خطأ أو إهمال مثل :** كتابة ٢٤ بدلاً من ٤٢. كتابة عنوان بريد الكتروني بشكل غير صحيح.
	أسباب بشرية متعمدة	**موجهة لجهاز معين في مكان معين** **مثل :** الهجوم (الاعتداء) الالكتروني.
		غير موجهة لجهاز معين **مثل :** نشر الفيروسات في المواقع الإلكترونية.

عوامل تقسيم (نجاح) الهجوم الالكتروني		
	الدافع	(١) رغبة في الحصول على المال. (٢) محاولة لإثبات القدرات التقنية. (٣) قصد الإضرار بالأخرين.
	الطريقة	(١) المهارات التي يتميز بها المعتدي الالكتروني. (٢) معرفته بتصميم وآلية عمل النظام. (٣) قدرته على توفير المعدات والبرمجيات الحاسوبية التي يحتاج إليها. (٤) معرفة نقاط القوة والضعف لهذا النظام.
	فرصة النجاح	(١) تحديد الوقت المناسب للتنفيذ. (٢) كيفية الوصول إلى الأجهزة.

أنواع الاعتداءات الالكترونية		
نوع الاعتداء	**الحالة**	**عنصر أمن المعلومات الذي يتأثر**
(١) التنصت على المعلومات.	الحصول على المعلومات السرية.	**سرية المعلومات**
(٢) التعديل على المحتوى.	اعتراض المعلومات وتغيير محتواها وإعادة إرسالها للمستقبل.	**سلامة المعلومات**
(٣) الإيقاف.	قطع قناة الاتصال. ومنع المعلومات من الوصول.	**توافر المعلومات**
(٤) الهجوم المزوّر (المفبرك)	إرسال المعتدي الإلكتروني رسالة إلى أحد الأشخاص على الشبكة يخبره فيها بأنه صديقه ويحتاج إلى معلومات أو كلمات سرية خاصة.	**سلامة وسرية المعلومات**

الثغرات

يقصد بها نقطة الضعف في النظام سواء أكانت في الإجراءات المتبعة أم مشكلة في تصميم النظام.

(١) عدم تحديد صلاحيات الوصول إلى المعلومات.

(٢) مشكلة في تصميم النظام.

(٣) عدم كفاية الحماية المادية للأجهزة والمعلومات.

تعد الثغرات من المخاطر التي تهدد أمن المعلومات لأنها تتسبب في فقدان المعلومات أو هدم النظام أو تجعله عرضة للاعتداء الالكتروني.

الحد من مخاطر أمن المعلومات

يرى المختصون في مجال أمن المعلومات بأن الحفاظ على المعلومات وأمنها ينبع من التوازن بين **تكلفة الحماية وفعالية الرقابة** من جهة و **احتمالية الخطر** من جهة أخرى.

وضعت مجموعة من الضوابط في نظام المعلومات **لتقليل المخاطر التي قد تتعرض لها المعلومات والحد منها.** **شتوية ٢٠١٨**

١ – الضوابط المادية : مراقبة بيئة العمل وحمايتها من الكوارث الطبيعية وغيرها ؛ مثل وجود حراس الأمن واستخدام الجدران.

٢ – الضوابط الإدارية : تستخدم مجموعة من الأوامر والإجراءات المتفق عليها مثل القوانين واللوائح والسياسات والعقود والاتفاقيات.

٣ – الضوابط التقنية : هي الحماية التي تعتمد على التقنيات المستخدمة مثل كلمات المرور والتشفير والجدران النارية وتحديد الصلاحيات.

الهندسة الاجتماعية

مفهوم الهندسة الاجتماعية : **شتوية ٢٠١٨**

هي الوسائل والأساليب التي يستخدمها المعتدي الإلكتروني لجعل مستخدم الحاسوب في النظام يعطي معلومات سرية أو يقوم بعمل ما يسهّل عليه الوصول إلى أجهزة الحاسوب أو المعلومات المخزنة فيها.

تعد الهندسة الاجتماعية من أنجح وأسهل الوسائل المستخدمة للحصول على المعلومات غير مصرح بالاطلاع عليها.

(١) قلة اهتمام المتخصصين في مجال أمن المعلومات. **(٢)** عدم وعي مستخدم الحاسوب بالمخاطر المترتبة عليها.

مجالات الهندسة الاجتماعية : (أ) البيئة. (ب) الجانب النفسي.

(أ) مجال البيئة	
(١) مكان العمل :	يكتب بعض الموظفين كلمات المرور على أوراق ملصقة بشاشة الحاسوب، وعند دخول الشخص غير المخول له الاستخدام **كزبون أو عامل نظافة أو عامل صيانة** يستطيع معرفة كلمات المرور ومن ثم يتمكن من الدخول إلى النظام بسهولة ليحصل على المعلومات التي يريدها.
(٢) الهاتف :	يتصل الشخص غير المخول بمركز الدعم الفني هاتفياً، ويطلب إليه بعض المعلومات الفنية ويستدرجه للحصول على كلمات المرور وغيرها من المعلومات ليستخدمها في ما بعد.
(٣) النفايات الورقية :	يدخل الأشخاص غير المخولين إلى مكان العمل ويجمعون النفايات التي قد تحتوي على كلمات المرور ومعلومات تخص الموظفين وأرقام هواتفهم وبياناتهم الشخصية وقد تحتوي على تقويم العام السابق وكل ما تحتويه من معلومات يمكن استغلالها في تتبع الموظفين أو الحصول على المعلومات المرغوبة.
(٤) الإنترنت :	حيث ينشئ المعتدي الإلكتروني موقعاً على الشبكة يقدم خدمات معينة ويشترط التسجيل فيه للحصول على هذه الخدمات، يتطلب التسجيل في الموقع اسم مستخدم وكلمة المرور وهي كلمة المرور نفسها التي يستخدمها الشخص عادةً، **وبهذه الطريقة** يتمكن المعتدي الإلكتروني من الحصول عليها.
يعد الإنترنت أكثر الوسائل شيوعاً ؛ **<u>وذلك بسبب استخدام الموظفين أو مستخدمي الحاسوب عادة كلمة المرور نفسها للتطبيقات جميعها</u>**	

(ب) الجانب النفسي	
(١) الإقناع :	**<u>الطريقة المباشرة :</u>** يستطيع المعتدي إقناع الموظف أو مستخدم الحاسوب بطريقة مباشرة **بحيث يقدم الحجج المنطقية والبراهين.** **<u>الطريقة غير المباشرة :</u>** يعمد إلى تقديم إيحاءات نفسية تحث المستخدم على قبول المبررات من دون تحليلها أو التفكير فيها. **إظهار نفسه بمظهر صاحب السلطة** أو **إغراء المستخدم بامتلاك خدمة نادرة ؛** حيث يقدم له عرضاً معيناً من خلال موقعه الإلكتروني لمدة محدودة يمكنه ذلك من الحصول على كلمة المرور.
(٢) انتحال الشخصية :	حيث يتقمص شخص شخصية آخر، وهذا الشخص قد يكون شخصاً حقيقياً أو وهمياً. فقد ينتحل شخصية فني صيانة معدات الحاسوب أو عامل نظافة أو حتى المدير أو السكرتير؛ وبما أن الشخصية المنتحلة غالباً تكون ذات سلطة يبدي أغلب الموظفين خدماتهم ولن يترددوا بتقديم أي معلومات لهذا الشخص.
(٣) مسايرة الركب :	يرى الموظف بأنه إذا قام زملاؤه جميعهم بأمر ما فمن غير اللائق أن يأخذ موقفاً مغايراً.

أمن الانترنت

علل : تم إيجاد وسائل تقنية تعمل على حماية الانترنت(الويب) :

(١) بسبب انتشار البرامج والتطبيقات المجانية وغير معروفة المصدر ومفتوحة المصدر "يمكن استخدامها في الأجهزة المختلفة".

(٢) الحد من الاعتداءات والأخطار التي تهدده بسبب انتشار البرامج المقرصنة والمعلومات الخاصة بكيفية اقتحام المواقع.

أشهر الاعتداءات الالكترونية على الويب

١ – الاعتداءات على متصفحات الانترنت. **٢ – الاعتداءات الالكترونية على البريد الالكتروني.**

١ – الاعتداءات على متصفحات الانترنت.

ما هو متصفح الانترنت :

برنامج ينقل المستخدم إلى صفحة **الويب** التي يريدها بمجرد كتابة العنوان والضغط على زر الذهاب ويمكنه من مشاهدة المعلومات على الموقع.

يتعرض متصفح الإنترنت إلى الكثير من الأخطار **لأنها قابلة للتغيير من دون ملاحظة ذلك من قبل المستخدم.**

الاعتداء الالكتروني على متصفحات الانترنت يتم بطريقتين :

(١) الاعتداء عن طريق (كود) بسيط.

يُمكن إضافته إلى المتصفح وباستطاعته القراءة والنسخ وإعادة إرسال أي شيء يتم إدخاله من قبل المستخدم.

يتمثل التهديد بالقدرة على الوصول إلى الحسابات المالية والبيانات الحساسة الأخرى.

(٢) توجيه المستخدم إلى صفحة أخرى غير الصفحة التي يريدها.

٢ – الاعتداءات على البريد الالكتروني

تحدث اعتداءات على الويب من خلال البريد الإلكتروني ، **لأن بعض الرسائل الإلكترونية التي تحمل عروضاً وهمية وروابط تحمل عناوين جذابة وتكون مزيفة ولا يمكن اكتشافها من خلال الأشخاص قليلي الخبرة والتي تحمل روابط لنقل المستخدم لصفحات أخرى.**

يحاول المعتدي الإلكتروني التعامل مع الأشخاص قليلي الخبرة ، حيث يقدّم عروض شراء لمنتجات بعض المصممين بأسعار زهيدة، **أو** رسائل تحمل عنوان كيف تصبح ثرياً ، وهذه الرسائل تحتوي روابط يتم الضغط عليها للحصول على مزيد من المعلومات وغيرها من الرسائل المزيفة والمضللة التي تحتاج إلى وعي من المستخدم.

تقنية تحويل العناوين الرقمية NAT

هي التقنية التي تعمل على إخفاء العنوان الرقمي للجهاز في الشبكة الداخلية ليتوافق مع العنوان الرقمي المعطى للشبكة.

هي إحدى الطرائق المستخدمة لحماية المعلومات من الاعتداءات الإلكترونية.

من خلال إخفاء العنوان الرقمي الداخلي لجهاز الحاسوب فيمنع ذلك من الاعتداء عليه.

تُسهم في **حماية الجهاز في الشبكة الداخلية من أي هجوم قد يُشن عليه بناءً على معرفة العناوين الرقمية.**

العناوين الرقمية – IP address

يرتبط ملايين الأشخاص عبر شبكة الانترنت بملايين الأجهزة، ولكل جهاز حاسوب أو هاتف خلوي عنوان رقمي خاص به يميزه عن غيره يسمى **(IP Address).**

أنواع العناوين الرقمية

١ – العناوين الرقمية (IP4).	**تتكون من ٣٢ خانة ثنائية تتوزع على أربعة مقاطع يفصل بينها نقاط.** **كل مقطع من هذه المقاطع يتضمن رقماً من (0) إلى (255)** كالآتي : **215.128.004.216**
٢ – العناوين الرقمية (IPv6).	**تتكون من ثمانية مقاطع** بدلاً من أربعة. **العناوين الالكترونية (IPv6) أكثر من العناوين الالكترونية (IP4).**

على الرغم من استخدام **(IPv6)** إلا إنه لا يكفي لإتاحة عدد هائل من العناوين الرقمية ولحل هذه المعضلة وجد ما يسمى **تقنية تحويل العناوين الرقمية (NAT).**

تقنية تحويل العناوين الرقمية – NAT

السلطة المسئولة عن منح أرقام الانترنت المخصصة لإعطاء العناوين الرقمية للأجهزة على الانترنت هي **أيانا – IANA.**

بسبب قلة أعداد هذه العناوين مقارنة بعدد المستخدمين **فإنها تعطي الشبكة الداخلية عنواناً واحداً (مجموعة عناوين) ويكون معرِّفاً لها عند التعامل في شبكة الإنترنت.**

كل شبكة داخلية **تمنح عنواناً خاصاً بها على الانترنت مختلفاً عن العناوين الأخرى.** (العنوان الرقمي للشبكة)

العنوان الرقمي للشبكة الداخلية لن يتكرر.

تعطي الشبكة الداخلية كل جهاز داخل الشبكة **عنواناً رقمياً لغرض الاستخدام الداخلي فقط** (العنوان الداخلي للجهاز)، ولا يعترف بهذا العنوان خارج الشبكة.

وهذا يعني أن العنوان الرقمي الداخلي للجهاز يمكن أن يتكرر في أكثر من شبكة داخلية.

عند رغبة أحد الأجهزة بالتواصل مع جهاز خارج الشبكة الداخلية **يعدّل العنوان الرقمي الخاص بالجهاز** باستخدام **تقنية تحويل العناوين الرقمية (NAT)** وذلك يتم باستخدام **جهاز وسيط**، يكون غالباً **موجّهاً (router)** أو **جداراً نارياً.**

وظيفة الجهاز الوسيط : يحوّل **العنوان الرقمي الداخلي إلى عنوان رقمي خارجي** ويسجل ذلك في سجل خاص للمتابعة يتم التواصل مع الجهاز الهدف في الشبكة الأخرى عن طريق هذا الرقم الخارجي على أنه العنوان الخاص بالمرسل.

عندما يقوم الجهاز الهدف بالرد على رسالة الجهاز المرسل تصل إلى الجهاز الوسيط الذي يحوّل **العنوان الرقمي الخارجي** إلى **عنوان داخلي** من خلال سجل المتابعة لديه ويعيده بذلك إلى الجهاز المرسل.

طرق العمل بتقنية تحويل العناوين الرقمية – NAT

(١) النمط الثابت لتحويل العناوين الرقمية :

بهذه الطريقة يكون عدد الأجهزة الداخلية في الشبكة أقل أو يساوي عدد العناوين الرقمية الخارجية لدى الجهاز الوسيط.

يتم عن طريق هذا النمط تخصيص عنوان رقمي خارجي لكل جهاز داخلي ، وهذا العنوان الرقمي ثابت لا يتغير.

(٢) النمط المتغير لتحويل العناوين الرقمية :

يتم إعطاء عنوان رقمي مؤقت للتواصل مع الأجهزة خارج الشبكة وحين انتهاء الاتصال يصبح هذا الرقم متاحاً لأي جهاز أخر داخل الشبكة.

بهذه الطريقة يكون لدى الجهاز الوسيط عدد من العناوين الرقمية الخارجية ولكنها **غير كافية** لعدد الأجهزة في الشبكة.

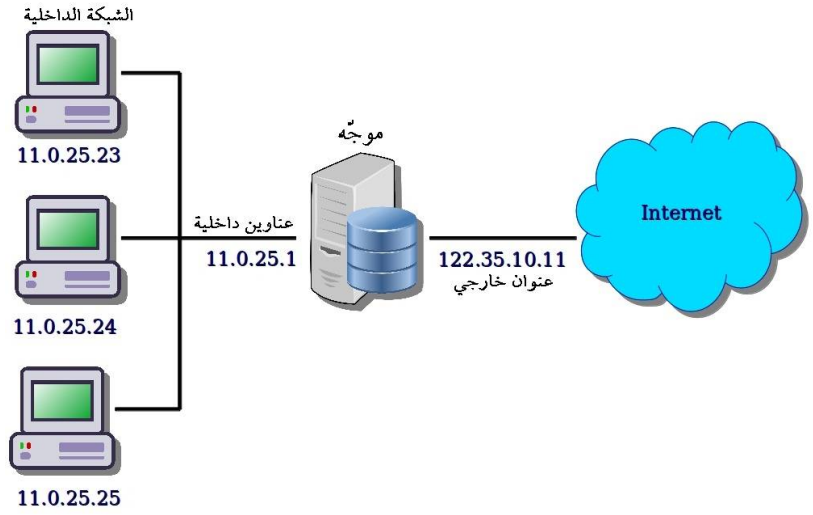
هذه العناوين تبقى متاحة لجميع الأجهزة على الشبكة ، وعند رغبة أحد الأجهزة بالتراسل خارجياً فإنه يتواصل مع الجهاز الوسيط الذي يعطيه **عنواناً خارجياً مؤقتاً** يستخدمه لحين الانتهاء من عملية التراسل ويعد هذا العنوان **عنواناً رقمياً خاصاً بالجهاز.**

عند انتهاء عملية التراسل يفقد الجهاز الداخلي هذا العنوان ويصبح العنوان متاحاً للتراسل مرة أخرى.

عند رغبة الجهاز نفسه بالتراسل مرة أخرى قد يعطى عنواناً مختلفاً عن المرة السابقة .

فسّر اختلاف IP Address للجهاز عند تراسله أكثر من مرة.

بسبب النمط المتغير لتحويل العناوين الرقمية ***NAT*** حيث يتم إعطاء الجهاز عنواناً رقمياً مختلفاً في كل مرة يتواصل فيها مع الأجهزة خارج الشبكة الداخلية.



الفصل الثالث – التشفير

السؤال الأول: علل كل من العبارات الآتية :

(١) يعد التشفير من أفضل الوسائل المستخدمة للحفاظ على أمن المعلومات.

حيث يعمل على إخفاء المعلومات عن الأشخاص غير المصرح لهم بالاطلاع عليها.

(٢) سميت خوارزميات المفتاح الخاص بهذا الاسم أو **بالخوارزميات التناظرية**.

حيث أن المفتاح نفسه يستخدم لعمليتي التشفير وفك التشفير.

(٣) تسمى خوارزميات المفتاح الخاص أيضاً **خوارزميات المفتاح السري**.

حيث يتم الاتفاق على اختيار المفتاح قبل بدء عملية التراسل بين المرسل والمستقبل.

(٤) تسمى خوارزميات المفتاح العام أيضاً **الخوارزميات اللاتناظرية**.

حيث تستخدم هذه الخوارزميات مفتاحين إحداهما لتشفير الرسالة ويكون معروفاً للمرسل والمستقبل (المفتاح العام) والآخر يكون معروفاً فقط للمستقبل يستخدم لفك التشفير (المفتاح الخاص).

(٥) شيفرات الكتل **أبطأ من** شيفرات التدفق.

حيث تقسم الرسالة إلى أجزاء ولكن بحجم أكبر من حجم الأجزاء في شيفرات التدفق. (حجم المعلومات أكبر).

السؤال الثاني: أجب عن الأسئلة الآتية :

(١) ما المقصود بالتشفير؟ وما الهدف منه؟

تغيير محتوى الرسالة الأصلية سواءً بمزجها بمعلومات أخرى أو استبدال الأحرف الأصلية والمقاطع بغيرها أم تغيير لمواقع الأحرف بطريقة لن يفهمها إلا مرسل الرسالة ومستقبلها فقط باستخدام خوارزمية معينة ومفتاح خاص.

الهدف من التشفير:

الحفاظ على سرية المعلومات أثناء تبادلها بين مرسل المعلومة ومستقبلها وعدم الاستفادة منها أو فهم محتواها حتى لو تم الحصول عليها من قبل أشخاص معترضين.

(٢) ما هي عناصر التشفير؟

(١) النص الأصلي.	محتوى الرسالة الأصلية قبل التشفير وبعد عملية فك التشفير.
(٢) خوارزمية التشفير.	الخطوات المستخدمة لتحويل الرسالة الأصلية إلى رسالة مشفرة.
(٣) مفتاح التشفير.	سلسلة من الرموز المستخدمة في خوارزمية التشفير وتعتمد قوة التشفير على قوة المفتاح.
(٤) شيفرة النص(النص المشفر).	الرسالة بعد عملية التشفير.

تصنيف خوارزميات التشفير حسب المعايير		
	نوع عملية التشفير	**(١) طريقة التشفير بالتعويض :** طريقة لتشفير النصوص يتم من خلالها **استبدال حرف مكان حرف أو مقطع مكان مقطع** ومثال عليها **شيفرة الإزاحة**. **(٢) طريقة التشفير بالتبديل :** تبديل أماكن الأحرف من خلال إعادة ترتيب أحرف الكلمة بشرط استخدام نفس الأحرف دون إجراء أي تبديل أو تغيير عليها ؛ مثال عليها : **خوارزمية الخط المتعرج.**
	عدد المفاتيح المستخدمة	**(١) خوارزميات المفتاح الخاص** (الخوارزميات التناظرية) **:** يطلق عليها أيضاً اسم الخوارزميات التناظرية ؛ **حيث أن المفتاح نفسه يستخدم لعملتي التشفير وفك التشفير.** **تسمى أيضاً خوارزميات المفتاح الخاص** حيث يتم الاتفاق على اختياره قبل بدء عملية التراسل بين المرسل والمستقبل. **(٢) خوارزميات المفتاح العام** (الخوارزميات اللاتناظرية) **:** تستخدم **مفتاحين**، **المفتاح العام** يستخدم للتشفير ومرئي للجميع **و المفتاح الخاص** يستخدم لفك التشفير و لا يعرفه سوى المستقبل.
	كمية المعلومات المرسلة	**(١) شيفرات التدفق :** يعمل هذا النوع على تقسيم الرسالة إلى مجموعة أجزاء، ويُشفر كل جزء منها على حدة، ومن ثم يرسله. **(٢) شيفرات الكتل :** تقسم الرسالة أيضاً إلى أجزاء ولكن بحجم أكبر من حجم الأجزاء في شيفرات التدفق، ويُشفّر أو يفكّ تشفير كل كتلة على حدة. يختلف عن شيفرات التدفق **بأن حجم المعلومات أكبر لذا فإنها أبطأ.**