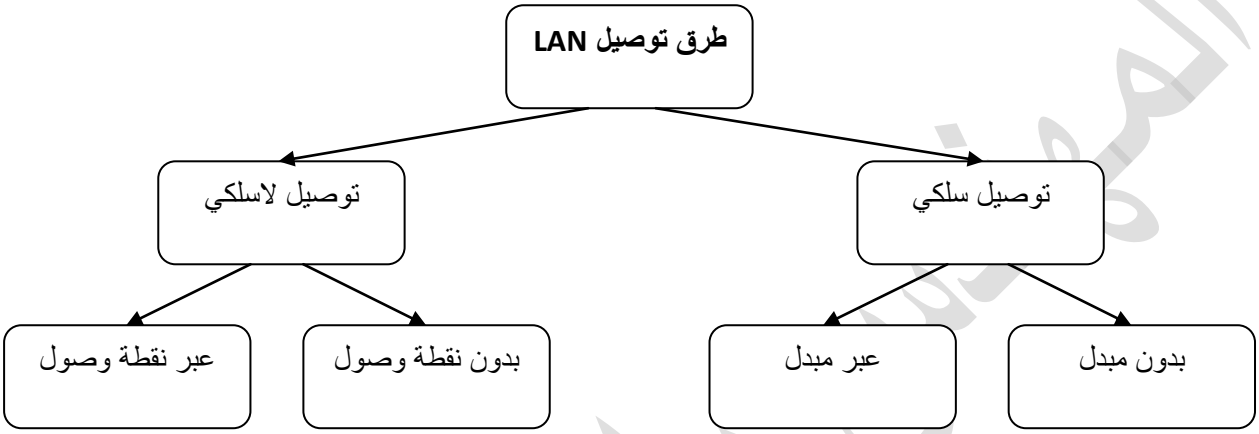
مقدمة: طرق توصيل LAN

سنركز في بداية القسم العملي من مقرر أمن شبكات1 على أمن الشبكة المحلية (Local Area Network: LAN) من نوع مجموعة العمل (Work Group)[1] والتي تتواجد في المنازل والمكاتب والشركات الصغيرة. ولكن قبل البدء في دراسة أمان الشبكة المحلية; لنتذكّر طرق توصيلها كما في الشكل (1).



الشكل (1)

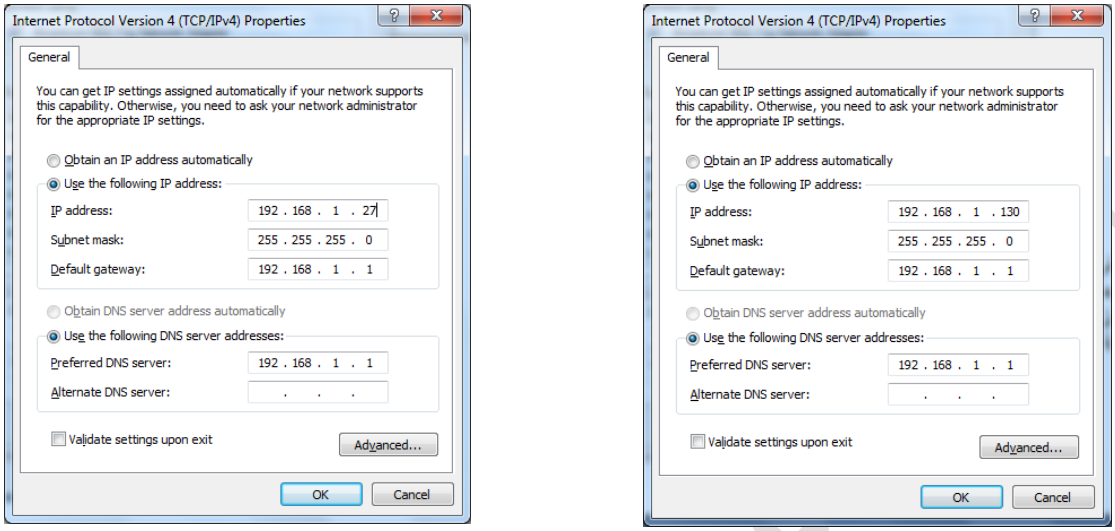
- بدون مبدل: ونستطيع ربط جهازين فقط بكبل يكون عادةً من نوع Cross[2].
- عبر مبدل: ونستطيع ربط جهازين أو أكثر بكبل يكون عادةً من نوع Straight[3].
- بدون نقطة وصول: وتسمى بتقنية Ad Hoc، وفيها نستطيع ربط 8 حواسيب كحد أقصى. وتعتبر من الحلول المؤقتة للربط الشبكي.
- عبر نقطة وصول: وهنا نستخدم نقطة وصول وفيها نستطيع ربط ما يصل إلى 30 جهاز شبكي كحد أقصى لضمان أداء فعال.

ملاحظة (1): من الشائع أن تحتوي LAN على: توصيل سلكي مع مبدل، وتوصيل لاسلكي عبر نقطة وصول معاً ضمن نفس الشبكة.

ملاحظة (2): في أي نوع توصيل من الأنواع السابقة يجب أن تكون عناوين IP لجميع الحواسيب الموجودة ضمن نفس الـ LAN من نفس عنوان الشبكة.

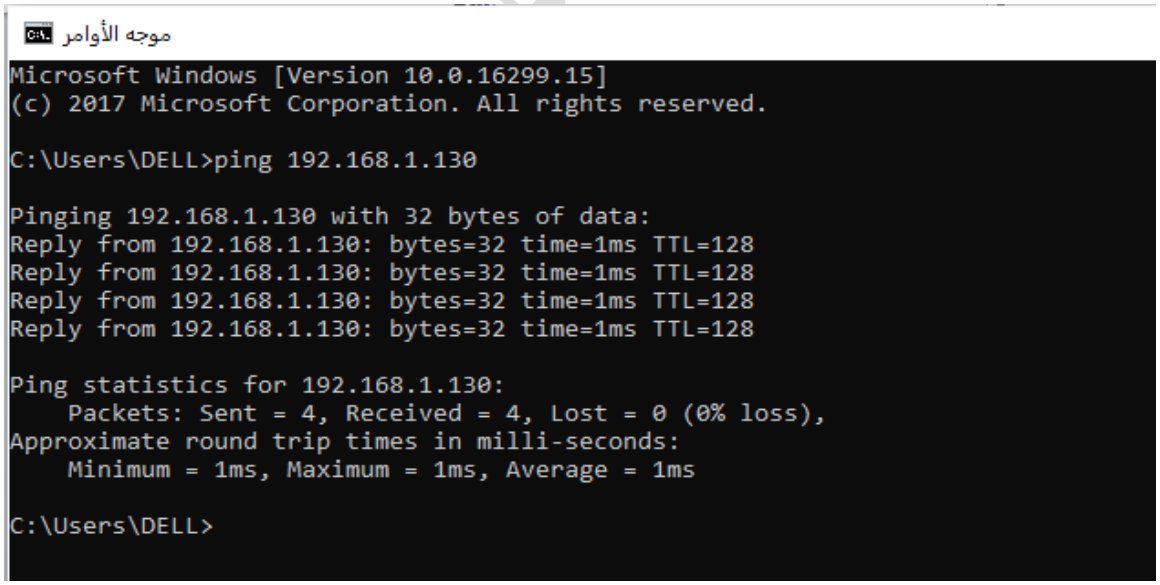
[1] قد توجد الشبكات المحلية على شكل مجموعة عمل (Work Group) أي ند لند (Peer to Peer)، أو على شكل شبكات مجال (Domain) أي مخدم-زبون (Server-Client).
[2] نستطيع أن نقوم بربطهما أيضاً بكبل من نوع Straight إذا استطاعا التفاوض فيما بينهما.
[3] نستطيع أن نقوم بربطهم بكبل من نوع Cross إذا استطاعوا التفاوض فيما بينهم.

يوضح الشكل (2) عنواني IP لحاسوبين. هذان العنوانان وهما 192.168.1.27 و 192.168.1.130 ينتميان لنفس الشبكة التي هي 192.168.1.0 ذات القناع 255.255.255.0. بالتأكيد يمكن لهذين الحاسوبين التواصل بنجاح بينهما ضمن LAN لأنهما ينتميان لنفس الشبكة.



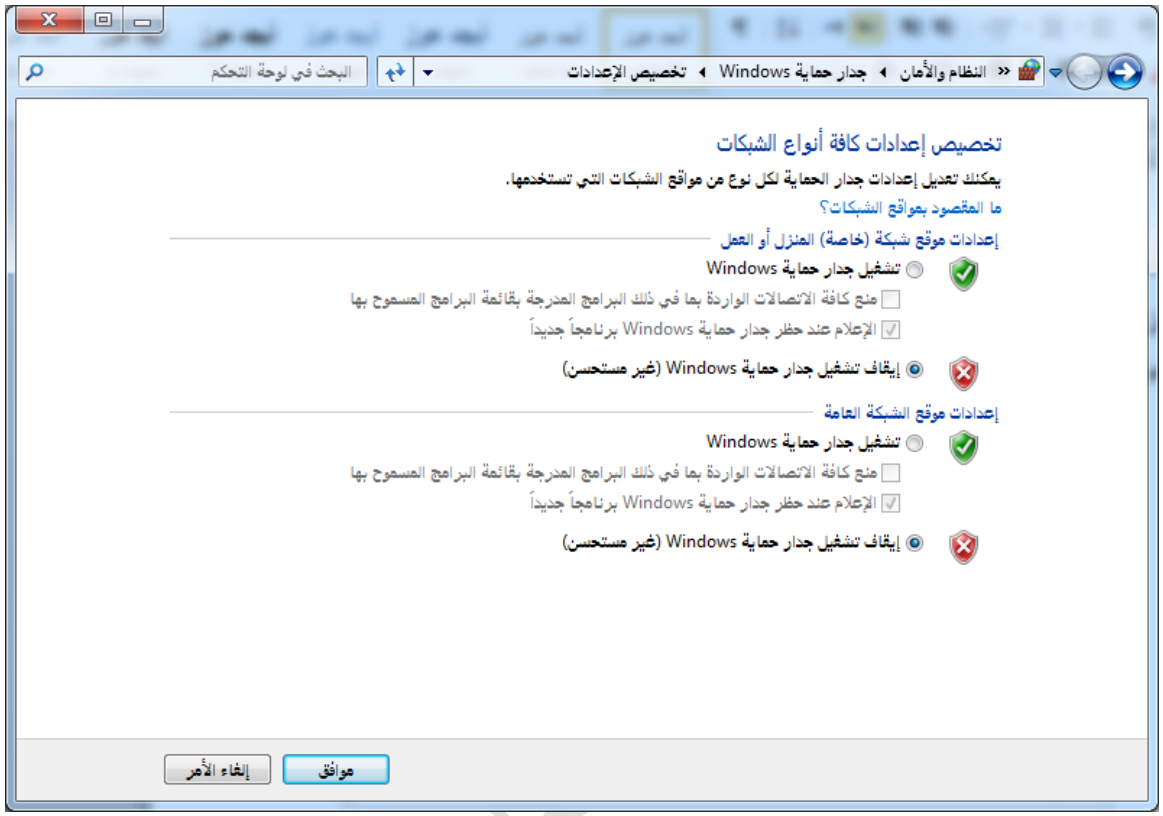
الشكل (2)

سنقوم باختبار الاتصال بين الحاسوبين من خلال الأمر ping و كتابة عنوان Ip الجهاز الذي نريد اختبار الاتصال معه. مثلاً إذا كنا في الجهاز ذو العنوان 192.168.1.27 ونريد التحقق من الاتصال مع 192.168.1.130، عندها سنقوم بكتابة الأمر ping 192.168.1.130



النتيجة تبين نجاح عملية الاتصال بزمن حياة Time-to-live TTL=128 للحزمة المرسلة. من أهم أسباب فشل الاتصال يجب فحص حالة جدار الحماية (Firewall) وايقافه في الحاسوبين.

من أجل تشغيل أو إيقاف جدار الحماية firewall من لوحة التحكم نختار "مركز الشبكة والمشاركة" نقوم بالنقر على خيار جدار حماية Windows ثم نختار من الجانب الأيمن "تشغيل جدار حماية أو إيقاف تشغيله" فنقوم بإيقاف التشغيل كما هو موضح في الشكل:



أمان مشاركة الملفات

تحدث عملية مشاركة الملفات والمجلدات في شبكات مجموعات العمل (Workgroup) بطرق مختلفة، منها:

1- مشاركة الملفات من أي مجلد على الكمبيوتر.

2- مشاركة الملفات من المجلد العمومي (Public Folder).

يعتمد اختيار المستخدم لأي الأسلوبين السابقين على: المكان الذي نرغب في تخزين المجلدات المشتركة عليه، ومن نرغب في المشاركة معه، وإلى أي مدى يكون التحكم في الملفات. يجب ألا يغيب عن الذهن أن عملية المشاركة تتم بين حسابات المستخدمين على نفس الحاسوب وتتم أيضاً بين الكومبيوترات على ضمن LAN.

1- مشاركة الملفات من أي مجلد على الكمبيوتر

يمكن بهذا الأسلوب من المشاركة تحديد من له حق القيام بتغييرات على الملف الذي تمت مشاركته، وأي أنواع التغيير يمكن القيام بها. يتم ذلك بواسطة إعدادات أذونات (Permissions) المشاركة.

تعريف الأذونات (Permissions): بشكل عام هي عملية تحديد صلاحيات من يمكنه رؤية الملف وما الذي يستطيع القيام به على هذا الملف. يمكن القيام بأحد الخيارين التالين:

A) قراءة: وهو خيار "النظر وعدم اللمس"، أي يستطيع المستفيدون من عملية المشاركة فتح الملف، لكن لا يمكنهم تعديله أو حذفه.

B) القراءة/ الكتابة: وهو خيار "افعل ما تريد"، أي يستطيع المستفيدون من عملية المشاركة فتح الملف أو تعديله أو حذفه.

يمكن منح أذونات المشاركة لمستخدم أو مجموعة مستخدمين على نفس الحاسب. على سبيل المثال: يمكن السماح لبعض الأشخاص بعرض الملفات المشتركة فقط، والسماح لآخرين بعرضها وتغييرها. سيتمكن من تقوم بالمشاركة معه من رؤية المجلدات التي تمت مشاركتها فقط.

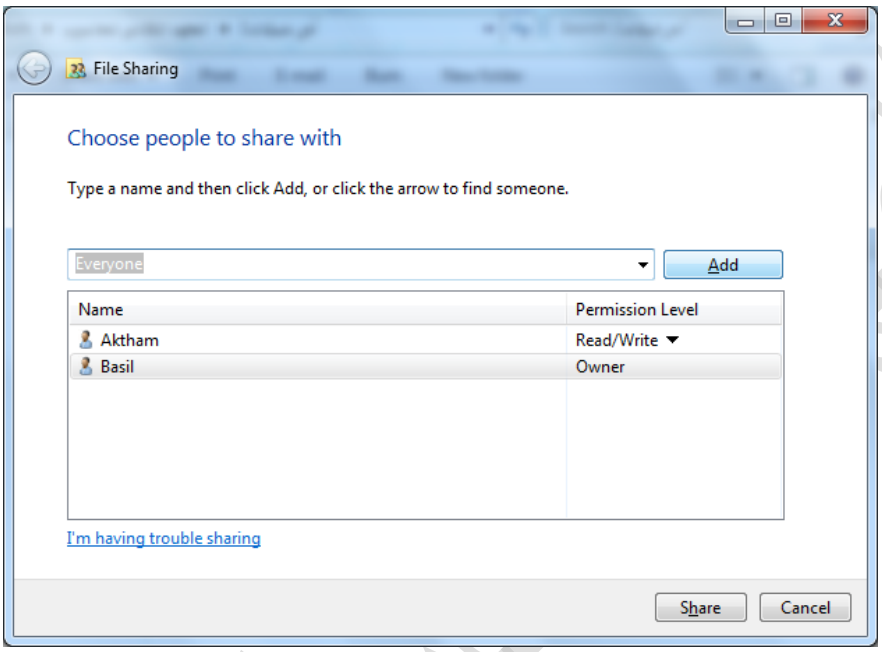
كما يمكن استخدام هذا الأسلوب من المشاركة كطريقة للوصول إلى الملفات المشتركة عند استخدامك حاسوب أخر عبر الشبكة.

اتبع الخطوات التالية لمشاركة الملفات بهذا الطريقة. تذكر أنه باستخدام هذا الأسلوب، يمكنك اختيار الأشخاص الذين ترغب في مشاركة الملفات معهم.

A) انقر فوق واحد أو أكثر من الملفات أو المجلدات التي ترغب في القيام بمشاركتها، ثم من شريط الأدوات، انقر فوق "مشاركة مع" (Share With) ثم "تحديد الأشخاص" (Specific People).

B) في مربع الحوار المفتوح الذي يشبه الشكل (3)، قم بإجراء واحد مما يلي:

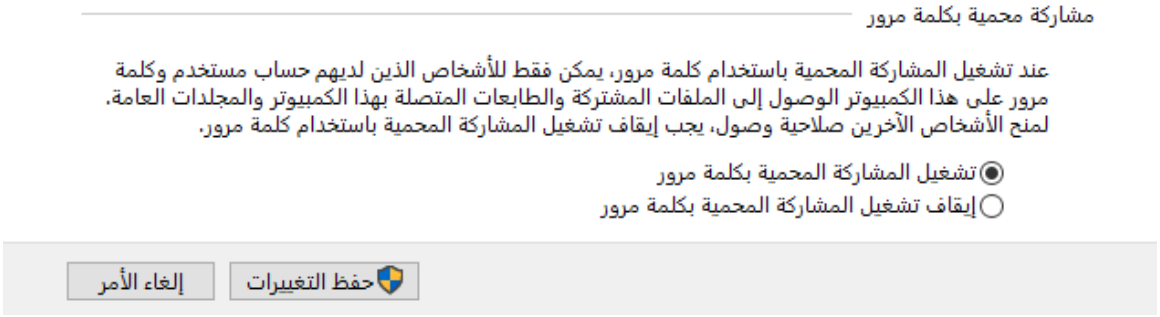
- إذا كنت ترغب في مشاركة الملف أو المجلد مع حساب آخر على نفس كمبيوترك، اختر ذلك الحساب ثم حدد مستوى الأذونات ثم انقر فوق "إضافة" (Add).
- إذا كنت ترغب في مشاركة الملف أو المجلد مع كمبيوتر آخر، اختر "الكل" (Everyone) ثم حدد مستوى الأذونات ثم انقر فوق "إضافة" (Add).



الشكل (3)

C) تابع العمل بالضغط على زر "مشاركة" (Share) ثم "التالي" (Next) ثم تم (Done).

ملاحظة (3): بالإمكان "تشغيل مشاركة محمية بكلمة مرور" أو إيقاف تشغيلها من "مركز الشبكة والمشاركة"[4] (Network and sharing Center). في حالة تشغيل الحماية باستخدام كلمة مرور على الكمبيوتر، يجب أن يكون لدى الكمبيوتر الذي نقدم المشاركة له حساب مستخدم وكلمة مرور على الكمبيوتر لدينا حتى يتمكن من الوصول إلى الملفات والمجلدات التي قمنا بمشاركتها..



[4] سنتحدث لاحقاً عن مركز الشبكة والمشاركة.

2- مشاركة الملفات من المجلد العمومي (Public Folder) الموجود على الكمبيوتر.

ماهو المجلد العمومي وأين يوجد؟ هو مجلد يحوي عدة مجلدات فرعية بداخله ويسمى أيضاً بـ"المكتبات" (Libraries) و يوجد في المسار C:\Users\Public كما يوضح ذلك الشكل (4).

الشكل (4)

بهذا الأسلوب من المشاركة، نقوم بنسخ الملفات أو نقلها إلى المجلد العمومي ثم نقوم بمشاركتها من هذا الموقع. في حالة "تشغيل مشاركة الملف للمجلد العمومي" من "مركز الشبكة والمشاركة"، سيتمكن أي شخص بحساب المستخدم وكلمة المرور الموجودة على الكمبيوتر، فضلا عن أي شخص على الشبكة، من رؤية كافة الملفات الموجودة على المجلد العمومي أو المجلدات الفرعية. يتعذر تقييد الأشخاص لمجرد رؤية بعض الملفات على المجلد العمومي. ومع ذلك، يمكن تعيين الأذونات التي تقيد الأشخاص من الوصول إلى المجلد العمومي تمامًا، أو من القيام بتغيير الملفات أو إنشاء ملفات جديدة.

ملاحظة (4): بالإمكان "تشغيل مشاركة محمية بكلمة مرور". وهذا يحصر الوصول إلى المجلد العمومي عبر الشبكة على من يستخدمون حساب المستخدم وكلمة المرور الموجودة على الكمبيوتر.

ملاحظة (5): افتراضيا، يتم "إيقاف تشغيل وصول الشبكة للمجلد العمومي" إلا إذا قمنا بتمكينه.

أي الطريقتين أفضل عند المشاركة:

يجب أن تراعى عوامل عديدة عند الرغبة بمشاركة الملفات من أي مجلد أو من المجلد العمومي.

تتم المشاركة من أي مجلد (الطريقة الأولى) إذا:

1- كنت تفضل مشاركة المجلدات مباشرة من موقع تخزينها (بشكل عام مجلدات المستندات، أو الصور، أو الموسيقي) وترغب في تجنب تخزينها على المجلد العمومي.

2- كنت ترغب في التمكن من تعيين أذونات المشاركة للأفراد بدلا من الجميع على الشبكة، مانحا بعضهم حق وصول أكثر أو أقل (أو عدم الوصول بالمرة).

3- كنت تقوم بمشاركة عدد كبير من الصور الرقمية، والموسيقى، أو ملفات أخرى كبيرة يثقل نسخها لمجلد مشترك منفصل. كنت لا ترغب في استهلاك هذه الملفات مساحة في موقعين مختلفين على الكمبيوتر.

4- كنت تقوم دائما بإنشاء ملفات جديدة أو بتحديث الملفات التي ترغب في مشاركتها وكنت لا ترغب في نسخها إلى المجلد العمومي.

تتم المشاركة من المجلد العمومي (الطريقة الثانية) إذا:

1- كنت تفضل مشاركة الملفات والمجلدات ببساطة من موقع واحد على الكمبيوتر.

2- كنت ترغب في رؤية كافة الأشياء التي قمت بمشاركتها مع الآخرين بسرعة، بمجرد النظر في المجلد العمومي.

3- كنت ترغب في إبقاء كافة الأشياء التي قمت بمشاركتها منفصلة عن مجلدات المستندات، والموسيقى، والصور الخاصة.

4- كنت ترغب في تعيين أذونات المشاركة للجميع على الشبكة، وعدم الاضطرار إلى تعيينها للأفراد.

مركز الشبكة والمشاركة

هو المكان الرئيسي لإدارة كيفية اتصال الكمبيوتر الخاص بك مع بقية شبكات الاتصال ويمكن الوصول لمركز الشبكة والمشاركة كما في المسار التالي:

Control Panel\All Control Panel Items\Network and Sharing Center\Advanced sharing settings

سنتحدث عنه وأهم إعداداته

إن إعدادات المشاركة المتقدمة في نظام Windows 7 تتكون من إعدادين وهما المنزل أو العمل، وآخر هو العام ولكل منهما إعدادات خاصة بالمشاركة كما يوضح ذلك الشكل الأيسر. أما في Windows 10 فأصبح بثلاث ملفات تعريف هي خاص، مضيف أو عام كما يوضح ذلك الشكل الأيسر، جميع الشبكات وهي في الأساس نفس الإعدادات الموجودة في Windows 7 ولكن يتم تقسيمها بشكل منطقي أكثر ومن الإعدادات المختلفة:

فيما يلي لقطات لمحتوى المشاركة المتقدمة في مركز الشبكة والمشاركة:

سنقوم بشرح كافة الخيارات السابقة وفق التالي:

اكتشاف الشبكة: يتم تشغيل هذا الإعداد للشبكات الخاصة افتراضياً وهذا يعني أنه يمكن للحاسوب الخاص بك أن يراه الحاسوب الآخر والعكس صحيح.

مشاركة الملفات والطابعات: سيسمح هذا الإعداد للآخرين بالوصول إلى المجلدات والطابعات المشتركة على جهاز الحاسوب الخاص بك.

اتصالات مجموعة المشاركة المنزلية: إذا كنت تريد بالفعل مشاركة الملفات والمجلدات، يجب عليك فقط إعداد مجموعة المشاركة المنزلية HomeGroup فإن مجموعة المشاركة المنزلية عبارة عن مجموعة من أجهزة الحاسوب الموجودة على شبكة منزلية واحدة والتي يمكنها مشاركة الملفات والطابعات فيما بينها حيث يمكنك حماية مجموعة المشاركة المنزلية الخاصة بك باستخدام كلمة مرور يمكنك تغييرها في أي وقت ولا يمكن للمستخدمين الآخرين تغيير الملفات التي تقوم بمشاركتها إلا عند منحهم الإذن بذلك وهو أكثر أمانًا وأكثر سهولة في التهيئة.

مشاركة المجلد العمومي : يجب إيقاف هذا الإعداد ما لم تكن بحاجة إلى تبادل البيانات مع جهاز حاسوب آخر ويرجع السبب في ذلك إلى أنه من السهل جدًا حفظ الملفات بطريق الخطأ في هذه المجلدات المشتركة بشكل عام

دون إدراكها، والتي يمكن لأي شخص على الشبكة الوصول إليها فهي ميزة مفيدة جدًا عندما تحتاج إليها، ولكن هناك خطر كبير في الخصوصية بخلاف ذلك.

دفق وسائط: هذا خيار آخر يجب أن يظل معطلًا حتى تحتاج إلى استخدامه و يؤدي هذا بشكل أساسي إلى تحويل الحاسوب الخاص بك إلى خادم DLNA بحيث يمكنك دفق الموسيقى والأفلام والصور إلى الأجهزة الأخرى على الشبكة عندما يتم تمكينه فإنه يفتح أيضًا عددًا قليلاً من المنافذ في جدار الحماية أيضًا.

اتصالات مشاركة الملفات: يقوم بحماية اتصالات مشاركة الملفات فيجب تعيين هذا الخيار دائمًا على استخدام تشفير 128 بت ما لم تكن بحاجة إلى مشاركة الملفات مع أجهزة Windows 95 أو Windows 98 أو Windows 2000.

مشاركة محمية بكلمة مرور: نوصي بشدة بتشغيل مشاركة محمية بكلمة مرور لأنها ستجبر المستخدمين على إدخال اسم مستخدم وكلمة مرور لحساب على الكمبيوتر للوصول إلى أي بيانات.

برنامج CrypTool 1.4.41

برنامج CrypTool 1.4.41 هو برنامج تعليمي تم إعداده من قبل جامعة ألمانية بهدف تمكين الطلاب من تنفيذ عمليات التشفير والحماية بطريقة سهلة وواضحة.

في هذه الجلسة سنستعرض بعض خوارزميات التشفير الكلاسيكي من حيث مبدأ عملها، وتطبيقها رياضيا، ثم تطبيقها على برنامج CrypTool.

أولاً: التشفير وفك التشفير باستخدام خوارزمية قيصر Caesar:

مبدأ عمل خوارزمية قيصر:

إن التشفير بالإزاحة يعتمد على مبدأ إزاحة حرف من حروف الرسالة plain text بمقدار معين (المفتاح) ولفك التشفير نقوم بالفعل المعاكس.

فتكون معادلة التشفير:

$$C=M + K \bmod 26$$

ومعادلة فك التشفير:

$$M=26+C - K \bmod 26$$

حيث:

C: رقم خانة الحرف بعد التشفير بالأبجدية.

M: رقم خانة العدد بعد فك التشفير بالأبجدية.

K: مفتاح التشفير (مقدار الإزاحة).

خوارزمية قيصر هي أول خوارزمية بالإزاحة حيث كانت تعتمد على الإزاحة بمقدار ثلاث حروف أي أن المفتاح K=3. ثم أصبحت تطبق على أي قيمة إزاحة. إذا كانت الازاحة بمقدار 13 فتسمى الخوارزمية بـ Rot-13.

تطبيق خوارزمية قيصر رياضياً

ليكن لدينا النص الواضح (Plain Text) التالي: M=" WE WELL MEET AT NIGHT"

والمطلوب تشفير النص M باستخدام خوارزمية قيصر بإزاحة 3 حروف

الحل:

نعطي كل حرف رقم كما في الشكل:

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

نحول الأحرف في النص الأصلي إلى ما يقابلها من أرقام:

W	E	W	I	L	L	M	E	E	T	A	T	N	I	G	H	T
22	4	22	8	11	11	12	4	4	19	0	19	13	8	6	7	19

ثم نقوم بتشفير كل حرف بحسب خوارزمية قيصر بالقانون التالي:

C1=22 +3 MOD 26 = 25 ➔ Z

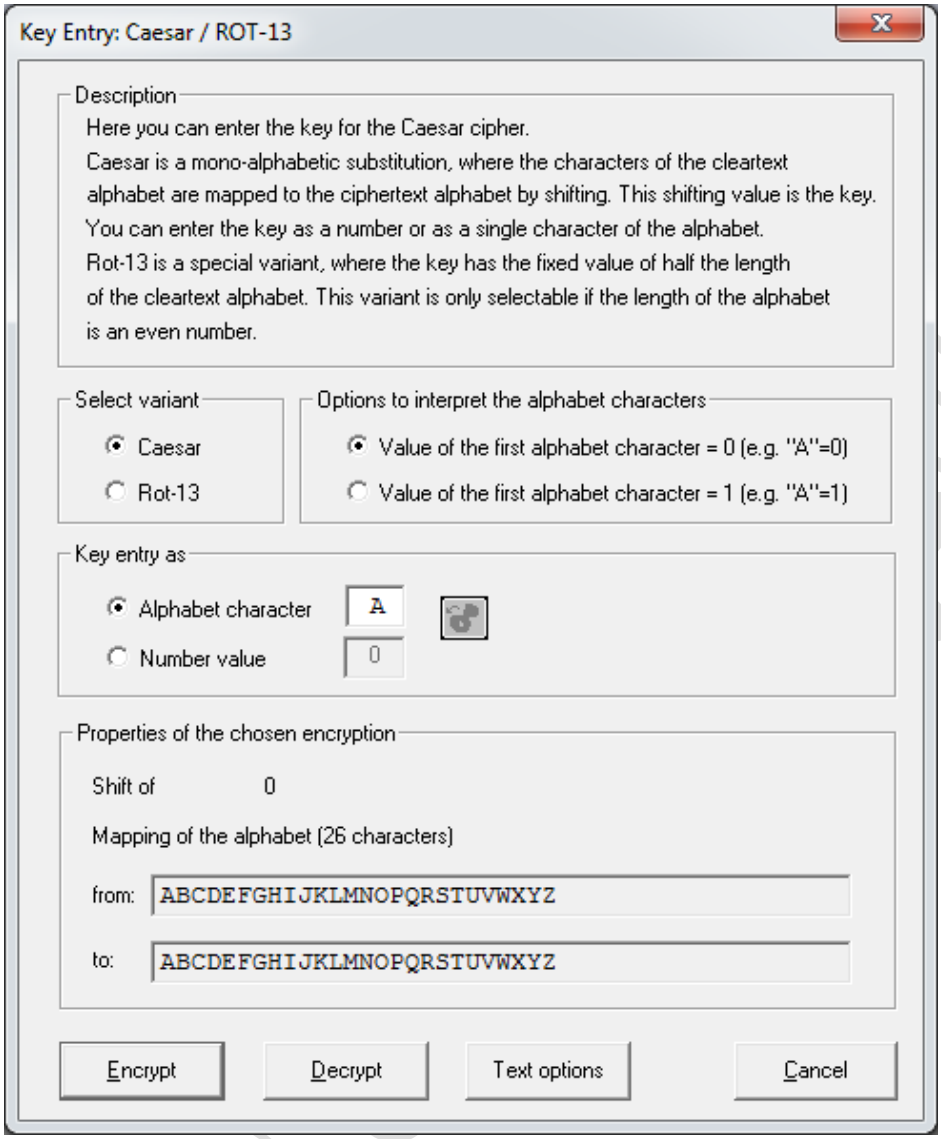
C2=4 + 3 MOD 26 = 7 ➔H

نتابع حتى نحصل على النص المشفر التالي:

ZH ZLOO PHHW DW QLJKW

تطبيق خوارزمية قيصر باستخدام برنامج Cryptool:

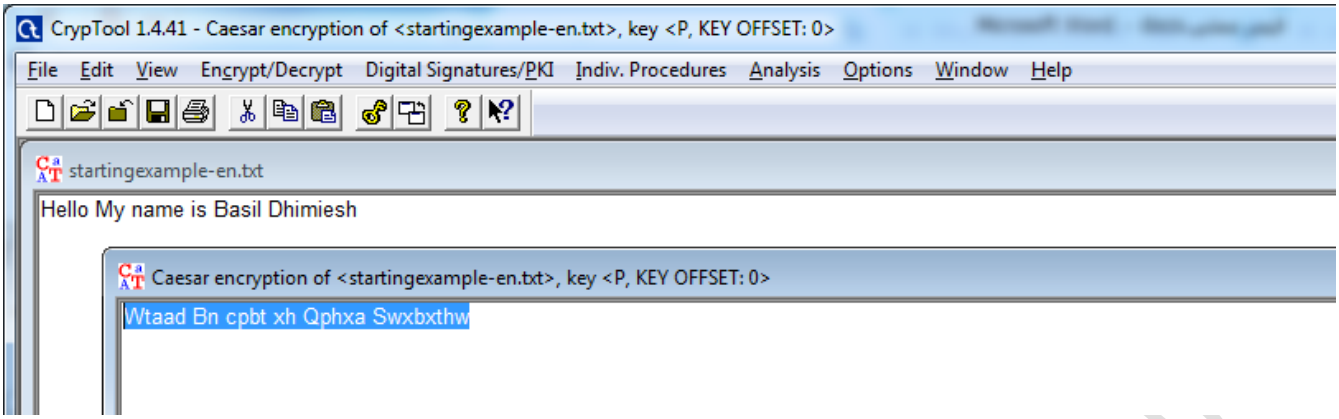
سنقوم بتشفير نص ثم فك تشفيره ثم سندع للبرنامج اكتشاف المفتاح. سنقوم أولا بكتابة نص وليكن Hello My name is Basil Dhimiesh، ثم سنختار التبويبة Encrypt/Decrypt ثم Symmetric (classic) ثم Caesar/Rot-13. ستظهر النافذة التالية:



المفتاح المدخل هو بمقدار الحرف A. إذا اعتبرنا أن ترقيم الحروف يبدأ من 0 عندها لن يكون هناك ازاحة وبالتالي سيتساوى النص المشفر مع النص الصريح، أي أن الحرف C قبل التشفير هو الحرف C نفسه بعد التشفير كما هو واضح في الشكل السابق، أما إذا اعتبرنا أن ترقيم الحروف يبدأ من 1 عندها سيكون مقدار الإزاحة الفعلية هو 1، أي أن الحرف C قبل التشفير هو الحرف D بعد التشفير.

تدريب: ما مقدار الإزاحة الفعلية إذا كان المفتاح المدخل بمقدار P، وبدأ ترقيم الحروف من 0؟

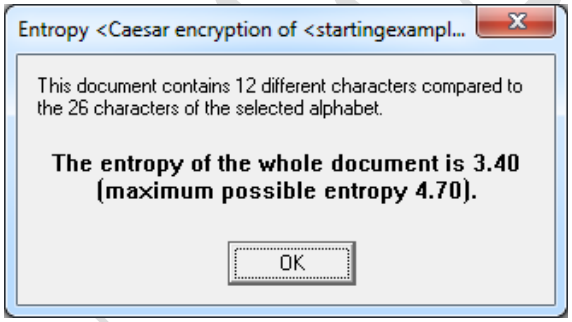
بعد اختيار ازاحة المفتاح ولتكن 15 مثلاً نقوم بالضغط على زر Encrypt لنحصل على الناتج المشفر Wtaad Bn cpbt xh Qphxa Swxbxthw كما هو واضح بالشكل:



لا تقوم خوارزمية قيصر بتشفير الرموز والفراغات.

من أجل فك التشفير نتبع نفس الخطوات السابقة من التبويبة Encrypt/Decrypt ثم Symmetric (classic) ثم Caesar/Rot-13. ندخل المفتاح وننقر على Decrypt.

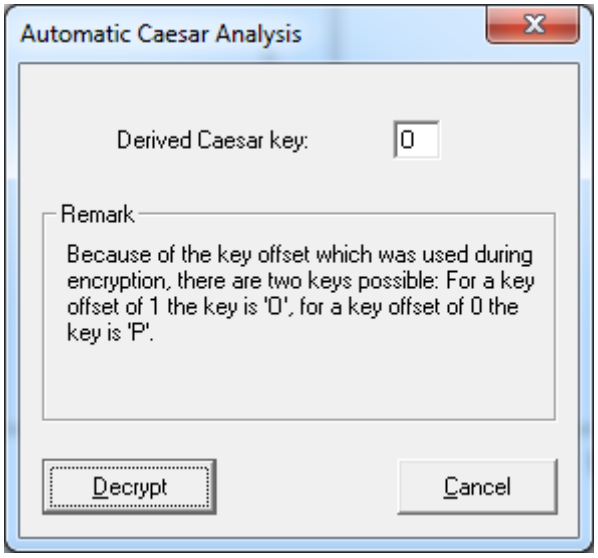
لإيجاد درجة عشوائية النص entropy نذهب إلى تبويبة Analysis ثم Tools of Analysis ثم Entropy، وبالطبع كلما كان النص متنوعاً بالحروف كلما كانت درجة العشوائية مرتفعة. الدرجة العظمى للعشوائية هي 4.70 نلاحظ أن عشوائية النص الصريح هي نفسها عشوائية النص المشفر وهي 3.40 في مثالنا.



نوجد الرسم البياني لتكرار الحروف في النص المشفر حيث نختار Analysis ثم Tools of Analysis ثم Histogram.

بفرض أننا نريد استنتاج ومعرفة المفتاح بطريقة غير شرعية:

نطبق التحليل الاحصائي للتراكيب من تبويبة Analysis ثم Symmetric Encryption (Classic) ثم ciphertext-only ثم Ceaser فينتج أن المفتاح هو الحرف O إذا اعتبرنا أن ترقيم الحروف يبدأ من 1، أو P بحال اعتبرنا أن ترقيم الحروف يبدأ من 0.



ثانياً: التشفير وفك التشفير باستخدام خوارزمية Atbash:

مبدأ عمل خوارزمية Atbash:

للتشفير باستخدام خوارزمية Atbash نقوم بكتابة حروف الأبجدية كاملة بشكل معاكس – أي بترتيب تنازلي – بحيث يصبح الحرف الأول هو الحرف الأخير والحرف الثاني يصبح الحرف ما قبل الأخير وهكذا ...

تطبيق خوارزمية Atbash رياضياً:

قم بتشفير النص M="hello world" باستخدام خوارزمية Atbash

الحل:

نقوم ترتيب الحروف الأبجدية تنازليا كما يلي:

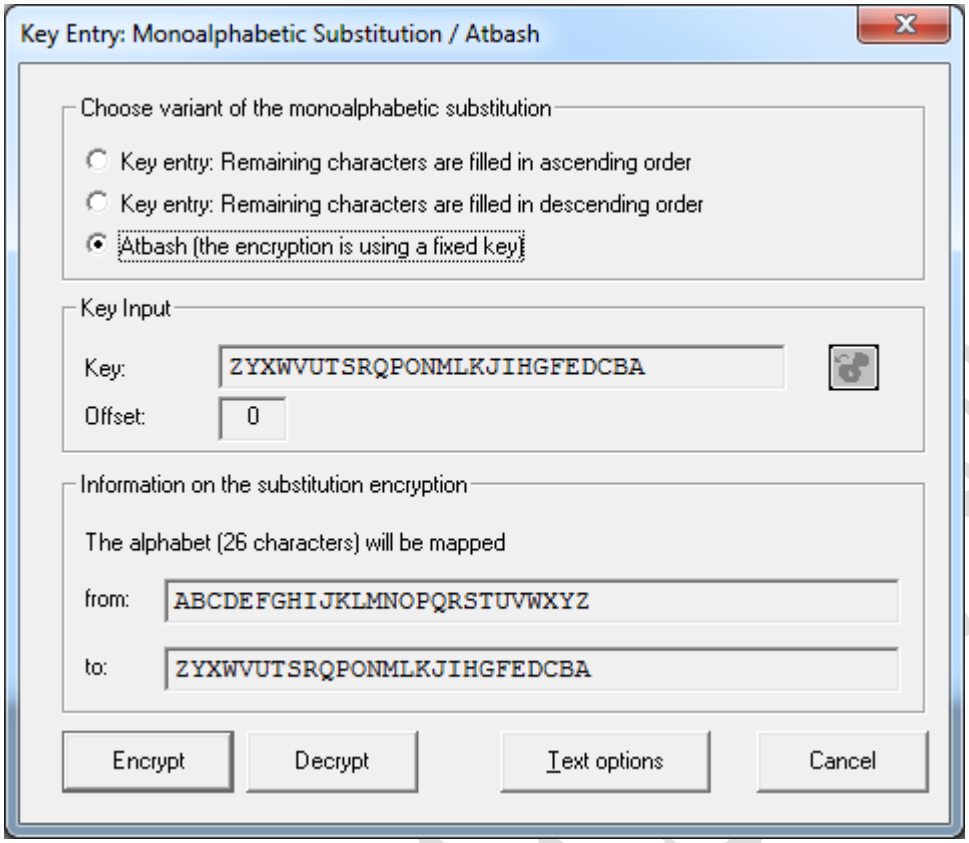
Plain	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Cipher	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A

ثم نقوم بالمقابلة فيصبح النص المشفر كالتالي: C="svool dliow"

تطبيق خوارزمية Atbash باستخدام برنامج Cryptool:

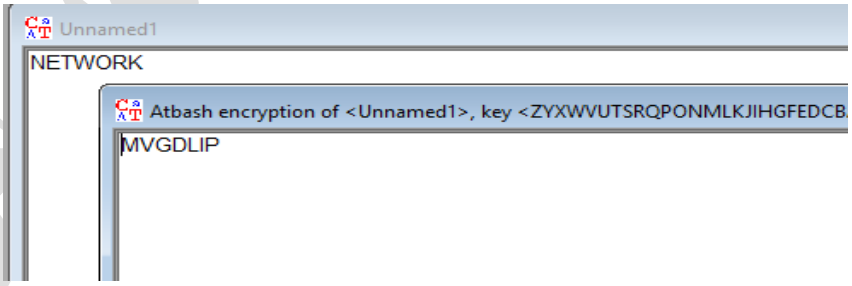
من تبويبة Encrypt/Decrypt ونقوم باختيار الخوارزميات المتناظرة الكلاسيكية Symmetric ثم نختار substitution/Atbash

فيظهر لنا مربع الحوار التالي نقوم بوضع الخيار على Atbash حيث يعطي مفتاح ثابت وهو عبارة عن الترتيب العكسي للأبجدية ثم ننقر على زر Encrypt

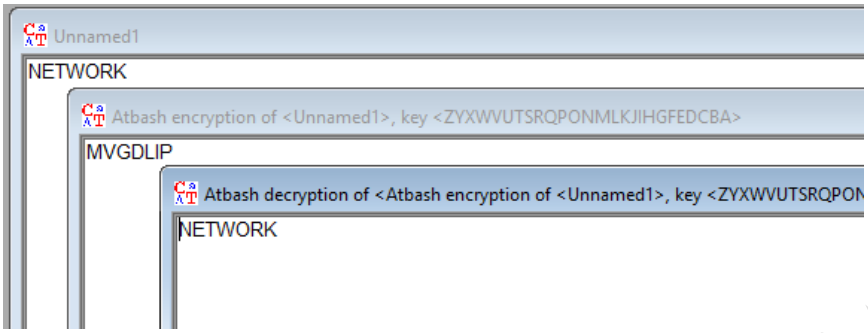


ملاحظة: يمكن من نفس النافذة السابقة استخدام التشفير بواسطة جملة تشفير، فالخيار Key entry: Remaining characters are filled in ascending order يعني أن الحروف المتبقية بعد كتابة المفتاح ترتب تصاعدياً، أما الخيار Key entry: Remaining characters are filled in descending order يعني أن الحروف المتبقية ترتب تنازلياً.

بعد الضغط على زر encrypt نحصل على النص المشفر التالي:



ولفك التشفير نتبع نفس الخطوات السابقة على النص المشفر ثم الضغط على decrypt فنحصل على النص الأصلي:



ثالثاً: التشفير وفك التشفير باستخدام خوارزمية هيل (Hill):

مبدأ عمل خوارزمية هيل:

في خوارزمية Hill يكون المفتاح عبارة عن كلمة مفتاحية يتم تحويلها إلى مصفوفة من نمط m*m القابلة للقلب فمن أجل مفتاح ما نعرف:

$E(x)=x\ K$ $D(y)=Y\ K^{-1}$

- حيث كل العمليات تنجز في Z_{26}
- حتى نستطيع فك التشفير في Hill يجب أن يكون للمصفوفة K مقلوب
- أن تكون المصفوفة المربعة قابلة للقلب وأن يكون المحدد لها لا يساوي الصفر أي $det(A)\neq 0$، حيث تكون المصفوفة المربعة A قابلة للقلب إذا وفقط إذا كان $gcd(det(A),26)=1$.
- في هذه الخوارزمية نأخذ m حرف أبجدي في عنصر واضح من أجل إعطاء m حرف ابجدي في عنصر مشفر واحد.
- نستخدم التابع mod 26 في حال كانت النتائج أكبر من 26، ونتخلص من العدد السالب بإضافة 26.

تطبيق خوارزمية هيل رياضياً:

لنفرض أن المفتاح هو $K=\begin{matrix}11 & 8\\ 3 & 7\end{matrix}$ المطلوب تشفير النص الواضح JULY من خلال خوارزمية HILL.

أولاً سنقوم بتحويل حروف النص الأصلي إلى الأرقام المقابلة :

J	U	L	Y
9	20	11	24

نقوم بتشفير كل حرفين من النص الأصلي سوياً وذلك من مرتبة مصفوفة المفتاح 2*2

J	U
9	20

L	Y
11	24

التشفير يكون كالتالي :

$\begin{pmatrix}11 & 8\\ 3 & 7\end{pmatrix}\begin{pmatrix}9\\ 20\end{pmatrix}$ =(11*9+8*20 3*9+7*20)=(259 167)mod 26=(25 11) = Z L

$\begin{pmatrix}11 & 8\\ 3 & 7\end{pmatrix}\begin{pmatrix}11\\ 24\end{pmatrix}$ =(11*11+8*24 3*11+7*24)=(313 201)mod 26=(1 19) = B T

وبالتالي تشفير النص الأصلي JULY هو ZLBT .

من أجل فك التشفير يتطلب حساب مقلوب $K=\begin{matrix}11 & 8\\ 3 & 7\end{matrix}$ (أي حساب K^{-1})

Det(K)=$\begin{pmatrix}11 & 8\\ 3 & 7\end{pmatrix}$ =77-24 mod 26= 53 mod 26= 1≠ 0

بما أن det(K) ≠ 0 فإن مقلوب k يتحدد بالخطوات التالية:

- نبدل كل عنصر بمتممه الجبري.

$\begin{pmatrix}11 & 8\\ 3 & 7\end{pmatrix}$ ➔ $\begin{pmatrix}7 & -3\\ -8 & 11\end{pmatrix}$

- نوجد منقول المصفوفة الناتجة (أبدل كل سطر بعمود).

$\begin{pmatrix}7 & -8\\ -3 & 11\end{pmatrix}$

- نقسم المصفوفة الناتجة على المحدد.

1/1 $\begin{pmatrix}7 & -8\\ -3 & 11\end{pmatrix}$ ➔ $K^{-1}=\begin{pmatrix}7 & -8\\ -3 & 11\end{pmatrix}$

ولكن بما أن المصفوفة تحوي على أعداد سالبة فنقوم بإيجاد mod 26:

$k^{-1}=\begin{pmatrix}7 & -8\\ -3 & 11\end{pmatrix}$ mod 26 = $\begin{pmatrix}7 & 18\\ 23 & 11\end{pmatrix}$

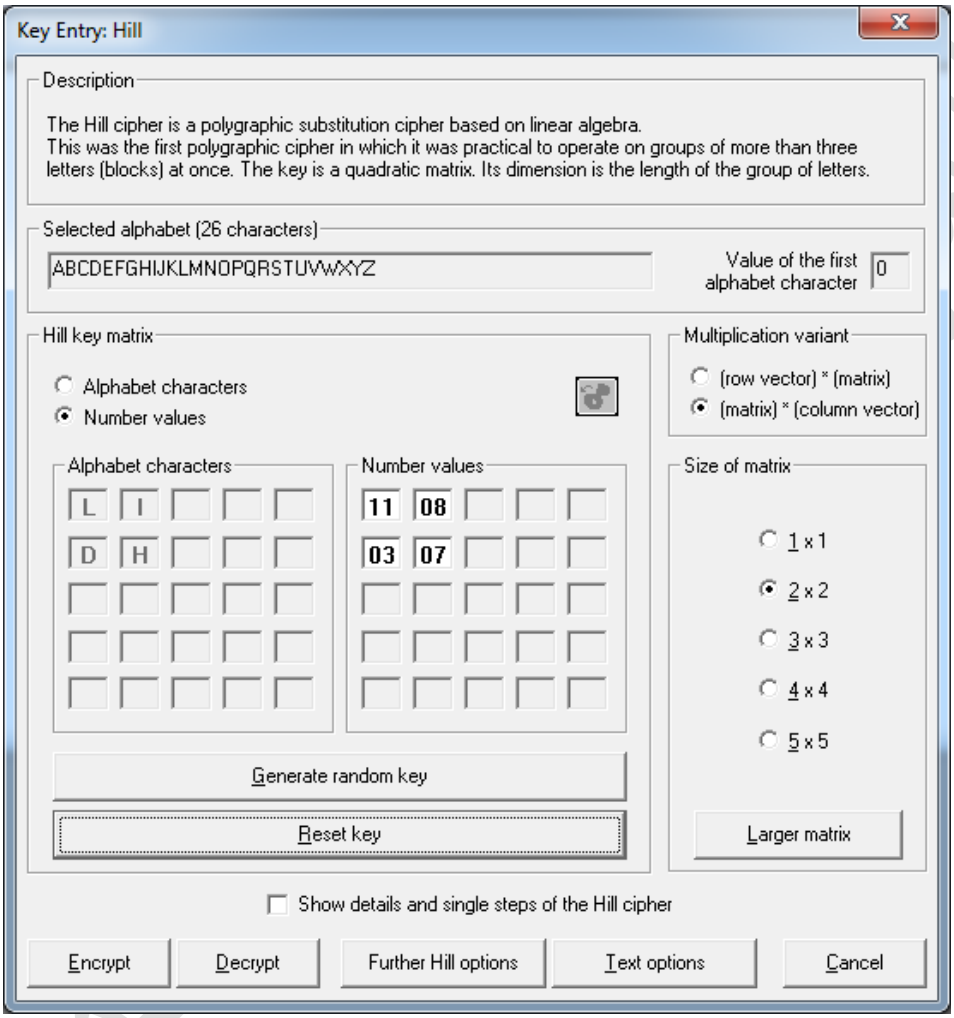
الآن لفك التشفير نستخدم القانون التالي: $D(y)= K^{-1}Y$

$\begin{pmatrix}7 & 18\\ 23 & 11\end{pmatrix}\begin{pmatrix}25\\ 11\end{pmatrix}$ =(7*25+18*11 23*25+11*11) =(373 696)MOD 26 = (9 20)= J U

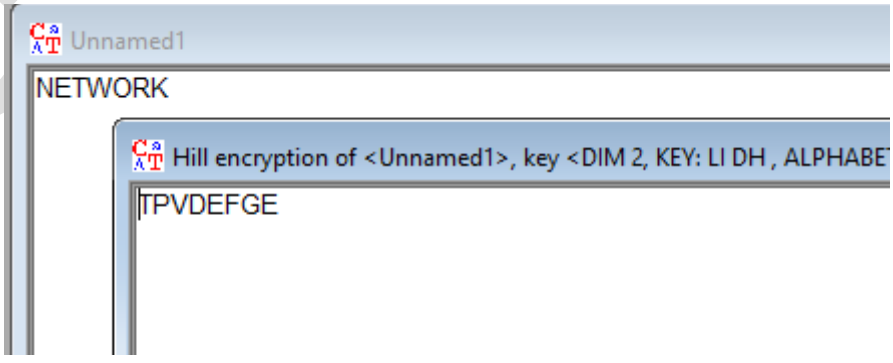
$\begin{pmatrix}7 & 18\\ 23 & 11\end{pmatrix}\begin{pmatrix}1\\ 19\end{pmatrix}$ =(7*1+18*19 23*1+11*19) =(349 232)MOD 26 = (11 24)= L Y

تطبيق خوارزمية Hill باستخدام برنامج Cryptool:

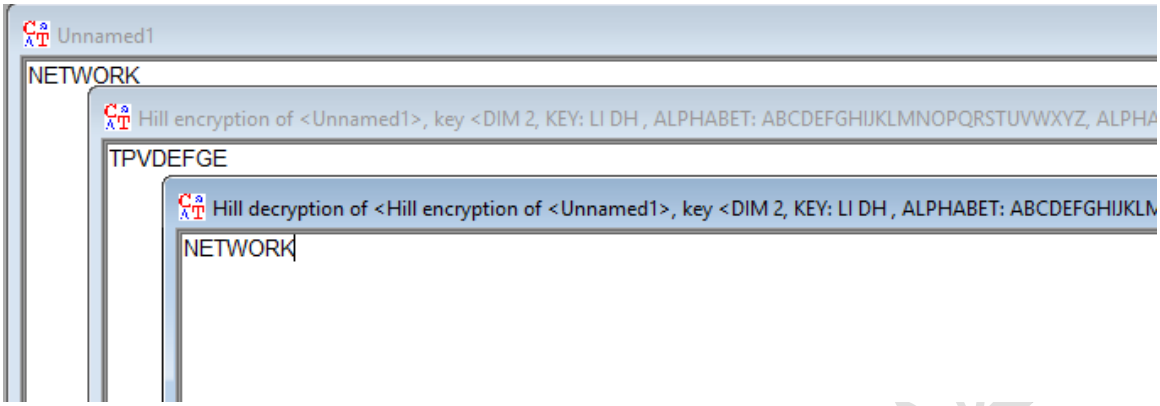
من تبويبة Encrypt/Decrypt ونقوم باختيار الخوارزميات المتناظرة الكلاسيكية Symmetric ثم نختار Hill فيظهر لنا مربع الحوار التالي نقوم باختيار بارامترات خوارزمية HILL وهي تحديد مرتبة المصفوفة المربعة M*M وتحديد عناصر المصفوفة المفتاح إما أحرف أبجدية ككلمة مفتاحية أو أرقام كمصفوفة عددية ثم ننقر على زر Encrypt



فنحصل على النص المشفر التالي:



من أجل فك التشفير نتبع نفس الخطوات السابقة من تبويبة Encrypt/Decrypt ونقوم باختيار الخوارزميات المتناظرة الكلاسيكية Symmetric واختيار خوارزمية Hill ثم نحدد المفتاح وننقر على Decrypt



رابعاً: التشفير وفك التشفير باستخدام خوارزمية بلايفير Playfair:

هي من الخوارزميات التقليدية وتعتمد على مبدأ تشفير كل حرفين من النص الأصلي معاً ولكن المقصود هنا ليس استبدال كل حرفين بحرف وإنما الحرف الواحد يتغير تشفيره ضمن النص بتغيير الحرف المصاحب له.

تعتمد هذه الخوارزمية على بناء جدول بأبعاد 5*5 بكل خانة نضع حرف واحد فقط وبالنسبة للغة الانكليزية بما أنه لدينا 26 حرف فإننا نأخذ بالاعتبار ونفرض أن حرف J هو نفسه حرف i

تطبيق خوارزمية بلايفير رياضياً:

- إذا كان لدينا النص الأصلي الذي نريد تشفيره هو m="TO NIGHT IS NOT POSSIBLE" المفتاح هو عبارة عن الكلمة k="codes" والتي من الأفضل ألا تحتوي على حروف مكررة وفي حال احتوائها نحافظ على أول تكرار ونقوم بحذف ما تم تكراره.
- نقوم بوضع المفتاح في الجدول من اليسار إلى اليمين و من ثم بقية الخانات نملأها بالأحرف الأبجدية المتبقية بالترتيب.

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

من أجل التشفير نقوم بتقسيم النص الأصلي إلى ثنائيات كالتالي ونقوم بالتعويض عن كل تكرار بحرف x :

TO NI GH TI SN OT PO SX SI BL EX

الآن إذا كان الحرفان في نفس السطر ضمن الجدول نقوم باستبدال كل منهما بالحرف الذي على يمينهما، أي تشفير الثنائية NI هي IK:

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

إذا كان الحرفان في نفس العمود ضمن الجدول نقوم باستبدال كل حرف منهما بالحرف الذي أسفل منه أي تشفير DL هو FR

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

إذا كان الحرفان غير مشتركين لا بالسطر ولا بالعمود نقوم بأخذ ما يقابل الثنائي بنفس سطر الأول أي مثلاً تشفير TO هو QE

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

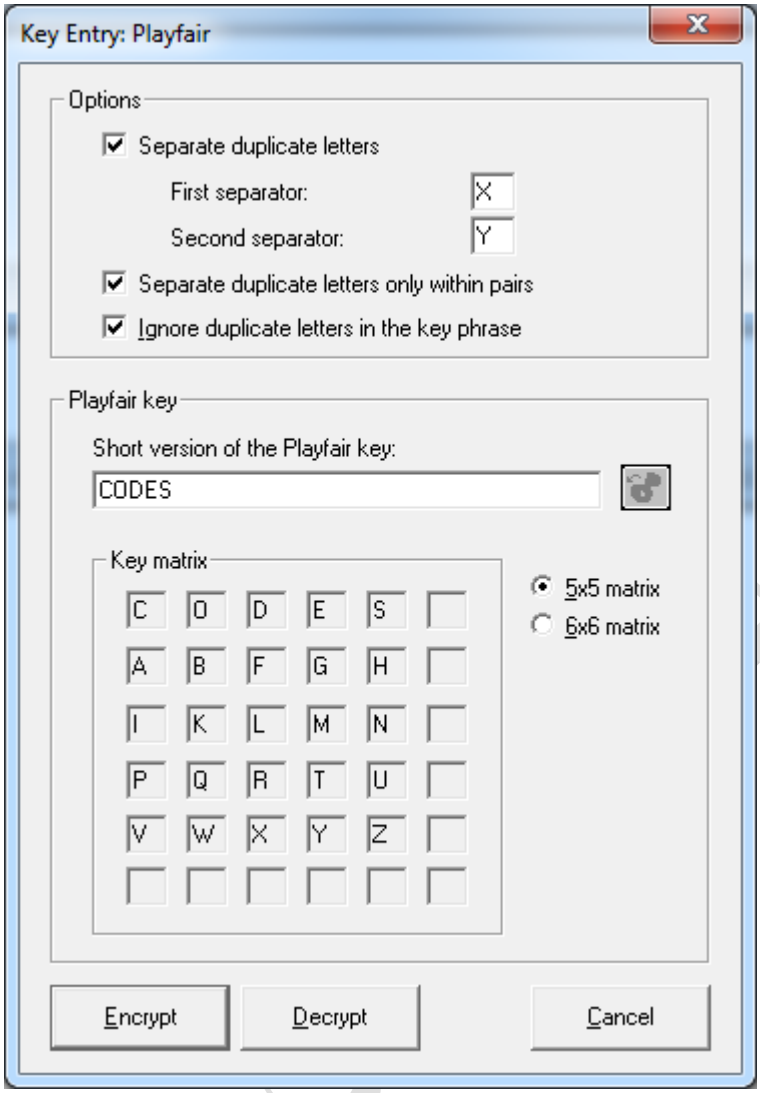
في النهاية نجمع كل ثنائيتان بعد التشفير لنحصل على النص المشفر.

C="QE IK HA PM HU EQ QC DZ CN FK DY"

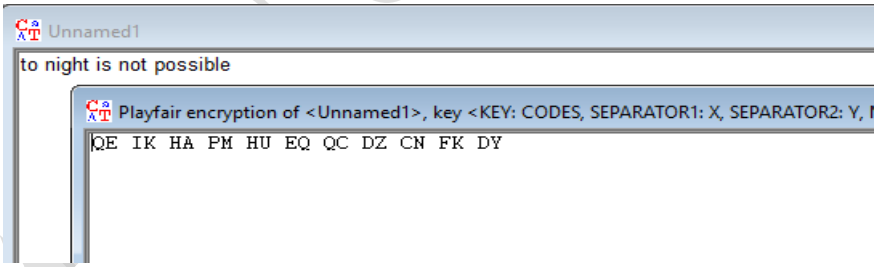
ولفك التشفير نحوله الى ثنائيات و نعود بحركات معاكسة ضمن الجدول.

تطبيق خوارزمية بلايفير باستخدام برنامج Cryptool:

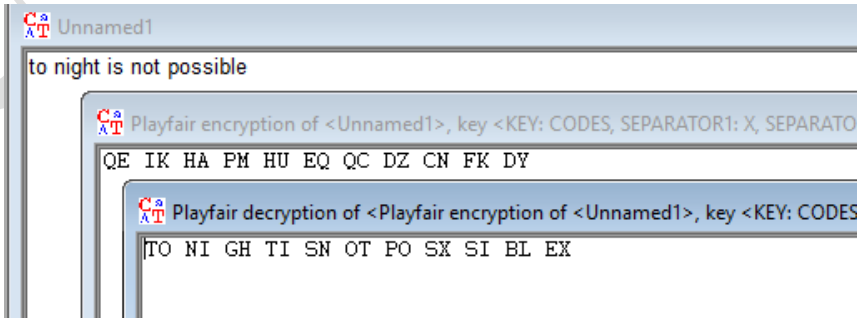
من تبويبة Encrypt/Decrypt ونقوم باختيار الخوارزميات المتناظرة الكلاسيكية Symmetric ثم نختار playfair نقوم بتحديد كلمة المفتاح واختيار الجدول بأبعاد 5*5 وننقر على Encrypt.



فنحصل على النص المشفر التالي :



ولفك التشفير نتبع نفس الخطوات السابقة فنستطيع استعادة النص الأصلي:



الشبكات المحلية اللاسلكية WLAN[5]

تطورت الشبكات اللاسلكية وانتشرت انتشار واسعاً في الفترة الأخيرة ومن المتوقع زيادة انتشارها إلى حد كبير بعد تزايد المنتجات اللاسلكية في أجهزة الحاسوب من الفأرة ولوحة المفاتيح والكاميرا الرقمية وغيرها من المعدات التي تزداد يوم وراء يوم وتتزايد تطبيقات الاتصال اللاسلكي من نقط الوصول في المطارات والاستراحات والصالات وقاعات الاجتماعات والأماكن العامة.

بدأ تطوير تكنولوجيا الشبكات اللاسلكية عن طريق عمل جماعي لمجموعة من المصنعين في محاولة لتلبية طلبات محدودة قاصرة على إنشاء تلك الشبكات من أماكن يصعب بها إنشاء الشبكات السلكية لذلك كانت بداية تكنولوجيا الشبكات اللاسلكية بطيئة وباهظة التكاليف. ومع ازدياد استخدام الحاسوب النقال (Laptop) وكثرة الإقبال عليه من قبل الموظفين وأصحاب الأعمال أو حتى مستخدمي المنازل ازدادت الرغبة في استخدام التوصيلات اللاسلكية أو بالأصح الشبكات اللاسلكية:.

يقصد بمصطلح الشبكات اللاسلكية توصيل جهازي حاسوب أو أكثر يبعضهما عن طريق بروتوكول اتصال قياسي، سواء كان TCP/IP وغيره، دون الحاجة إلى استخدام كابلات لتحقيق الاتصال بين كل ما هو موجود من تكنولوجيا وأجهزة.

يتزامن انتشار الشبكات مع انتشار السرعات العالية لاستخدام الانترنت، حيث بالإمكان استخدام هذه السرعة فيتم توزيعها على أكثر من جهاز.

وبما أن مستخدمي الشبكات المنزلية في ازدياد، وأعداد الأجهزة تزداد أيضاً، فإن ذلك يسبب تزاحم بين الأسلاك مما قد يزعج بعض المستخدمين، خاصة إذا كانت تلك الشبكة شبكة موسعة تحوي أكثر من جهاز.

قد يعتقد البعض أن عملية استخدام الشبكة اللاسلكية هي عملية صعبة ومعقدة وتحتاج إلى خبراء حتى يقومون بها، على العكس .. فهي تشبه شبكات الكبل في عملية التنصيب وغيره، غير أنها تحتاج خطوات معينة قد لا تكون موجودة في شبكات الكبل.

أصبحت الشبكات اللاسلكية متداولة وبكثرة، خاصة خارج مجال الحاسوب، فتقنية Infrared الموجودة في الهواتف النقالة هي عبارة عن شبكة لاسلكية، وأيضاً تقنية Bluetooth تعتبر شبكة لاسلكية، لكن الاثنتين شبكات بسيطة جداً، حيث أن مداها صغير، وأيضا سرعة نقل البيانات بطيئة، ولذلك هي تستخدم في الهواتف النقالة و Pocket PC، وسائر الأجهزة الصغيرة والكفية..

أما الحواسيب، فهي تحتاج إلى تقنية أعلى، يصل مداها إلى ابعد من الشبكيتن أعلاه، وأيضاً تكون سرعة نقل البيانات أكبر .. والتقنية التي يستخدمها الحاسوب في شبكاته اللاسلكية تسمى: Wi-Fi.

[5] عرّف معهد IEEE عائلة معايير IEEE 802.3 لشبكات Ethernet LAN، بينما عرّف معيار IEEE 802.11 لشبكات WLAN.

ايجابيات الشبكات اللاسلكية:

- **ميسورة التكلفة.** نظرًا لأن الشبكة اللاسلكية تلغي نفقات الأسلاك أو تقلّلها؛ فإنها تتميز بتكلفة أقل عند التركيب، والتشغيل، والتوسيع مقارنةً بالشبكات السلكية.
- **الوصول المريح.** تمتع بالوصول إلى موارد الشبكة من أي مكان في نطاق التغطية اللاسلكية للشبكة، مثل غرفة الاجتماعات، أو من أي نقطة اتصال لاسلكية عامة.
- **سهولة الإعداد والتوسيع.** باستخدام الشبكات اللاسلكية، ليست هناك حاجة إلى الكابلات السلكية لتوصيل أجهزة الحاسوب والطابعات والأجهزة الأخرى، أو الاتصال بالإنترنت. كما أصبحت إضافة مستخدمي حاسوب جدد إلى الشبكة من الأمور البسيطة جدًا.
- **سهولة الاستخدام:** الشبكات اللاسلكية سهلة الإعداد والاستعمال فببرنامج مساعد تستطيع تجهيز Laptop أو Desktop ببطاقة شبكة اتصالات لاسلكية وهناك حواسب مجهزة بهذه البطاقة مثل أجهزة سنترينو.

سلبيات الشبكات اللاسلكية:

إن الشبكات اللاسلكية تكون غالباً أبطأ من الشبكات الموصولة مباشرةً باستخدام تقنيات الإيثرنت Ethernet عبر الكابلات. هذه السلبيات هي:

- الجدران والمسافة الطويلة تعيق من عمل الشبكة، لذلك ستحتاج إلى أكثر access point
- التداخل مع الإشارات الميكروية
- الأسطح المعدنية تؤثر سلباً على الشبكات اللاسلكية.

معايير الشبكات اللاسلكية المحلية (WLAN Standards):

عرفت اللجنة الاستشارية لسياسة المعايرة الوطنية US-NSPAC في العام 1978 المعايرة بشكل عام بأنها:

"مجموعة محدده مسبقا من القواعد، الشروط أو المتطلبات المتعلقة بتعريف المصطلحات، تصنيف المكونات، تحديد المواد، الأداء أو الإجراءات، تخطيط العمليات، القياسات الكميه أو الجودة لتوصيف المواد، المنتجات، الأنظمة، الخدمات أو الممارسة. "

1- معيار IEEE 802.11 : تتطلب معدات الاتصال اللاسلكية استخدام نوع من أنواع التكنولوجيا ذات معايير معينة تمكنها من التعامل مع ترددات الراديو بطريقة تضاهي طريقة نقل البيانات، والأكثر استخداما في ذلك هي ما يطلق عليها 802.11 التي أنتجت بواسطة خبراء متخصصين في هذا المجال من معهد مهندسي الكهرباء والالكترونيات IEEE ويعرّف هذا النظام جميع جوانب الاتصال اللاسلكي.

ويقدم هذا المعيار بعدة خدمات منها الخدمات التالية:

1. التوزيع: بإيصال الإطار إلى الشخص المرغوب حالما يقبل الإطار المرسل من نقطة الوصول.
2. التكامل: وذلك بالسماح للاتصالات التي تأتي من شبكات لاتعتمد المعيار IEEE 802.11
3. التوثيق والتحقق: بضمان هوية المستخدم المتصل بالشبكة.
4. ضمان الخصوصية بين مستخدمي الشبكة.

2- معيار تحالف Wi-Fi (Wi-Fi Alliance Standards):

Wi-Fi هي علامة تجارية مرخصة يمنحها تحالف Wi-Fi للمنتجات المتطابقة مع متطلبات التوافقية و إمكانية التشغيل بين المنتجات التي تعتمد على معيار، IEEE 802.11 بعبارة أخرى فإن شبكة Wi-Fiهي شبكه متوافقة مع المعيار IEEE 802.11. يستخدم الاسم Wi-Fi حالياً علي نطاق واسع للإشارة إلى الشبكات اللاسلكية عوضاً عن IEEE 802.11.

3- منظمة ITU-R:

هي منظمة عالمية مختصة بإدارة توزيع النطاقات الترددية.

القنوات (Channels):

يمكن تقسيم المجال الترددي إلى عدد من القنوات الترددية و تستخدم كل قناة كوصلة اتصال يتم عبرها إرسال و استقبال المعلومات بحيث يتم تعيين قيمة ترددية و عرض نطاق ترددي محدد لكل قناة و يراعى تحديد فاصل ترددي كاف بين القنوات المتقاربة تفاديا للتداخل

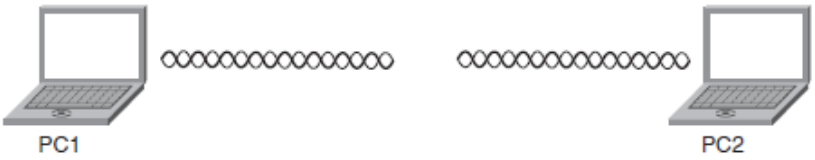
المعايير المستخدمة في شبكات WLAN:

IEEE 802.11	الترددات	معدل نقل البيانات	عدد القنوات المتاحة	القنوات غير المتداخلة
802.11a	5 GHZ	54 mbps	23	12
802.11b	2.4 GHZ	11 mbps	14	3
802.11g	2.4 GHZ	54 mbps	14	3
802.11n	5 GHZ	750 mbps	14	3

أنماط الشبكة اللاسلكية:

1- Independent Basic Service Set- IBSS : وتعرف بـ ADHOC وهي كلمة لاتينية قديمة معناها for" this" أو "لهذا" و هي طوبولوجية لاسلكية لمعايير 802.11 نحتاج اليها عندما يريد جهاز الاتصال بجهاز آخر

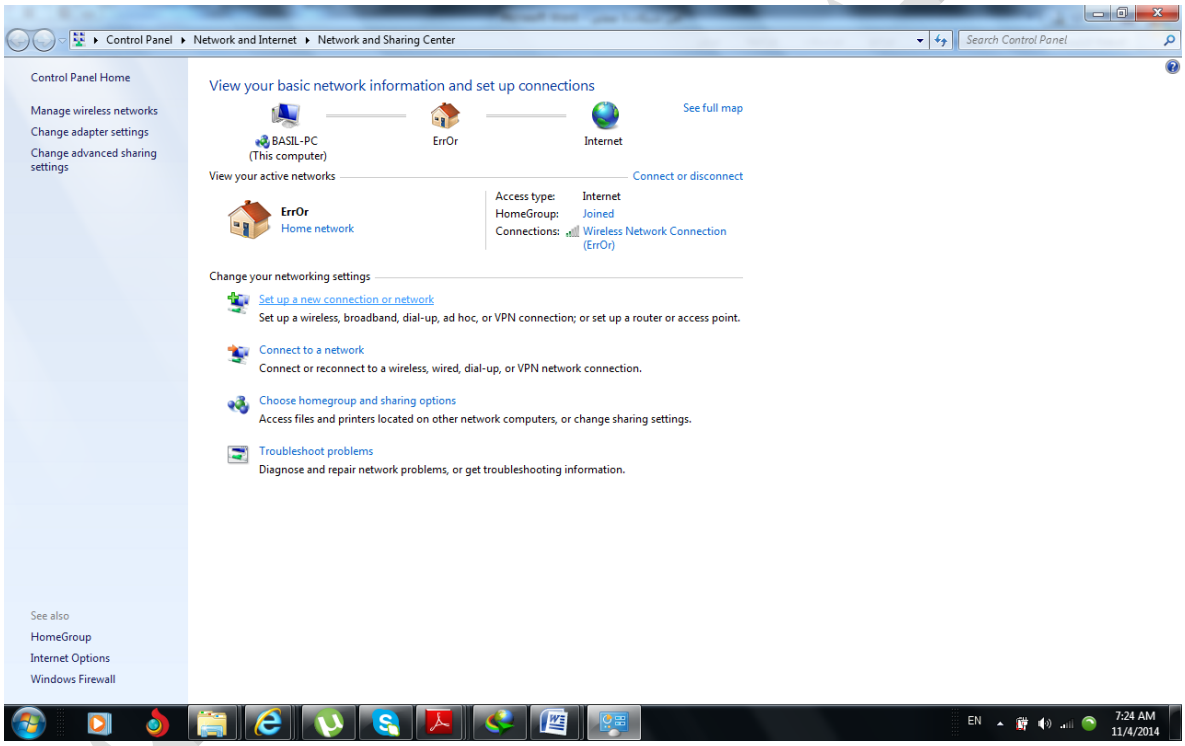
بدون الحاجة إلى جهاز وسيط حيث يقوم أحد الجهازين بعمل مجموعة العمل و تحديد لبارمترات الإرسال (radio parameters) مثل SSID[6] و أسلوب الأمن و التوثيق ثم يقوم الآخر بطلب الاتصال طبقا للبرامترات التي وضعها الجهاز الأول. وهذه العملية تسمي Independent basic service set IBSS حيث لا يعتمد الاتصال علي جهاز وسيط. كما يبين ذلك الشكل (1)



الشكل (1)

لإعداد شبكة بهذا النمط علينا إتباع الآتي:

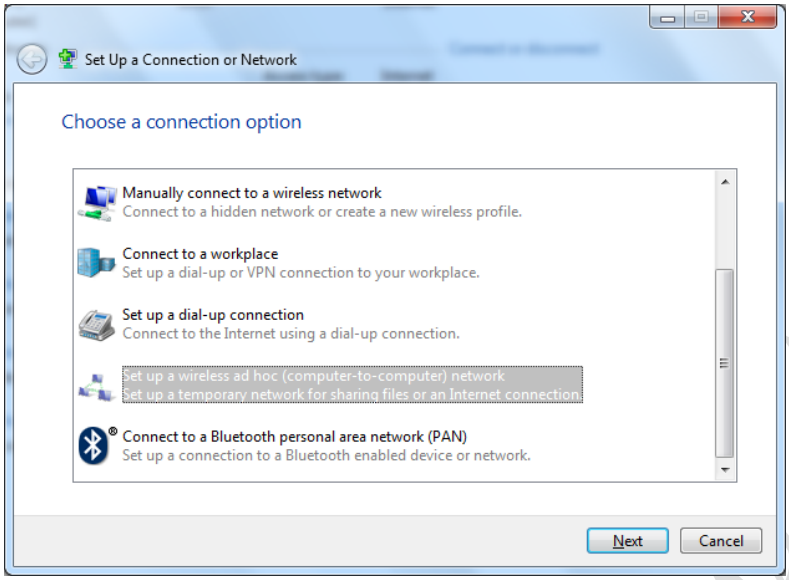
فتح مركز المشاركة والشبكة ثم اختيار: اعداد اتصال أو شبكة جديدة كما في الشكل (2)



الشكل (2)

ثم اختيار اعداد شبكة لاسلكية من نمط Ad hoc كما في الشكل (3).

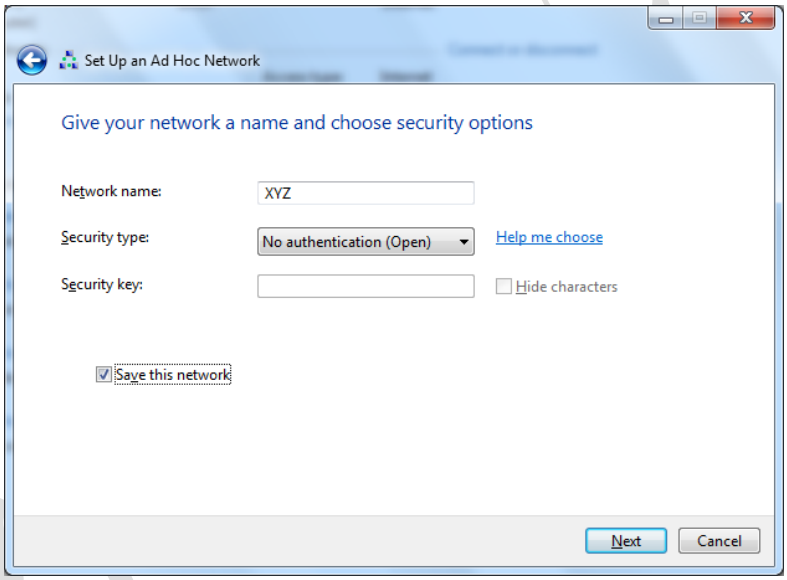
[6] SSID هو اسم الشبكة اللاسلكية المحلية التي نرغب ببثه.



الشكل (3)

نتابع عملية الاعداد بالضغط على التالي ثم التالي حتى نصل للشكل (4) الذي يطلب إدخال اسم الشبكة ونمط الأمان.

سنختار اسم الشبكة XYZ، ونمط الأمان "مفتوح" أي متاح مبدأياً

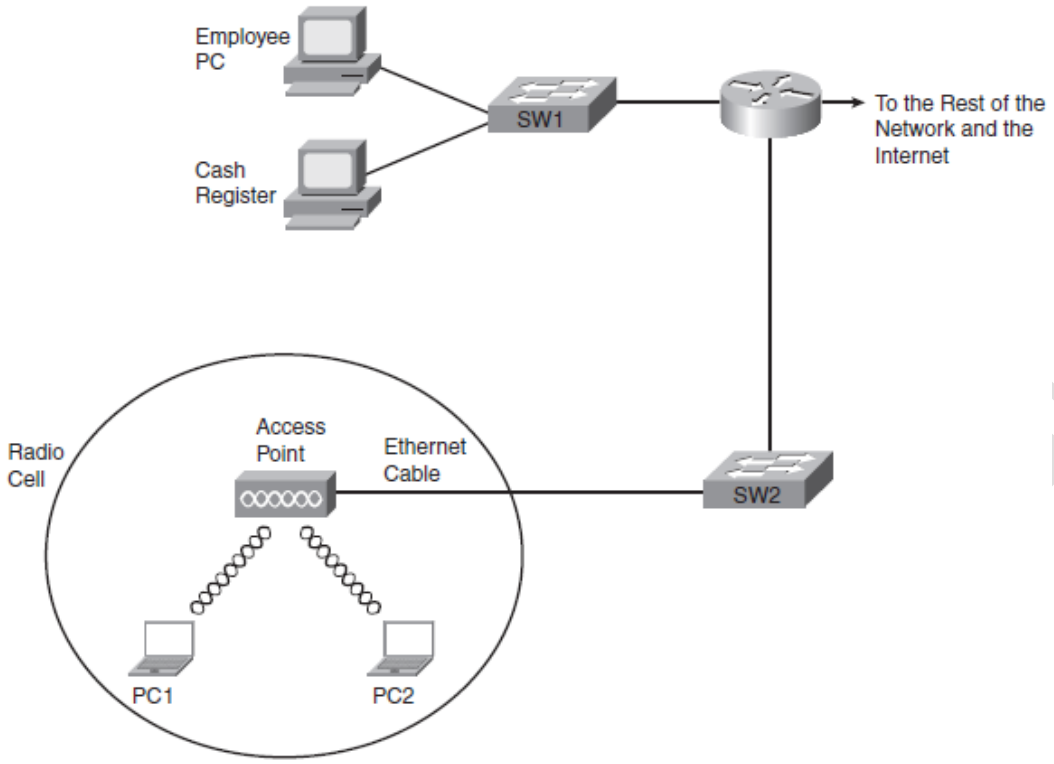


الشكل (4)

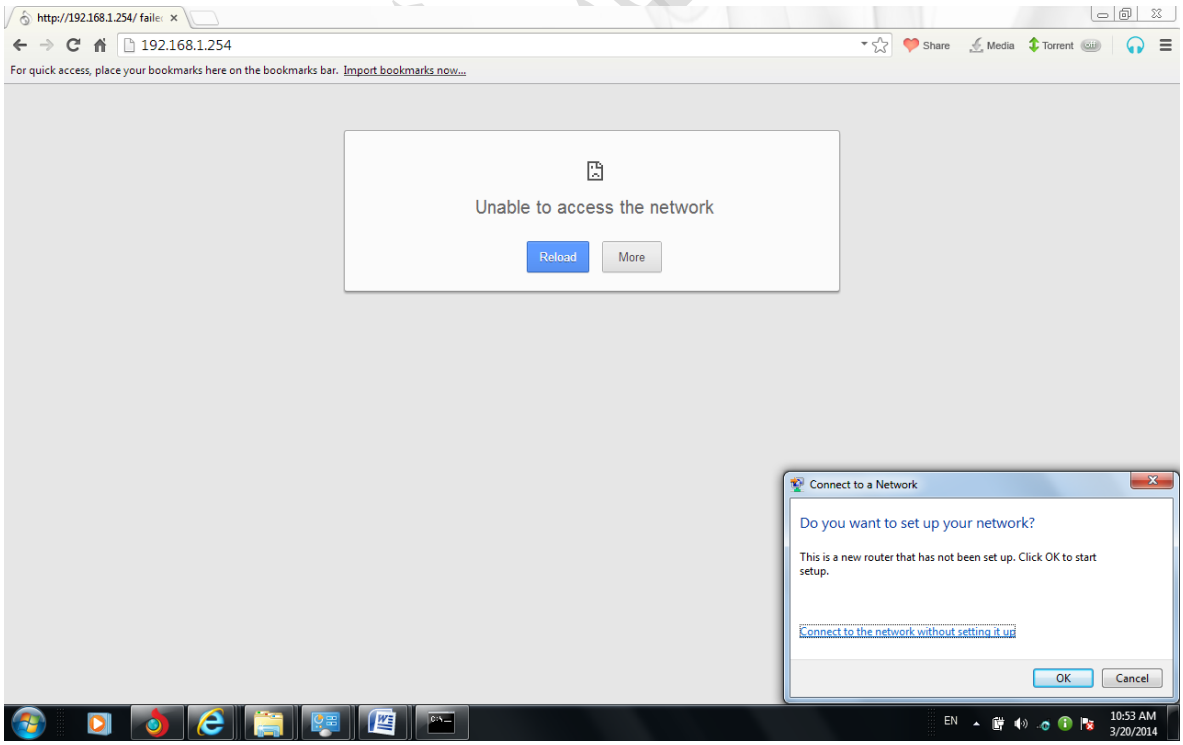
ثم نختار "إغلاق" بعد إتمام عملية الإعداد.

2- Infrastructure mode: تستخدم جهاز مركزي لتوصيل الأجهزة مع بعضها البعض يدعى ACCESS POINT

1.2 Basic Service Set-BSS: هي طبولوجيا لاسلكية نحتاج إليها عندما يريد جهاز ان يتصل بجهاز أخر باستخدام وسيط أو جهاز مركزي يسمح لهذه الأجهزة بالتواصل مع بعضها البعض يدعى نقطة وصول (Access Point) (شبكة لاسلكية باستخدام ACCESS POINTواحد) و يطلق عليه مصطلح Infrastructure Device و الأجهزة التي ستتصل بهذا الجهاز يطلق عليها مصطلح محطات (Stations). انظر الشكل (2)

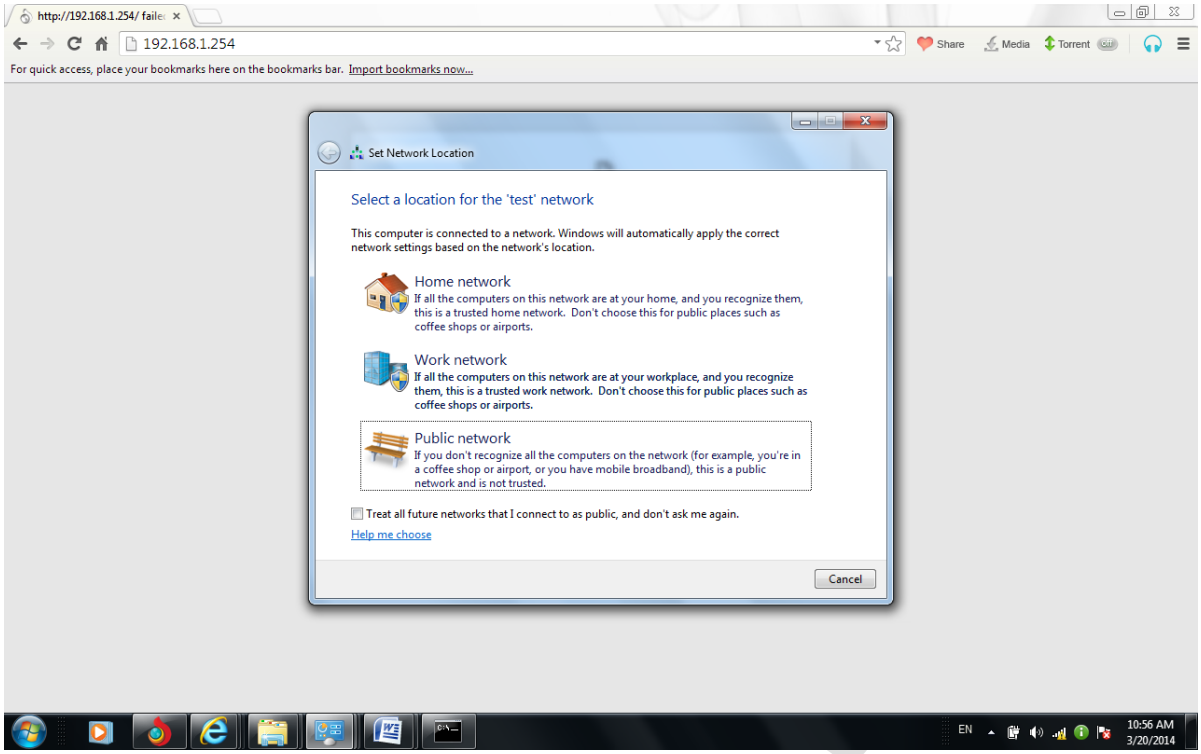


أثناء الاتصال بالشبكة عبر نقطة الوصول قد تظهر الرسالة التالية والتي تطلب إعداد الاتصال بنقطة الوصول نختار الخيار .....connect to the كما في الشكل (3)



الشكل (3)

ثم نحدد نوع الشبكة المطلوب إعدادها وفق الشكل (4) نحن اخترنا شبكة منزل Home Network

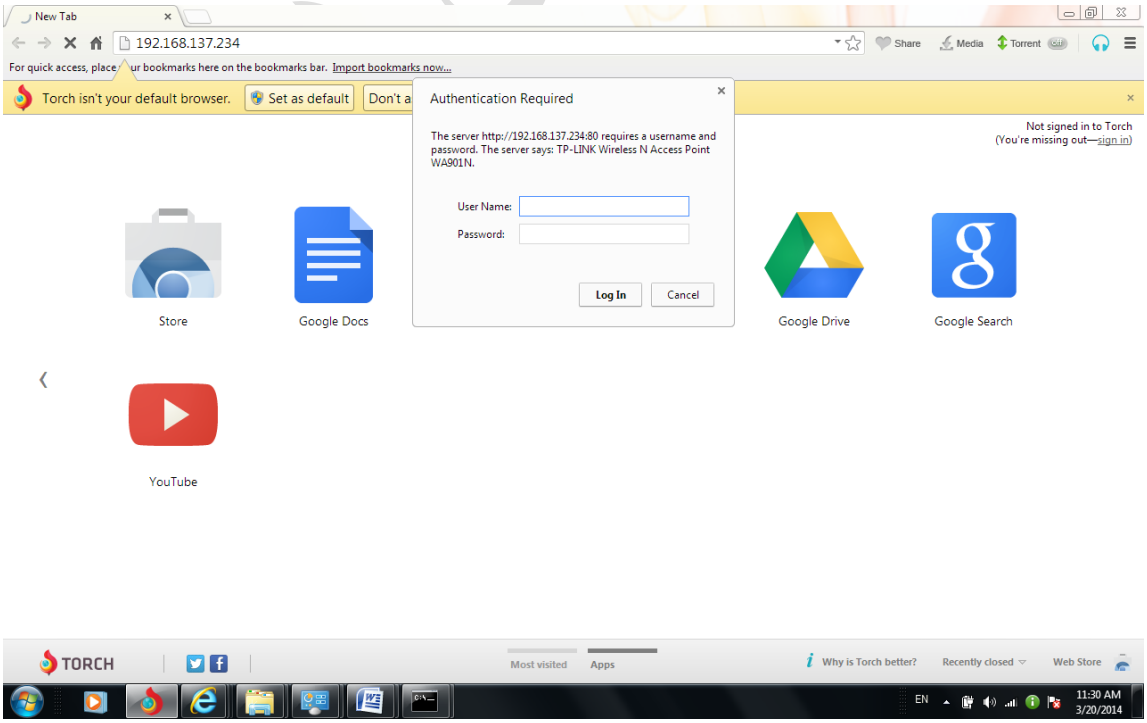


الشكل (4)

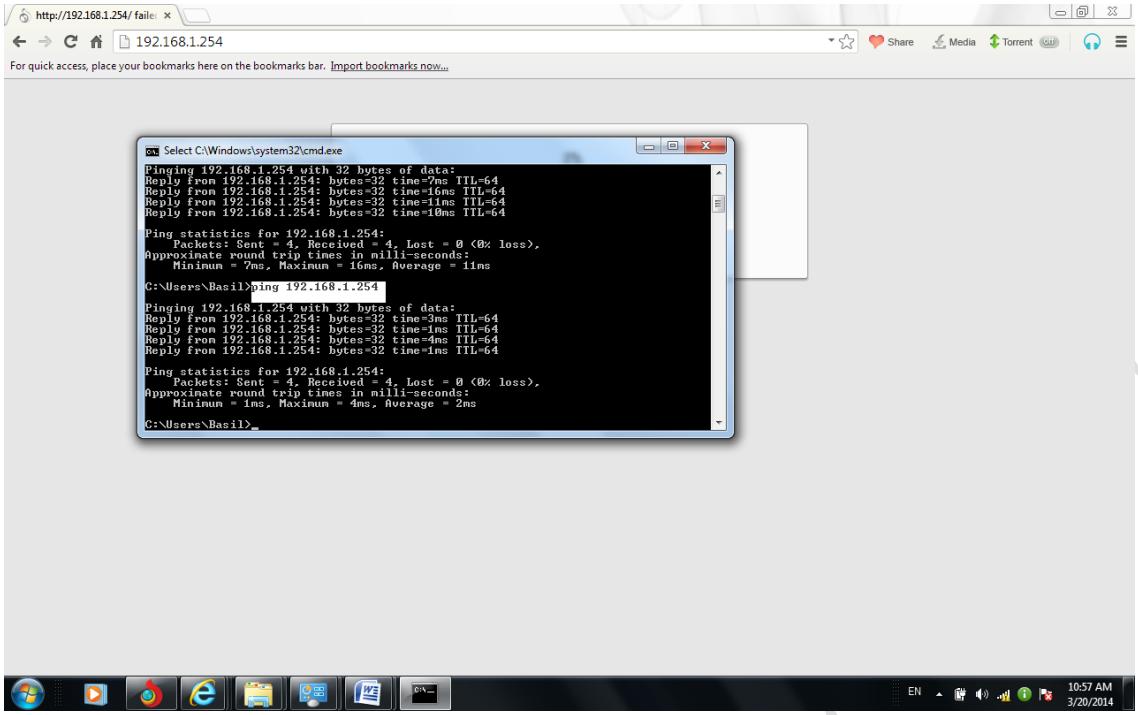
أثناء الدخول على برنامج التجهيزة عن طريق كتابة IP الخاص بها في نافذة المتصفح يطلب عادة اسم مستخدم و وكلمة مرور كالتالي:

User Name : admin وهو الافتراضي ومكتوب أسفل التجهيزة

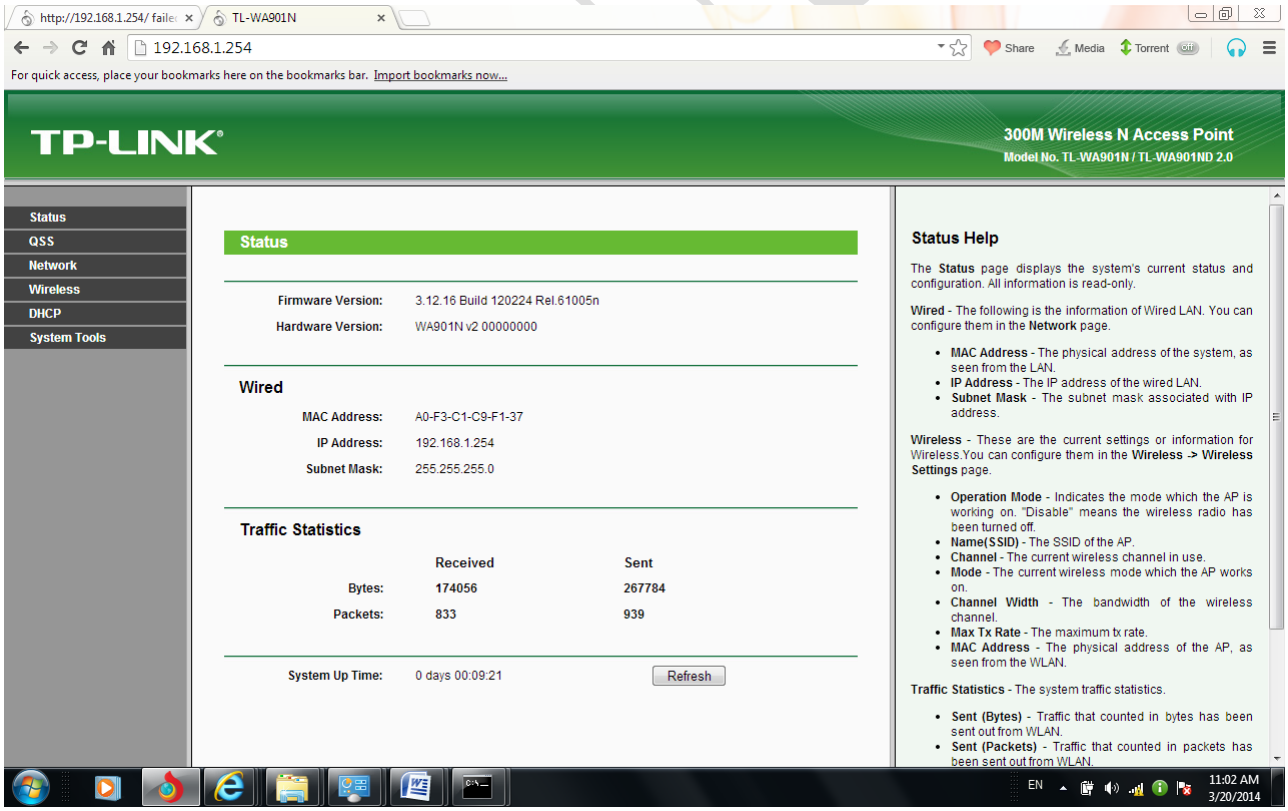
Password : admin وهو الافتراضي ومكتوب أسفل التجهيزة



يمكن دائماً التحقق من اتصالنا بنقطة الوصول عن طريق تعليمة Ping ثم عنوان IP لنقطة الوصول



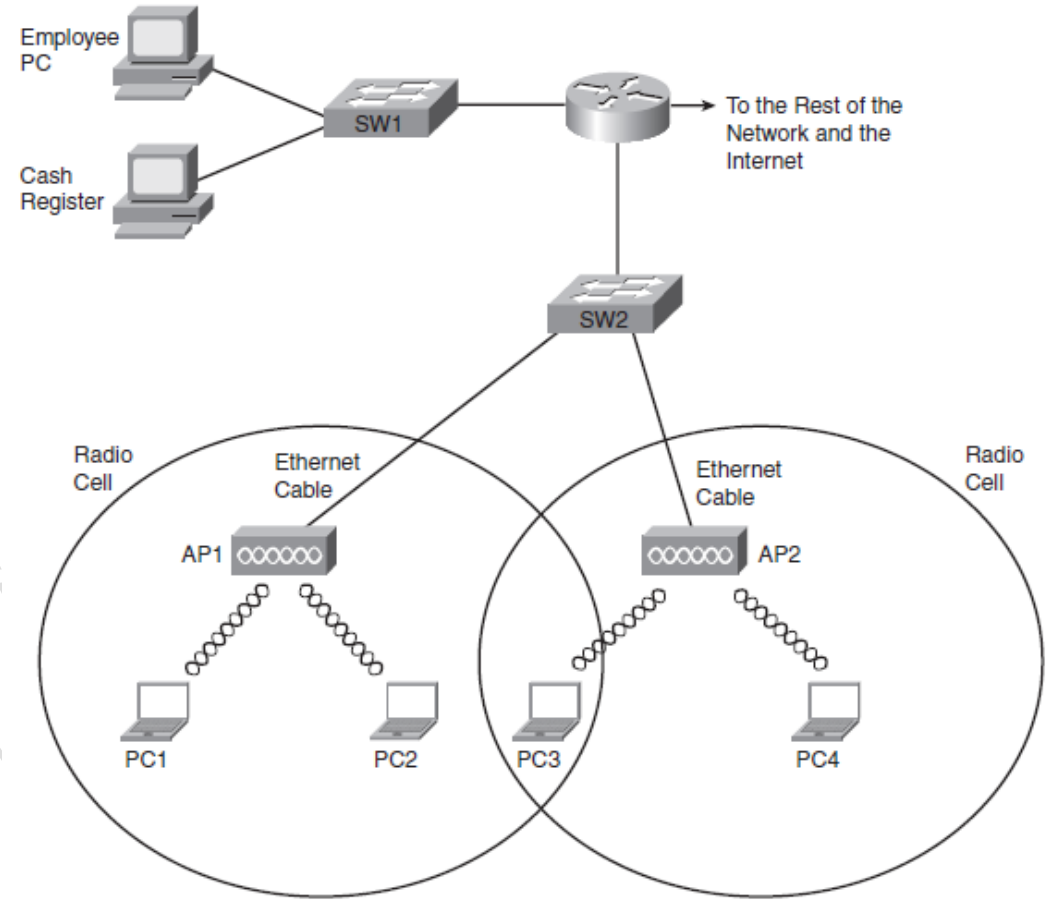
عن طريق المتصفح ندخل إلى برنامج AP وإلى واجهته الرئيسية.



1.2 - ESS:extended service set: طبولوجيا لاسلكية نحتاج إليها عندما يريد جهاز ان يتصل بجهاز أخر باستخدام وسيط أو جهاز مركزي يسمح لهذه الأجهزة بالتواصل مع بعضها البعض يدعى ACCESS POINT (شبكة لاسلكية باستخدام أكثر من ACCESS POINT) و يطلق عليه مصطلح Infrastructure Device و الأجهزة التي ستتصل بهذا الجهاز يطلق عليها مصطلح station و تستخدم هذه الطبولوجيا لتوسعة الشبكة المحلية اللاسلكية وهذه الشبكة يتم في كل أجهزتها استخدام اسم واحد فقط للشبكة SSID لتستطيع كافة الأجهزة الاتصال عبر أي من أجهزة نقطة الوصول الموجودة.

كما تحتاج أيضا أن يكون هناك تداخل Overlap بين خلايا أجهزة نقطة الوصول، و هي المسافة المشتركة بين ACCESS POINTS الموجودة في الشبكة كما بالشكل كي لا يكون هناك مناطق ميتة Dead Zone لا تستطيع الإشارة الوصول إليها و يجب أن تكون من 10-15%

يتم ضبط كل خلية في الشبكة اللاسلكية الممتدة علي قناة ترددية Channel مختلفة عن جارتها كي لا يحدث تداخل بين أجهزة نقاط الوصول. ويعطي معيار 802.11 b ثلاث قنوات ممكنة للنشر بين هذه الخلايا هي 1 و 6 و 11.



قبل الدخول في مفاهيم تأمين وحماية نقطة الوصول يجب ايضاح ما يلي:

ملاحظة1: تحوي تجهيزة موجه ADSL على أربعة تجهيزات مدمجة فيها وهي:

1- موجه (Router): فهو يربط الشبكة المحلية بالشبكات البعيدة.

2- مودم (Modem): فهو يحول اشارة DSL إلى إشارة يفهمها الحاسوب

3- مبدل (Switch): فهو يحتوي على أربعة منافذ Ethernet تعمل كمبدل سلكي.

4- نقطة وصول (Access Point): فهي تربط المستخدمين اللاسلكيين بالشبكة السلكية، وهي محور حديثنا والتي سنقوم بتأمينها.

ملاحظة2: قد توجد نقاط وصول في تجهيزات مستقلة (أي ليس ضمن موجه ADSL) وتكون أكثر احترافية وتحوي على مزايا أكثر، وتسمى بالمصطلح الدارج بالنواشر.

ملاحظة3: حتى نقوم بإعداد موجه ADSL وتجهيزه للاتصال بالإنترنت يجب أن نملك حساب (اسم المستخدم وكلمة المرور) لدى مزود خدمة الانترنت ISP ونعرف الاعدادات المطلوبة وندخلها في الحقول المناسبة. أسهل طريقة لذلك هي بعد الدخول للواجهة الرئيسية له نقوم بالدخول إلى تبويبة اعداد المنافذ (Interface Setup) ثم اختيار منفذ WAN الذي يسمى في بعض الأحيان بمنفذ الانترنت Internet ثم ادخال ما يلي:

رقم المسار الوهمي VPI: هو 8 ، وهو رقم محدد من ISPs في سوريا

رقم الدارة الوهمية VCI: هو 35 ، وهو رقم محدد من ISPs في سوريا

نمط التغليف (Encapsulation): هو PPPoE LLC

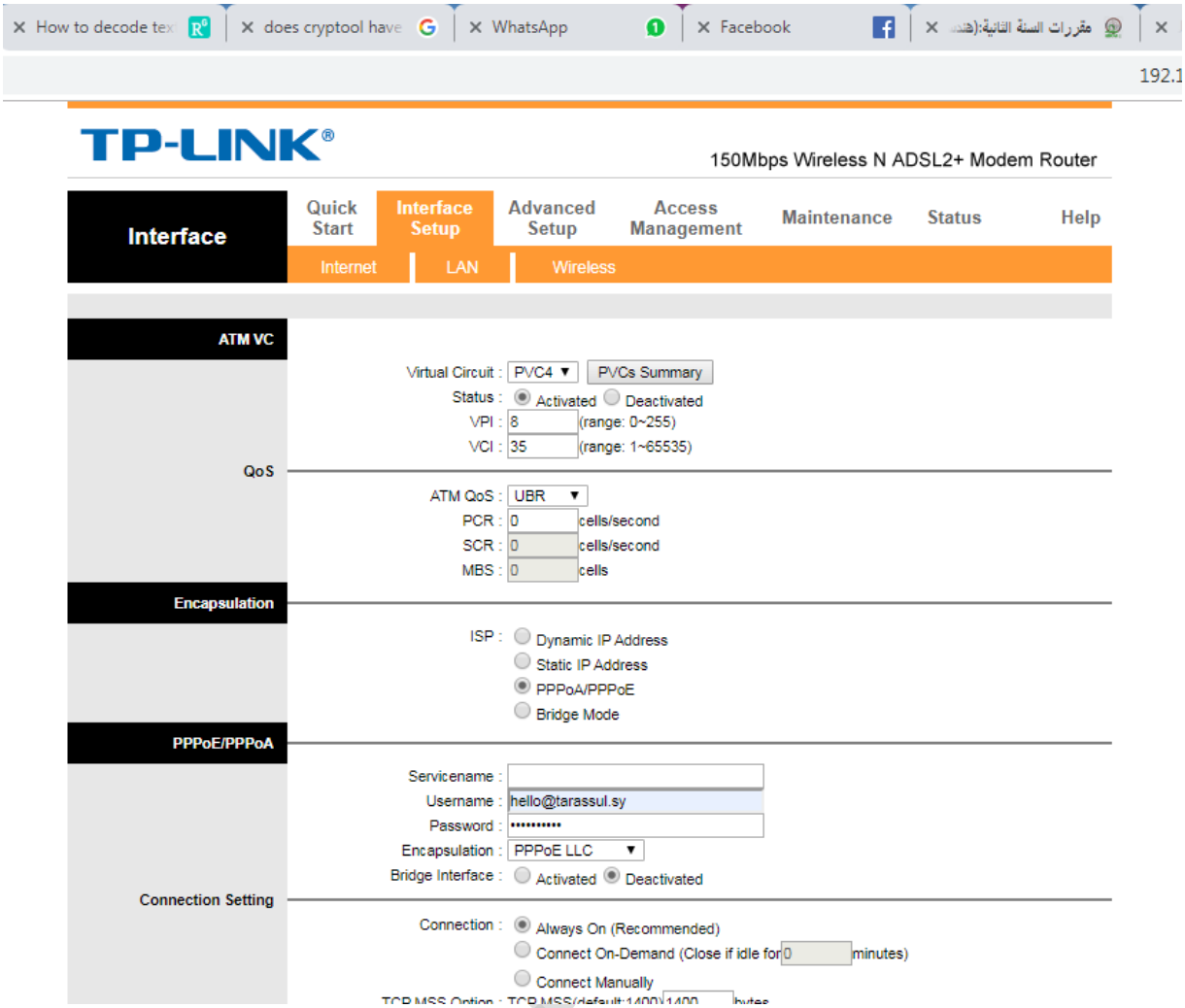
ثم كتابة اسم المستخدم (Username) الممنوح من ISP وهو في مثالنا hello@tarassul.sy

ثم كتابة كلمة المرور Password الممنوح من ISP المشتركين معه،

تترك كل الاعدادات غير ذلك على حالها دون تغيير.

ثم نحفظ الاعدادات.

يوضح الشكل التالي ما قمنا به:



أنواع التقنيات[7] [8] الأمنية المستخدمة في الاتصال مع الشبكات اللاسلكية:

يوجد ثلاثة معايير رئيسة هي:

1- WEP

2- WPA

3- WPA2

ملاحظة (1): يجب التفريق بين المفتاح المستخدم في التشفير للحصول على السرية وبين المفتاح المستخدم في التوثيق لنتمكن من التحقق من الهوية.

سنناقش كل معيار وفقاً للتوثيق والسرية والسلامة.

7 تحوي كل تقنية على مجموعة بروتوكولات وآليات تستخدم للتوثيق و للسرية وللسلامة.
8 تسمى التقنية أيضاً بالمعيار أو النمط.

1- معيار WEP (الخصوصية المكافئة للشبكة السلكية):

وهو اختصار لمصطلح البروتوكول المكافئ للأسلاك (Wired Equivalency Protocol: WEP). تقوم هذه التقنية بتوفير الأمان والخصوصية للشبكة اللاسلكية بشكل مشابه للأمان و الخصوصية الموجودة في الشبكات السلكية، و تم إطلاقها في عام 1999

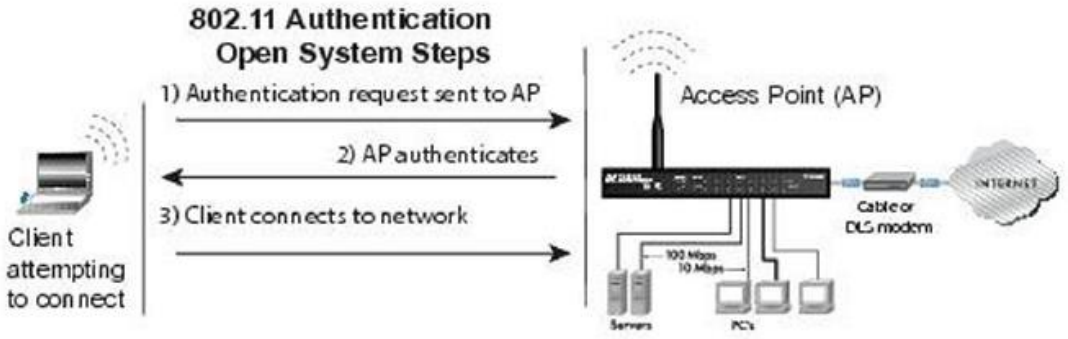
التوثيق في WEP:

التوثيق: هو حماية الشبكة من الوصول غير المصرح به و التحقق من كون الزبون الذي يحاول الولوج إلى الشبكة هو شخص مصرح له بذلك .

يتم التوثيق في WEP بطريقتين هما:

1- الدخول المتاح (Open Authentication):

لايتطلب الدخول إلى الشبكات اللاسلكية الموجودة في المرافق العامة مثل المطارات والمعارض و غيرها غالباً إدخال كلمة مرور لأن الشبكة تكون مفتوحة للجميع ولذلك يتم تفعيل خاصية الدخول المتاح (Open Authentication). يوضح الشكل (1) المراحل الثلاث للتوثيق بهذه الطريقة.



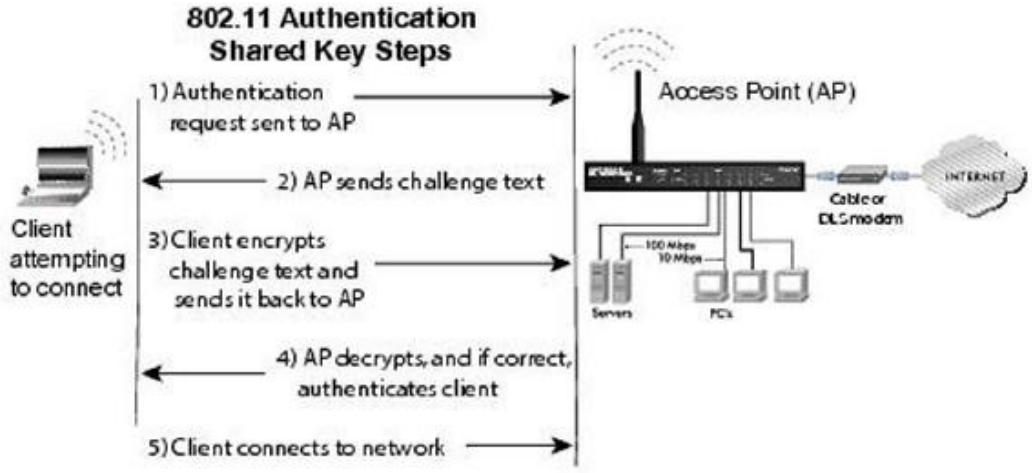
الشكل (1)

2- التوثيق بكلمة سر متعارف عليها مسبقاً (Pre-Shared Key: PSK):

هنا يتم الاتفاق على كلمة سر يتم تشفير بها عدة حروف عشوائية يرسلها الجهاز المراد الدخول للشبكة إلى AP ثم تقوم AP باستقبالها و تعيد فك شفرتها بواسطة نفس كلمة السر و عند التوافق يتم الاتصال بين الاثنين و السماح للجهاز بالدخول إلى الشبكة.

يقوم الجهاز بتوثيق دخوله بواسطة AP ولا يتم توثيق نفسه هو كعضو معروف في الشبكة مسبقا، و لذلك فإن أي شخص يمتلك اسم الشبكة و كلمة التوثيق قادر على الولوج إليها. يعرف هذا النوع من التوثيق بالشخصي (Personal) ويستخدم عادة في الشبكات الصغيرة. يوضح الشكل (2) المراحل الخمسة للتوثيق بهذه الطريقة، حيث يقوم الزبون بإرسال طلب توثيق لدخول شبكة الأكسس بوينت يقوم بعدها نقطة الوصول بالرد برسالة غير مشفرة تسمي clear-text challenge يقوم الزبون بعد استلام الرسالة بتشفيرها باستخدام مفتاح WEP ثم يرسلها لنقطة

الوصول. تقوم AP بعد استلام الرسالة ثم إذا نجحت في فك تشفيرها decrypt باستخدام مفتاح WEP فيتم السماح للجهاز بالولوج للشبكة.

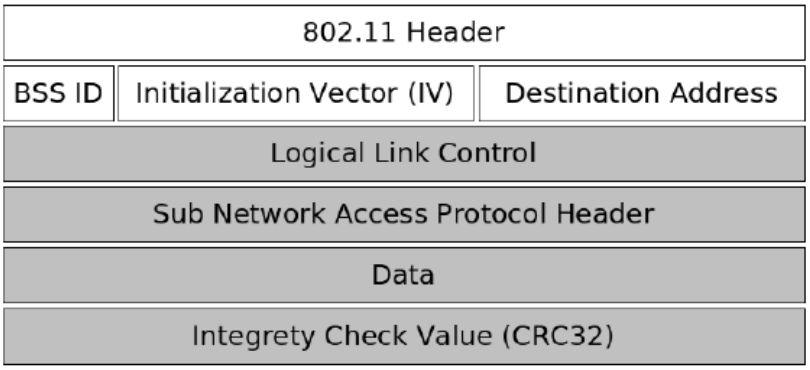


الشكل (2)

لا زال الكثيرون يستخدمون في أجهزتهم بل إن المصنعون لازالوا يضعونها كأحد وسائل الحماية في أنظمتهم رغم أنها سهلة الكسر والاختراق.

التشفير في WEP

يبين الشكل (3) محتويات الرزمة في الشبكات اللاسلكية عموماً:



الشكل (3)

ويتكون من جزأين أولهما غير مشفر و هو الجزء غير المظلل في الشكل ويحوي:

- 802.11 Header : وهي مقدمة الرزمة و التي تعبر عن الشبكات اللاسلكية غير مشفرة
- Basic Service Set Identifier BSS ID : وهو العنوان الفيزيائي لنقطة الوصول AP MAC
- initialization vector IV رقم عشوائي يتم اختياره من قبل المرسل و المستقبل و يرسل بشكل غير مشفر

الجزء الثاني وهو باقي أجزاء الرزمة وتكون مشفرة، تحتوي على البيانات (Data) والذيل.

لتشفير البيانات يستخدم WEP خوارزمية تسمى (Ron's Code 4: RC4) لتوليد مفتاح التدفق (Key Stream)

ملاحظة (2): تعتبر RC4 خوارزمية متماثلة (Symmetric Algorithm) أي أن المفتاح المستخدم في التشفير عند المرسل هو نفسه المستخدم في فك التشفير عند المستقبل.

وينقسم كل Key stream إلى جزأين: أولهما هو WEP Key وهو المفتاح المشترك (Shared Key) الذي تم إدخاله في الجهاز، والجزء الثاني هو شعاع التهيئة (Initialization Vector: IV) وهو رقم خاص بعملية التشفير و يتم توليده بشكل عشوائي. يكون طول Key stream أحد القيم التالية:

1- WEP 64-bit

2- WEP 128-bit

3- WEP 256-bit

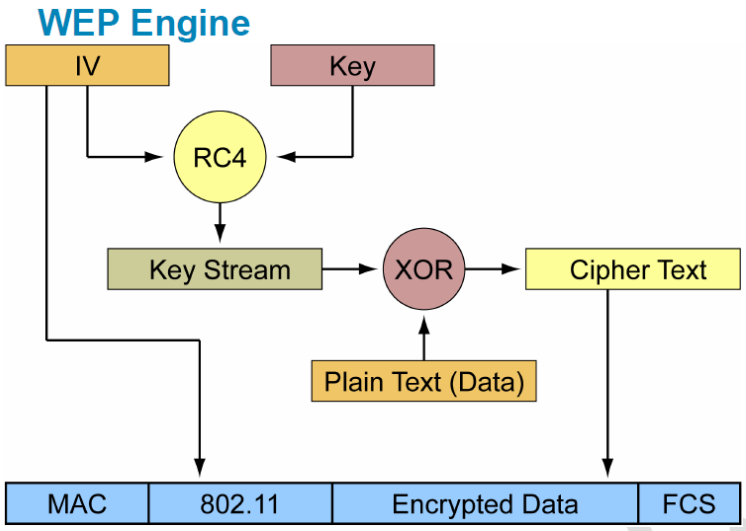
1- WEP 64-bit : يسمي أيضا (WEP-40) لأن Shared Key الذي يدخله المستخدم يحتوي على 10 خانات ست عشرية(A-F , 0-9) ، كل خانة يحتوي علي 4 bits بمجموع40bits، يتم إضافة initialization vector (IV) بطول 24 bit لعمل RC4 ليصل المجموع الكلي إلى 64-bit .

لكن الكثير من الأجهزة قد تجبرك على إدخال خمس بايتات من النوع ASCII و هي بدورها تحول كل حرف أو رقم الي ثمانية بت لتصل في النهاية إلى 40 bit أيضاً.

2- WEP 128-bit : يسمى أيضا (WEP-104) لأن Shared Key الذي يدخله المستخدم يحتوي على 26 خانة ست عشرية(A-F , 0-9) ، كل خانة يحتوي علي 4 bits بمجموع 104bits، يتم إضافة initialization vector (IV) بطول 24 bit لعمل RC4 ليصل المجموع الكلي إلى 128-bit .

3- WEP 256 bit-: يسمى أيضا (WEP-232) لأن Shared Key الذي يدخله المستخدم يحتوي على 58 خانة ست عشرية(A-F , 0-9) ، كل خانة يحتوي علي 4 bits بمجموع 232bits، يتم إضافة initialization vector (IV) بطول 24 bit لعمل RC4 ليصل المجموع الكلي إلى 256-bit .

ويتم جمع IV مع Key ثم الدخول لخوارزمية RC4 لينتج Keystream ثم جمعها بطريقة XOR مع plain text لينتج في النهاية النص المشفر. يوضح الشكل (4) عملية التشفير في WEP



الشكل (4)

السلامة في WEP: تعتمد على خوارزمية CRC الموجودة في ذيول الرزم والتي تعتبر ضعيفة أيضاً.

عيوب معيار WEP:

1- نقطة الضعف الأساسية في هذا البرتوكول هي استخدام مفتاح توثيق ثابت على جميع الأجهزة المسموح لها التعامل مع الشبكة، وهو نفسه المفتاح المستخدم في عملية التشفير

2- خوارزمية RC4 هي خوارزمية ضعيفة يسهل اختراقها و معرفة البيانات المرسلة.

3- طريقة التشفير تعتبر بدائية تستخدم خوارزمية خطية Linear Checksum أي أن تسلسل فك التشفير هو معكوس تسلسل التشفير بالضبط كأنك تقوم بفك تغليف علبة هدايا بعد أن قمنا بتغليفها.

4- يستخدم مفتاح أساسي WEP Key يتم إضافة بيانات عشوائية IV إليه كي لا يستطيع أحد فهم طريقة التشفير، و رغم أن هذه بيانات عشوائية يصعب توقعها إلا أنها بيانات صريحة (plain text) أي مقروءة بالإضافة الي أنها ليست بالطول الكافي فيمكن تكرار نفس IV بعد إرسال 5000 رزمة.

ملاحظة (3): ظهرت عدة تحديثات وتحسينات لـ WEP إلا أنها بقيت قابلة للكسر بسهولة.

2- معيار WPA (الوصول المحمي للشبكة اللاسلكية):

برتوكول WPA يعتمد على برتوكول (Temporal Key Encryption Protocol: TKIP) وظيفته هي القيام بتوليد مفاتيح تشفير متغيرة لكل حزمة بيانات مرسلة وبالتالي فان هذا البرتوكول يجعل من الصعب على المتطفلين اختراق الشبكات المستخدمة له.

مازال WPA يعتمد على RC4 بشكل أو بآخر، وبالتالي يجب استخدام معيار WPA2 و الذي يستخدم برتوكول آخر غير RC4 .

التوثيق في WPA:

يتم التوثيق في WPA بطريقتين عبر استخدام مفتاح يسمى بـ Master key وطوله 256 بت.

1- التوثيق بكلمة سر متعارف عليها مسبقاً (Pre-Shared Key: PSK):

وهي مشابهة تماماً للنفس الطريقة في WEP.

2- التوثيق باستخدام RADIUS (Extensible Authentication Protocol: EAP)[9]**:**

هنا يستخدم مخدّم مخصص يتم بواسطته معالجة طلبات دخول الأشخاص إلى الشبكة بواسطة حساباتهم (أسمائهم و كلمات مرورهم) كل على حده ويسمي هذا المخدّم: راديس" (Remote Authentication Dial-in User Service: RADIUS). هذه الطريقة ليست قاصرة على الشبكات اللاسلكية فقط، فهي معروفة و شائعة كأسلوب توثيق متقدم للدخول للتعامل مع إعدادات الكثير من الأجهزة مثل الموجهات. تعرف هذه التقنية أيضاً بـ "الشركة" (Enterprise) وتستخدم عادة في شبكات الشركات التي تتطلب آماناً عالياً.

التشفير في WPA:

يتم التشفير بواسطة بروتوكول TKIP المعتمد على خوارزمية RC4 مع تطوير وتعقيد بعض المراحل التي أعطت نوعاً من القوة وصعبت عملية الكسر. مثلاً أصبح طول IV هي 48 بت بدلاً من 24، ولم يعد يدخل مباشرة في صنع مفتاح التشفير. TKIP تعتمد على تقنية إدارة المفاتيح (Key Management) وعلى تقنية المصافحة رباعية الطرق (4-Way handshake) لاشتقاق وإنتاج أزواج من المفاتيح الخاصة بكل زبون والمتغيرة باستمرار.

السلامة في WPA:

يعتمد WPA على خوارزمية MIC القوية والتي تسمى بخوارزمية ميشيل، و تكشف وتمنع أي تعديلات على الرزمة أو السيطرة عليها.

3- معيار WPA2 : بروتوكول WPA2 هو تطوير لبروتوكول WPA مع بعض التطويرات عليه.

التوثيق في WPA2

[9] تعرف هذه التقنية أيضاً بـ 802.1X

1- التوثيق بكلمة سر متعارف عليها مسبقاً (Pre-Shared Key: PSK):

وهي مشابهة تماماً لنفس الطريقة في WEP و WPA.

2- التوثيق باستخدام RADIUS (Extensible Authentication Protocol: EAP):

وهي مشابهة تماماً لنفس الطريقة في WPA.

التشفير في WPA2:

يستخدم بروتوكول CCMP المعتمد على خوارزمية AES القوية. CCMP تعتمد على تقنية إدارة المفاتيح (Key Management) وعلى تقنية المصافحة رباعية الطرق (4-Way handshake) لاشتقاق وإنتاج أزواج من المفاتيح الخاصة بكل زبون والمتغيرة باستمرار.

السلامة في WPA2:

يتم استخدام تقنية CBC-MAC القوية في المحافظة على سلامة الرسالة.

ملاحظة: بعد فترة من ظهور بروتوكول WPA2، تم التعديل عليه والسماح له بتشفير البيانات عبر TKIP، والعكس صحيح فأيضاً تم التعديل على WPA والسماح له بتشفير البيانات عبر AES.

بالنتيجة: هل بإمكان حاسوب يعمل على WPA2-Personal+TKIP الاتصال بنقطة وصول تعمل على WPA-Personal+TKIP علماً أن كلاهما يستخدمان مفتاح توثيق متشابه بالقيمة والطول؟؟

ملخص مقارنة بين المعايير الأمنية الثلاث

البروتوكول الأمني	التوثيق	السرية	السلامة
1-WEP	بإمكاننا استخدام: 1- Open أو 2- SK	يشفر البيانات عبر خوارزمية RC4 وهي خواروزمية ضعيفة أساساً	تعتمد تقنية CRC الموجودة أصلاً في ذيول الرزم، وهي تقنية ضعيفة أيضاً
2-WPA	بإمكاننا استخدام: 1- PSK(Personal) أو 2-(Enterprise) عبر مخدم Radius	تستخدم أساساً بروتوكول TKIP لإنشاء مفاتيح ديناميكية متغيرة مع كل رزمة مما يصعب الاختراق. يبقى عيب اعتمادها على خوارزمية التشفير الضعيفة RC4.	تعتمد على تقنية مايكل (Michael) والتي تسمى أيضاً MIC، وتعتبر قوية في التحقق من الصحة.
3-WPA2	بإمكاننا استخدام: 1- PSK(Personal) أو 2-(Enterprise) عبر مخدم Radius	تستخدم أساساً بروتوكول CCMP المعتمد على خوارزمية AES القوية	CBC-MAC

واجهة برنامج Access Point

يظهر الشكل التالي اتصال بين حاسوب مع نقطة وصول اسمها [10] "default" من طراز ASUS، ودخوله على برنامج الإعدادات الخاص بها.

يمكن الدخول لإعدادات نقطة الوصول الافتراضية عبر كتابة العنوان الشهير 192.168.1.1 في متصفح الويب.

كما ويمكن تغيير هذا العنوان الافتراضي بالتأكيد الى أي عنوان آخر.

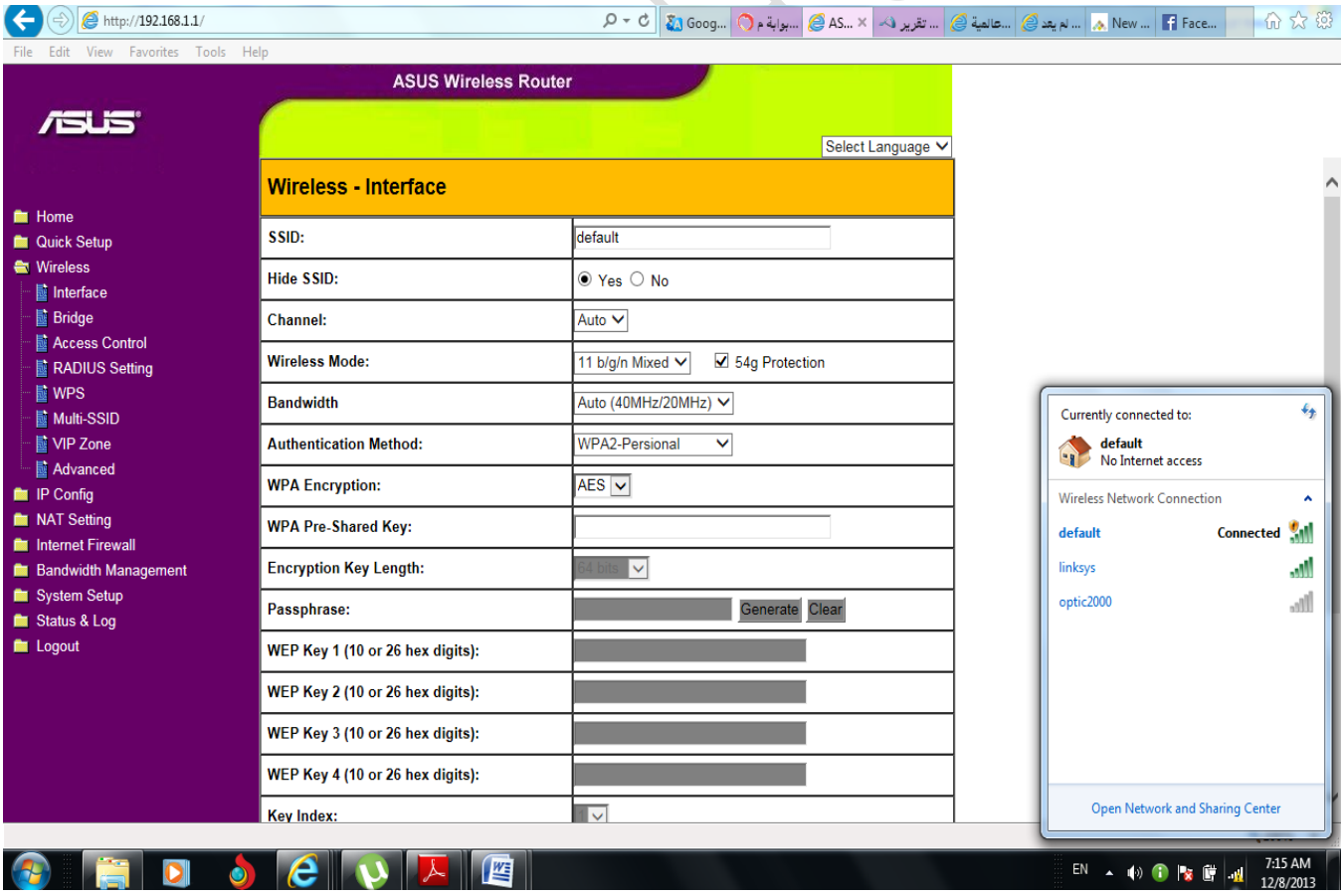
ما يهمنا أولاً هو دراسة الخيارات اللاسلكية في نقاط الوصول. أي سنركز على تبويبة "Wireless" الموجودة في القائمة اليسرى.

نلاحظ أن الاعدادات موضوعة على عدم بث وإظهار اسم نقطة الوصول في الهواء، لأن خيار اخفاء الاسم Hide SSID مفعل. وهذا يعتبر اجراء أمني لا بأس به.

نلاحظ أن قناة نقل البيانات الحالية هي Auto أي تلقائية. بإمكاننا إذا أردنا اختيار قناة اتصال محددة من 1 إلى 13.

نلاحظ أنه قد تم ضبط البروتوكول الأمني WPA2-Personal مع خوارزمية تشفير بيانات WPA Encryption هي AES.

لم ندخل حتى الآن قيمة مفتاح التوثيق لأن الخيار WPA Pre-Shared Key ما زال فارغاً.



[10] يرمز لاسم الشبكة بالمصطلح SSID

تدريب:

- كيفية عمل إعادة ضبط تجهيزه AP بإعدادات المصنع الافتراضية.
- كيفية الدخول إلى واجهة برنامج AP.
- كيفية تغير اسم المستخدم وكلمة المرور اللازمين للدخول للAP
- كيفية ضبط إعدادات WEP و WPA و WPA2
- كيفية تغيير IP الخاص بـ AP إلى IP خاص مختلف.
- كيفية تحديث برنامج (Firmware) الخاص بال AP
- كيفية تفعيل أو إيقاف تفعيل خدمة DHCP.

خاصية إعداد شبكة WiFi المحمية (WiFi Protected Setup :WPS)

الهدف من هذه الخاصية هو تسهيل وتسريع عملية توثيق الاتصال بشبكة WiFi مع الاحتفاظ بأمان تشفير عالي دون أن يضطر المستخدم لمعرفة البروتوكولات الأمنية والمفاتيح PSK. اعتمدت هذه الخاصية في معيار WiFi ولن يتم اعتماد وتوافقية أي تجهيزة لاسلكية لمعيار Wifi إذا لم تدعم هذه التجهيزة لخاصية WPS. يبين الشكل التالي الشعار الدال على هذه الخاصية.

فهي إذاً صممت لمساعدة الأشخاص ذوي الخبرة التقنية القليلة عبر وصل أجهزتهم إلى الشبكة اللاسلكية دون عناء.

ملاحظة: للاستفادة من هذه الخاصية يجب أن تكون مفعلة في تجهيزة نقطة الوصول اللاسلكية.

طريقتان لشبك الزبائن بنقطة الوصول (AP) عبر خاصية WPS:

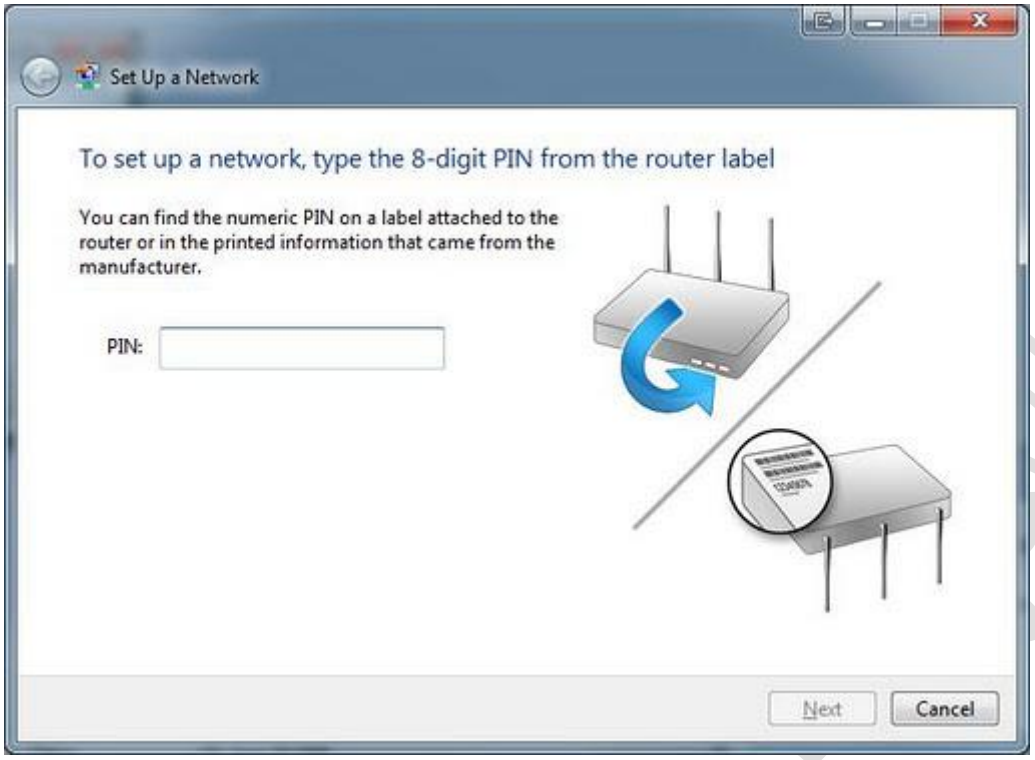
1- طريقة ضغط الأزرار (PBC): تحتوي الأجهزة التي تدعم خاصية WPS على زر فيزيائي بجانبه شعار WPS يستخدم للبحث عن الأجهزة التي تطلب هذه الخدمة ويستمر البحث عادة دقيقتين، و في بعض الحالات يوجد زر خاصية WPS برمجياً من خلال واجهة الإعدادات في تجهيزة نقطة الوصول. بعض التجهيزات تدعم وجود زر فيزيائي وزر برمجي .

يقوم الزبون بالضغط أيضاً على زر WPS بشكل متزامن مع التجهيزة وضمن الدقيقتين، وبذلك تكتمل عملية التوثيق.

الثغرة في هذه الطريقة أن أي جهاز تصادف الضغط به على زر WPS مع ضغط صاحب نقطة الوصول لهذا الزر أيضاً، سيتمكن من الدخول إلى الشبكة اللاسلكية دون إذن.

2- طريقة إدخال رقم التعريف الشخصي (Personal Identification Number: PIN): يمكن أن يكون لكل كرت شبكة رقم تعريف خاص به على الشبكة مكون من 8 أرقام عشرية. أي: لنقطة الوصول رقم تعريف شخصي وللزبون رقم تعريف شخصي.

في خاصية WPS: إما نضع رقم التعريف الخاص بالزبون داخل إعدادات نقطة الوصول، أو نضع رقم تعريف نقطة الوصول داخل إعدادات الزبون، وبذلك تكتمل عملية التوثيق. عادة يوضع رقم التعريف لنقطة الوصول على لصاقة خلفها. يوضح الشكل التالي طريقة إدخال رقم تعريف نقطة الوصول داخل إعدادات الزبون.



الشكل ()

الثغرة في هذه الطريقة هو أن رقم التعريف الشخصي يتكون من ثمان أرقام عشرية مما يسهل عملية التخمين للمخترقين عبر أداة اسمها ريفر (Reaver) بالهجوم العنيف الذي يقوم بتجريب كل الإحتمالات الممكنة للخانات العشرية الثمانية. يترواح وقت التخمين بين ساعتين إلى أربع أو خمس ساعات فقط.

ملاحظة: رقم PIN هو رقم غير ثابت لكرت الشبكة ويمكن تغييره.

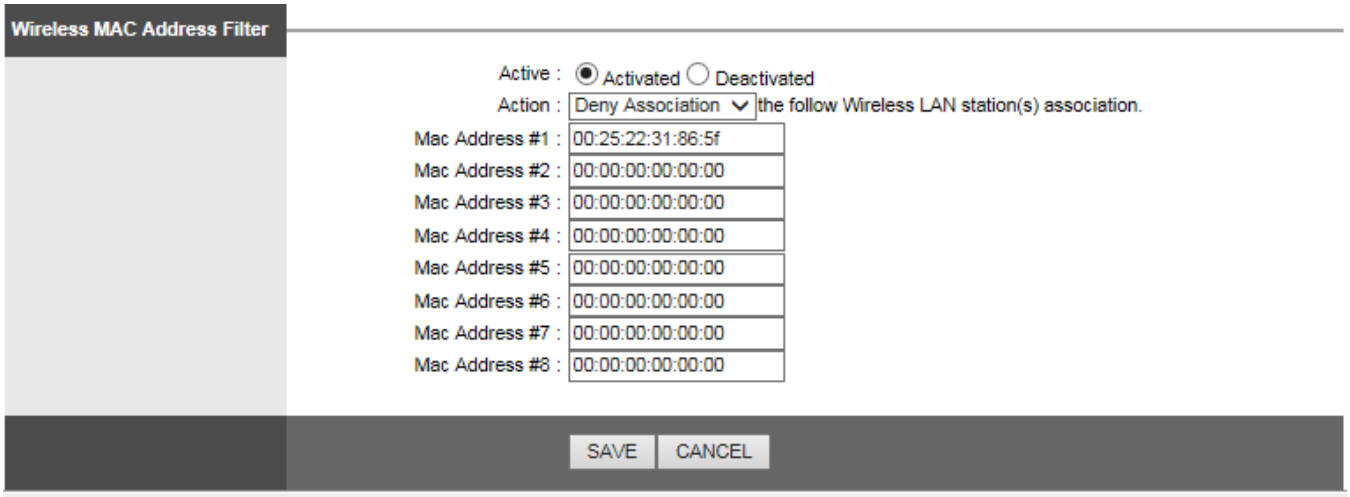
تصفية الأطر باستخدام عنوان MAC

لكل كرت شبكة عنوان MAC فريد يتميز به عن غيره. يمكن لنقاط الوصول تقييد الاتصال اللاسلكي بها عبر السماح (Permit) (Allow) لعناوين MAC موجودة بقائمة عنوانين الاتصال بها وحجب (Deny) (Disable) العناوين الأخرى غير الموجودة بالقائمة، أو حجب العناوين الموجودة بالقائمة والسماح للعناوين الأخرى غير الموجودة بها.

ملاحظة: لاستخدام خاصية التصفية حسب عنوان MAC يجب تفعيلها (Enable) (Activated) أولاً.

ملاحظة: تطبيق هذه الخاصية مستقل عن تطبيق البروتوكولات الأمنية WEP و WPA و WPA2.

مثال: لدينا الشكل التالي المأخوذ من إعدادات إحدى نقاط الوصول.



الشكل ()

من الشكل نلاحظ التالي:

1- خاصية التصفية باستخدام عناوين MAC مفعلة (Activated).

2- كل ما هو موجود في القائمة سيتم حجبه (Deny Association).

3- لن يسمح للزبون ذو العنوان 00:25:22:31:86:5f الاتصال والارتباط بنقطة الوصول، بينما سيسمح لكل الأجهزة الأخرى الاتصال بها.

الممارسات الأمثل لحماية الشبكة اللاسلكية المحلية (Best Practices for Securing WLAN)

1- إخفاء اسم الشبكة (Hide SSID)، أو تعطيل خيار السماح ببثه (No Broadcast SSID).

2- تعقيد PSK.

3- تمكين بروتوكول الأمان WPA2 بخوارزمية تشفير AES.

4- تفعيل التصفية عبر استخدام عنوان MAC.

5- إبطال تفعيل خاصية WPS.

6- تغيير حساب اسم المستخدم وكلمة المرور لحساب المسؤول اللازمين للدخول لإعدادات AP.

7- تغيير IP الخاص بالدخول لإعدادات AP إلى IP خاص مختلف.

8- إيقاف خدمة DHCP.