الوحدة الرابعة: أمن المعلومات والتشفير

❖ **مقدمة نظرية:**

س١: هل اهتمت الشعوب القديمة بالمحافظة على سرية المعلومات، ما السبب في ذلك ؟

نعم، وذلك للحفاظ على أسرارها وهيبتها ومكانتها، وخاصة لإنجاح مخططاتها العسكرية، وعدم تمكين العدو منها.

س٢: على ما ذا اعتمدت سرية المعلومات قديما ؟

اعتمدت على موثوقية حاملها وقدرته على توفير الظروف المناسبة لمنع اكتشافها وتسريبها.

س٣: مع تطور العلم واستخدام شبكات الحاسوب، هل هنالك حاجة أكبر للمحافظة على سرية المعلومات ؟

نعم، حيث نحتاج دوما لطرق جديدة لحماية المعلومات من السرقة والتعديل عليها والحذف لها، مما له من آثار سلبية خطيرة على كافة المجالات.

التوزيع المتوقع
لعلامات الوحدة الرابعة

المحتوى	العلامة المتوقعة
الوحدة الرابعة : أمن المعلومات والتشفير	٣٢
الفصل الأول: أمن المعلومات	١١
الفصل الثاني: أمن الإنترنت	٦
الفصل الثالث: التشفير	١٥

الفصل الثاني: أمن الإنترنت

❖ **مقدمة:**

اعتمد الأفراد واعتمدت المؤسسات والحكومات على تكنولوجيا المعلومات والاتصالات بشكل كبير وفي شتى المجالات بشكل واسع، أذكر آثار ذلك ؟

١. تم انتشار البرامج والتطبيقات بشتى أنواعها، فمنها المجاني ومنها الغير معروف المصدر ومنها المفتوح الذي يمكن استخدامه على الأجهزة المختلفة.
٢. تم انتشار البرامج المقرصنة والمعلومات الخاصة بكيفية اقتحام مواقع الإنترنت (الويب).
٣. أصبح من الضروري إيجاد وسائل تعمل على حماية مواقع الويب والحد من الاعتداءات والأخطار التي تهددها.

أولا: الاعتداءات الإلكترونية على الويب

س١: بماذا تتصف الاعتداءات الإلكترونية على المواقع الإلكترونية (مواقع الويب) ؟

تتصف بأنها غير محسوسة وغير مرئية، فلا يتمكن المستخدم من اكتشافها بسهولة.

س٢: أذكر أمثلة على الاعتداءات الإلكترونية على المواقع الإلكترونية (الويب) ؟

١. الاعتداء على متصفحات الإنترنت.
٢. الاعتداء على البريد الإلكتروني.

س٣: ما المقصود بمتصفح الإنترنت ؟

متصفّح الإنترنت برنامج ينقل المستخدم الى صفحة (الويب) التي يُريدها بمجرد كتابة العنوان والضغط على زر الذهاب، ويمكّنه من مشاهدة المعلومات على الموقع.

س٤: تتعرض متصفحات الإنترنت إلى الكثير من الأخطار كونها قابلة للتغيير دون ملاحظة المستخدم، أذكر طريقتين للاعتداء عليها ؟

١. **الاعتداء عن طريق كود بسيط:** حيث يُضاف للمتصفح مما يمكن المعتدي من قراءة ونسخ وإعادة إرسال أي شيء يتم إدخاله من قِبل المستخدم، ويبرز التهديد بالقدرة على الوصول للحسابات المالية والبيانات الحساسة والسرية.
٢. **توجيه المستخدم لصفحة أخرى غير الصفحة التي يريدها.**

س٥: وضح كيفية الاعتداءات الإلكترونية على البريد الإلكتروني ؟

من خلال قيام المعتدي بإرسال رسائل مزيفة بعضها يسهل اكتشافه والبعض الآخر احترافي إلى أشخاص قليلو الخبرة، ومن أشكاله:

- تقديم عروض شراء لمنتجات بعض المصممين بأسعار زهيدة.
- إرسال رسائل تحمل عنوان كيف تصبح ثريا.

حيث تحتوي هذه الرسائل على روابط يتم الضغط عليها للحصول على مزيد من المعلومات، وبالنهاية تكون هذه الرسائل مظللة وتحتاج لوعي كاف من المستخدم لتجنب التعامل معها.

ثانيا: تقنية تحويل العناوين الرقمية (NAT) (Network Address Translation)

س١: ما المقصود بالعنوان الرقمي (IP Address) (Internet Protocol Address) ؟

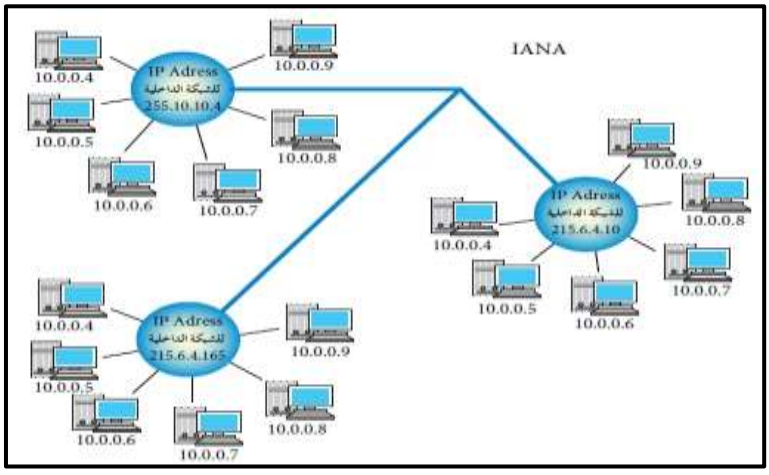
هو العنوان المُعطى للحاسوب أو الهاتف الذي يرغب بالاتصال بشبكة الإنترنت ويمكن أن يكون داخليا أو خارجيا، ويستخدم لتمييز الجهاز المرسل والمستقبل مما يحقق التواصل بينهما، وصاحبة السلطة في تحديد هذه العناوين الخارجية هي منظمة الأيانا (IANA) وفق أنواع معينة منها.

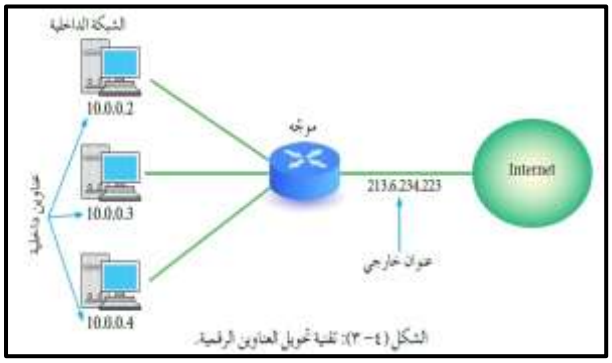
س٢: ما هي أنواع العناوين الرقمية المستخدمة في شبكة الإنترنت ؟

١. **IPv4:** وهو أول الأنواع ظهورا، ويخدم ملايين الأجهزة المرتبطة عبر شبكة الإنترنت، حيث يتكون من أربعة مقاطع يفصل بينها نقاط مثل (192.168.10.1)، وكل مقطع يمثل رقما من 0 إلى 255، وعند تمثيلها بالنظام الثنائي يظهر الرقم مكون من 32 خانة (بحيث يكون لكل مقطع ثمانية خانات ثنائية).

٢. **IPv6:** وهو ثاني نوع ظهر لعدم قدرة النوع الأول (IPv4) على تغطية الأعداد الهائلة من الأجهزة المرتبطة عبر شبكة الإنترنت، حيث يتكون من ثمانية مقاطع بدلا من أربعة.

س٣: كيف نظمت الأيانا (IANA) آلية إعطاء العناوين للأجهزة المرتبطة بشبكة الإنترنت ؟





أولا: تحديد عناوين الشبكات الداخلية والأجهزة الداخلية فيها (الشكل جهة اليمين):

نظرا لقلة العناوين الرقمية مقارنة بأعداد الأجهزة المستخدِمة للإنترنت، قامت منظمة الأيانا بإعطاء كل شبكة داخلية عنوانا فريدا لا يُعطى لأي شبكة داخلية أخرى لاستخدامه للدخول لشبكة الإنترنت مثل (255.10.10.4)، وبإمكان الشركات حجز عنوانين فريدين أو مجموعة منها، ومن ثم تقوم الشبكات الداخلية بإعطاء عناوين لأجهزتها الداخلية بغرض الاستخدام الداخلي فقط، وهذه العناوين يمكن أن تتكرر في أي شبكة داخلية أخرى مثل (10.0.0.5).

ثانيا: استخدام تقنية تحويل العناوين الرقمية الداخلية إلى خارجية عند الاتصال الخارجي (الشكل جهة اليسار):

في حال أراد أحد أجهزة الشبكة الداخلية التواصل مع جهاز خارج شبكته عندها يتم تحويل العنوان الرقمي الداخلي للجهاز من خلال الموجه (Router) أو الجدار الناري (Fire Wall) إلى عنوان رقمي خارجي بتقنية تسمى (NAT)، ويسجل في سجل خاص للمتابعة، وبالعكس عن الجهاز المستقبل.

س٤: ما المقصود بتقنية تحويل العناوين الرقمية (NAT) ؟

- هي إحدى الطرق المستخدمة لحماية المعلومات من الاعتداءات الإلكترونية، حيث تتضمن إخفاء العنوان الرقمي للجهاز المُرسِل في الشبكة الداخلية وتحويله لعنوان رقمي خارجي متوافق مع عنوان الشبكة الداخلية الخاص بها، فيصبح العنوان الرقمي الداخلي غير معروف بالنسبة إلى الجهات الخارجية، مما يُسهم في حمايته من أي هجوم قد يُشنُّ عليه بناء على معرفة العناوين الرقمية له.
- استخدمت هذه التقنية نظرا لقلة أعداد العناوين المستخدمة للاتصال الخارجي مقارنة بأعداد المستخدمين للإنترنت ولتنظيم عملية التراسل ومتابعتها.

س٥: أذكر طرائق تقنية تحويل العناوين الرقمية، مع التوضيح لكل منها ؟

١. النمط الثابت للتحويل:

يتم بها تخصيص عنوان رقمي خارجي ثابت لكل جهاز داخلي يرغب بالتراسل الخارجي فلا يتغير.

٢. النمط المتغير للتحويل:

وهنا يكون لدى الموجه أو الجدار الناري عددا من العناوين الرقمية الخارجية المتاحة للاستخدام، ويتم إعطاء الجهاز الداخلي أحد العناوين الخارجية للتراسل الخارجي بشكل مؤقت، ويصبح هذا الرقم الخارجي متاحا لجهاز داخلي آخر عند انتهاء التراسل، وإن رغب نفس الجهاز الداخلي التراسل مرة أخرى فقد يحصل على نفس الرقم أو يُعطى رقما آخرا.

س٦: ما وظيفة الموجه أو الجدار الناري في الشبكات بوصفه جهازا وسيطا ؟

- تقوم بعملية تحويل العناوين الرقمية (NAT) حيث تحول العنوان الرقمي الداخلي إلى عنوان رقمي خارجي عند الإرسال إلى الشبكة الخارجية والعكس عن الاستقبال.
- يربط الشبكة الداخلية بشبكة داخلية أخرى.
- يربط الشبكة الداخلية بالشبكة الخارجية.

لا تقم بدراسة الفصل الثالث من هذه الوحدة
قبل أن تجيب عن أسئلة الفصل الثاني صفحة ١٤٥

إجابات أسئلة الفصل الثاني

١- ما أسباب إيجاد وسائل تقنية لحماية الإنترنت؟

١. تم انتشار البرامج والتطبيقات بشتى أنواعها، فمنها المجاني ومنها الغير معروف المصدر ومنها المفتوح الذي يمكن استخدامه على الأجهزة المختلفة.
٢. تم انتشار البرامج المقرصنة والمعلومات الخاصة بكيفية اقتحام مواقع الإنترنت (الويب).
٣. السبب الأهم هو: ظهور الاعتداءات الإلكترونية على المواقع الإلكترونية كالاعتداء على متصفحات الإنترنت والبريد الإلكتروني، فكان لا بد من إيجاد وسائل تقنية لحماية الإنترنت.

٢- ما أشهر الاعتداءات على (الويب)؟

١. الاعتداء على متصفحات الإنترنت.
٢. الاعتداء على البريد الإلكتروني.

٣- حدّد نوع الاعتداء في كلٍّ مما يأتي:

أ – توجيه المستخدم إلى صفحة أخرى غير الصفحة التي يريدها.

ب– كود بسيط يُمكن إضافته إلى المتصفّح وباستطاعته القراءة، والنسخ، واعادة الإرسال لأي شيء يتم إدخاله من قِبَل الـمُستخدم.

جـ– يتضمن عروضًا وهمية ومضلّلة، ويحتوي رابطًا يتم الضغط عليه للحصول على معلومات إضافية.

الفرع	نوع الاعتداء
أ-	الاعتداء على متصفحات الإنترنت
ب-	الاعتداء على متصفحات الإنترنت
ج-	الاعتداء على البريد الإلكتروني

٤ – وضّح ما يأتي:

أ – تحدث اعتداءات على (الويب) من خلال البريد الإلكتروني.

ب– تُحافظ تقنية تحويل العناوين الرقمية على أمن المعلومات في (الويب).

الفرع	التوضيح
أ-	من خلال قيام المعتدي بإرسال رسائل مزيفة بعضها يسهل اكتشافه والبعض الآخر احترافي إلى أشخاص قليلو الخبرة، مثل تقديم عروض شراء لمنتجات بعض المصممين بأسعار زهيدة، وإرسال رسائل تحمل عنوان كيف تصبح ثريا، حيث تحتوي هذه الرسائل على روابط يتم الضغط عليها للحصول على مزيد من المعلومات، وبالنهاية تكون هذه الرسائل مظللة وتحتاج لوعي كاف من المستخدم لتجنب التعامل معها.
ب-	حيث تتضمن إخفاء العنوان الرقمي للجهاز المُرسِل في الشبكة الداخلية وتحويله لعنوان رقمي خارجي متوافق مع عنوان الشبكة الداخلية الخاص بها، فيصبح العنوان الرقمي الداخلي غير معروف بالنسبة إلى الجهات الخارجية، مما يُسهم في حمايته من أي هجوم قد يُشنُّ عليه بناء على معرفة العناوين الرقمية له.

---

٥ – ما الفرق بين العناوين الرقمية IP4 و IPv6؟

أوجه المقارنة	IPv4	IPv6
حسب عدد مقاطعه	يتكون من أربعة مقاطع	يتكون من ثمانية مقاطع
حسب عدد الأجهزة التي يخدمها	أقل	أكثر

---

٦ – مَن السلطة المسؤولة عن منح أرقام الإنترنت المخصصة لإعطاء العناوين الرقمية؟

منظمة الأيانا (IANA).

---

٧ – ما وظيفة الجهاز الوسيط؟

يقوم بتقنية تحويل العناوين الرقمية (NAT)، حيث يحول العنوان الرقمي الداخلي إلى عنوان رقمي خارجي عند الإرسال إلى الشبكة الخارجية والعكس عن الاستقبال.

٨ – قارن بين طريقتي العمل لكلٍّ من:

النمط الثابت لتحويل العناوين الرقمية، والنمط المتغير لتحويل العناوين الرقمية.

أوجه المقارنة	النمط الثابت بالتحويل	النمط المتغير بالتحويل
آلية العمل	يتم بها تخصيص عنوان رقمي خارجي ثابت لكل جهاز داخلي يرغب بالتراسل الخارجي فلا يتغير.	وهنا يكون لدى الجهاز الوسيط عددا من العناوين الرقمية الخارجية المتاحة للاستخدام، ويتم إعطاء الجهاز الداخلي أحد العناوين الخارجية للتراسل الخارجي بشكل مؤقت، ويصبح هذا الرقم الخارجي متاحا لجهاز داخلي آخر عند انتهاء التراسل، وإن رغب نفس الجهاز الداخلي التراسل مرة أخرى فقد يحصل على نفس الرقم أو يُعطى رقما آخرا.
عدد العناوين الخارجية لديه	عنوان واحد فقط	عدة عناوين