# تقييم هجمات كورك لاستعادة مفتاح تشفير بروتوكول الحماية WEP في الشبكات اللاسلكية

د.م. رزق غانم د.م. محمد الحسين


## الملخص

**هَدَفَ هذا البحث إلى شرح بروتوكول الحماية المكافئة WEP لحماية الشبكات اللاسلكية وآلية عمله وخوارزمية التشفير المستخدمة ونقاط ضعفه، والهجمات التي تستهدفه إذْ جرى التركيز على هجمات كورك لاستعادة المفتاح وهي عبارة عن سبع عشرة هجمة نُشِرَتْ من قبل كورك على شكل كود مصدري في منتدى Netstumbler ولم يقم بالتطرق لشرح آلية عملها، وقد تم الانطلاق من هذه الهجمات واكتشاف هجمات جديدة فيما بعد. لذلك دَرَسْنَا في هذا البحث دراسةً مفصَّلة هذه الهجمات وشرح مبدأ عملها، فضلاً عن تطبيق هذه الهجمات وتقييم عملها والمقارنة فيما بينها.**

**كما هَدَفَ هذا البحث إلى إبراز الثغرات الأمنية لهذا البروتوكول وسهولة كسر حمايته، وذلك بهدف التوجه إلى بروتوكولات حماية أكثر وثوقية وأمن، وقد بينت دراسة حديثة أنَّ نحو 40% من الشبكات اللاسلكية تستخدم هذا البروتوكول كوسيلة حماية حتى اليوم.**


**الكلمات المفتاحية:** هجمات استعادة المفتاح، خوارزمية جدولة المفتاح، خوارزمية التوليد شبه العشوائي للمفتاح، بروتوكول الحماية المكافئة لحماية الشبكات السلكية، استيقان وهمي، استيقان باستخدام مفتاح مشترك.

# Evaluation of Cork attacks to restore WEP security key encryption in wireless networks

**Dr. Rzek Ghanem Dr. Muhmed Al-Huseen**

## Abstract

**This research aims to explain a working mechanism, encryption algorithm, and weaknesses of Wired Equivalent Privacy (WEP) Wi-Fi security protocol ,and attacks against it.**

**We will focus on korek's key recovery attacks, which are seventeen attacks published on the web as a source code by person called Korek . but, because Korek was not engaged in the details and didn't explain the mechanism of action of this attacks ,we try to study these attacks in depth and explain the principles of its work , in addition we try to implement these attacks and evaluate its work and make comparison between it.**

**This research also aims to highlight the vulnerabilities of this protocol and the ease of breaking the protection, aiming to more reliable and secure protection protocols. A recent study showed that about 40% of wireless networks are using this protocol as a protection method until today.**

**Keywords:** Key recovery attacks, Key scheduling algorithm, Pseudo Random Generator Algorithm , Wired Equivalent Privacy, Fake authentication, shared key authentication.

## 1- مقدمة:

إن الميزة الأهم في الشبكات اللاسلكية التي أدت إلى الانتشار الواسع لها وجعلتها مفضلة على الشبكات السلكية هي تجنب استخدام البنية الفيزيائية المستخدمة في الشبكات السلكية .ولكن من جانب آخر تتعرض الشبكات اللاسلكية تبعاً لطبيعتها لتهديدات أمنية أكثر من تلك الموجودة في الشبكات السلكية إذْ تتصل الحواسب في الشبكات السلكية مع بعضها بعضاً بواسطة أسلاك؛ وبهذا تصبح أسهل في الإدارة والتحكم بإمكانية النفاذ، واستخدام موارد الشبكة، في حين تنتشر البيانات المرسلة عبر الشبكات اللاسلكية في الاتجاهات جميعها عبر الهواء، ومن ثَمَّ يمكن اعتراض هذه البيانات من قبل المخترقين ونسخها والاطلاع عليها أو تعديلها؛ ولذلك كان لابدَّ من وجود وسائل حماية إضافية لحماية البيانات التي تُنْقَلُ عبرها، ولتحقيق ذلك نحتاج لتطبيق تقنيات التشفير، لضمان عدم تمكن أحد من الاطلاع على البيانات المرسلة ما لم يملك مفتاح التشفير الخاص بالشبكة.

ومن أجل هذا تم إطلاق بروتوكول الحماية المكافئة لحماية الشبكات السلكيةWired Equivalent Privacy WEP الذي كان الهدف منه الحصول على مستوى الحماية نفسه الموجود في الشبكات السلكية، لكن سرعان ما تبيَّنَ أنَّ هذا البروتوكول يحتوي على العديد من الثغرات الأمنية، ويوجد العديد من الهجمات التي تستهدفه ، والتي أدت في النهاية إلى كسر حماية هذا البروتوكول كلّه.

سُلِطَ في هذا البحث الضوء على بعض هجمات استعادة المفتاح key Recovery attacks التي استهدفت هذا البروتوكول وجرى التركيز على الهجمات التي اِقْتُرِحَت من قبل شخص يدعى كورك، إذْ دُرِسَتْ واسْتُخلِصَتْ القواعد والمعادلات التي تعتمد عليها هذه الهجمات ومن ثم نُفِذَتْ بعض هذه الهجمات، ودُرِسَ سلوكها، وقُيِّمَ عملها وقُورِنَ فيما بينها.

### 1-1- محفزات البحث:

مع ازدياد تطور النظم المعلوماتية، وتشعبها، وتضخم الشبكات الواصلة بينها، واتساع انتشار الشبكات اللاسلكية، وتنوع تطبيقاتها، وازدياد الضغط عليها واستخدام البروتوكولWEPفي هذه الشبكات وظهور الثغرات الأمنية لهذا البروتوكول وسهولة كسر حمايته، هذا دفع بالتوجه إلى بروتوكولات حماية أكثر وثوقية وأكثر أمنا.

### 1-2- أهداف البحث:

هَدَفَ هذا البحث إلى شرح بروتوكول الحماية المكافئة لحماية الشبكات اللاسلكيةWEP وآلية عمله ،وخوارزمية التشفير المستخدمة ونقاط ضعفه، والهجمات التي تستهدفه وخوارزمية التشفير RC4 وتحليل مبدأ عملها ونقاط ضعفها. والهجمات التي تستهدف الشبكات التي تستخدم البروتوكول WEP والمعتمدة على نقاط ضعف الخوارزمية RC4.

### 1-3- أهمية البحث:

تكمن أهمية هذا البحث في إبراز الثغرات الأمنية للبروتوكولWEP وسهولة كسر حمايته ، وذلك بهدف التوجه إلى بروتوكولات حماية أكثر وثوقية وأمن ،والبحث في تقييم هجمات كورك والمقارنة فيما بينها من حيث فعاليتها، ووقت تنفيذها، وإمكانية إجراء تحسينات عليها.

## 2- خوارزمية التشفير RC4:

صممت هذه الخوارزمية من قبل Ron Rivest عام 1987 ،وبقيت هذه الخوارزمية سرية حتى عام 1994 .

تستخدم هذه الخوارزمية في البروتوكول SSL/TLS، والبروتوكول WEP و TKIP فضلاً عن العديد من البروتوكولات والتطبيقات. وتتكون خوارزمية التشفير RC4 من خوارزميتين هما:

### 2-1 خوارزمية جدولة المفتاح:

RC4 Key Scheduling Algorithm KSA

يتم فيها إعادة توزيع مصفوفة الأعداد الصحيحة $s\ \{0,\ldots n1\}$ وذلك بالاعتماد على قيم مفتاح التشفير k، ونبين فيما يأتي خطوات هذه الخوارزمية:

**Initialization:**

For i = 0. . . 255

S[i ] = i

j = 0

**Scrambling:**

For i = 0. . . 255

j = j + S[i] + K[i mod Len[K]] mod 256

**Swap**(S[i]، S[j])

**2-1 خوارزمية توليد المفتاح:**

Pseudo Random Generator Algorithm PRGA

في البداية تُعْطَى قيمة صفر لكل من الدليلين i و j، ثم يتم الدخول إلى حلقة، يتم ضمنها زيادة i كعداد وزيادة jبالاعتماد على قيمتها السابقة وعلى قيمة S[i]، ويتم تبديل قيم Sالخاصة بالدليلين i، j(أي يتم التبديل بين S[i] و S[j]) ويكون الخرج S[S[i] + S[j]] .

**Initialization:**

i = 0

j = 0

**Generation loop:**

i = i + 1

j = j + S[i]

Swap(S[i]، S[j])

Output X = S[S[i] + S[j]]

## 3- بروتوكول الحماية المكافئة لحماية الشبكات السلكية:

أدرك الباحثون في معهد IEEE هشاشة الشبكات اللاسلكية في مواجهة المخاطر الأمنية، لذلك صَمَّمَتْ هذه الهيئة بروتوكول حماية أطلقت عليه اسم بروتوكول الحماية المكافئة لحماية الشبكات السلكية ( Wired Equivalent Privacy).

وتتلخص الأهداف الرئيسة لبروتوكول WEP في توفير عناصر أمن المعلومات الثلاث (المصادقة Authentication، السرية Confidentiality، سلامة المحتوىIntegrity).

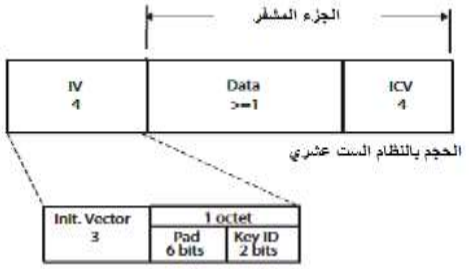
اعتمد بروتوكول WEP في بنيته على خوارزمية التشفير RC4، مع مفتاح مشترك بطول يساوي 40 أو 104 بت.

تتكون بنية وحدة المعطيات في هذا البروتوكول WEP من الثلاثة أقسام MPDU MAC Protocol Data Unit رئيسة هي:

البيانات وقيمة التحقق من الصحة Integrity Check Value (ICV)، وشعاع التهيئة (قيمة التهيئة) Initialization Vector (IV) وتُغَلَّفُ هذه الوحدة MPDU بترويسة 802.11.

في هذا البروتوكول تُشَفَّرُ رسالة البيانات الفعلية وقيمة التحقق من الصحة فقط، في حين يُرْسَلُ شعاع التهيئة وترويسات. 802 11 دون تشفير.

الشكل (1) يبيّن هذه البنية:




**الشكل (1) وحدة معطيات البروتوكول ويب WEP MPDU**

**3-1-عملية التشفير:** تُشَفَّرُ إطارات البيانات Data frames جميعها عند استخدام هذا البروتوكول في حين لا يتم تشفير إطارات الإدارة مثل beacon frames، acknowledgment frames وغيرها. وتجري عملية التشفير كما يأتي:

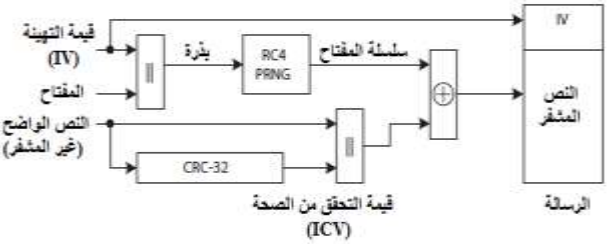
1) تقوم الطرفية باختيار قيمة تدعى شعاع التهيئة أو قيمة التهيئةIV تتكون من 24 بتاً تضاف إلى مفتاح التشفير لتجنب استخدام المفتاح نفسه في تشفير رزمة ثانية، ومن

ثـــمَّ لـــدينا $2^{24}$ مفتـــاح تشـــفير مختلـــف ويكـــون $K = IV \,||\, RK$.

2) تُحْسَبُ قيمة CRC32 لكامل الحمولة الخاصة بالرزمة وتضاف هذه القيمة إلى الحمولة الأصلية، وتدعى هذه القيمة قيمة التحقق من الصحة (ICV) .

3) يُدْخَلُ مفتاح التشفير الخاص بالرزمة K إلى الخوارزمية RC4 لتوليد سلسلة المفتاح key stream.

4) تُكَوَّنُ الرزمة النهائية من النص المشفر فضلاً عن قيمة شعاع التهيئة (IV) مع بعض الحقول الخاصة بالترويسة وتُرْسَلُ للمستقبل.




**الشكل (2) عملية التشفير في البرتوكول ويب**

**3-2-عمليـــة فـــك التشـــفير:** هـــي عمليـــة معاكســـة لعمليـــة التشفير إذْ تبدأ العملية بإضافة شعاع التهيئة IV إلى مفتاح التشفير فتنتج قيمة تُسْتَخدَمُ لاحقاً كدخل للخوارزمية RC4 PRGA لإنتاج سلسلة المفتاح، ومن ثم يتم عمل XOR بـين الـنص المشـفر وسلسـلة المفتـاح للحصـول الرسـالة الصريحة وقيمة التحقق من الصحة ICV، ومن ثم تُمَرَّرُ الرسـالة عبـر خوارزميـة CRC-32 لحسـاب قيمـة أخـرى لـICV وبعدها يتم مقارنـة قيمتـي ICV للتأكد مـن سـلامة محتـوى الرسـالة فـإذا تطابقـت القيمتـان تُمَـرَّرُ الرزمـة وإلا فَتُرْفَضُ.

**3-3-نقاط الضعف في البروتوكول ويب :**

1) **المصادقة Authentication:** تُسْتَخْدَمُ المصادقة ذات المفتاح المشترك key authentication Shared إذْ يقوم المستخدم بطلب الاتصال بالشبكة من نقطة النفاذ، فتستجيب نقطة النفاذ بإرسال سلسلة محارف غير مشفرة تدعى challenge، ليقوم المستخدم بعدها بتشفير هذه السلسلة باستخدام مفتاح التشفير المشترك وإعادة إرسالها إلـى نقطـة النفـاذ. فـإذا مـا قـام المختـرق بالتنصـت sniffing علـى البيانـات المرسـلة، وقـام بنسـخ عمليـة المصـادقة يمكنـه بكـل بسـاطة عمـل XOR بـين الـنص الصـريح المرسـل مـن قبـل نقطـة النفـاذ والـنص المشـفر المرسل من قبل المستخدم فيحصل على مفتاح التشفير.

2) **التحكم بالنفاذ Access Control:** لا يوجد أي تحكم بالنفاذ ضمن البروتوكول WEP سوى عملية المصادقة التي تكلمنا عنها، على كل حال تحتوي معظم التجهيزات علـى إمكانيـة الـتحكم بالعنـاوين الفيزيائيـة MAC التـي يمكنهـا النفـاذ إليهـا، ولكـن هـذه الطريقـة يمكـن تخطيهـا بسهولة باستخدام بعض أوامر لينوكس كما يأتي:

Ifconfig<interface>hw ether <fake-mac>

هذا باعتبار أنَّ العنوان الفيزيائي لا يتم تشفيره ومن ثَمَّ يمكن نسخ العنوان الفيزيائي لأي طرفية شرعية وأن يُسْتَبْدَلَ به العنوان الفيزيائي الخاص بحاسوب المخترق.

3) **إمكانية إعادة إرسال الرزم Replay Protection:** لم يقـدم البروتوكـول WEP أي وسـيلة للحمايـة مـن إعـادة إرسـال الـرزم ومـن ثـمَّ تبقـى الرزمـة صـحيحة لـزمن غيـر محدد ويمكن للمخترق التقاط الرزم ومن ثم إعادة حقنها إلى الشبكةPacket injection.

4) **التـــابع CRC-32:** يعـدُّ CRC-32 تابعـاً جيـداً عنـد استخدامه ضمن سياق كشف الخطأ، ولكن يُسْتَخْدَمُ في WEPللتأكد من صحة البيانات التي تم استقبالها، ويُحَدَّدُ هل تم تعديلها في أثنـاء عمليـة الإرسـال، كمـا أنWEP يسـتخدم عمليـة XOR لتشـفير الـنص الصـريح، وبعمـل ذلك سيتم قلب البتات في مكانها ولا يتم تغيير أماكنها في النص المشفر.

المشكلة الثانيـة فـي التـابع CRC-32 أنَّـه تـابع خطـي؛ وهذا يعني أنـه يمكن التنبؤ ببت الخرج الذي سيتغير في حال تغير بت في الدخل، أي أنَّـه بدون معرفة أي من النص الواضـح Clear text أو قيمـة التحقـق مـن الصـحة،

وباختيار بت في النص الواضح لدينا معلومات عن موقعه يمكن حساب أي بت سيتغير في قيمة التحقق من الصحة بتغير هذا البت، والآن بأخذ بالحسبان حقيقة أنَّ البتات لا يتغير موقعها بعد التشفير، سنرى أنَّه يمكن تطبيق ذلك أيضاً على الرزمة المشفرة.

5) **حجم المفتاح:** عرف المعيار IEEE802.11 حجمين للمفاتيح من أجل البروتوكولWEP وهما 40 بتاً و104 بتاً، فباستخدام مفاتيح ذات حجم 40 بتاً يصبح من السهل اختراق الشبكة عن طريق هجمة المسح الشامل brute force attack إذْ يمكن الحصول على مفتاح التشفير خلال ثوانٍ ،وبتوسيع حجم المفتاح إلى104 بت يصبح من غير الممكن تنفيذ هذه الهجمة.

6) تحتوي خوارزمية التشفير RC4 على ثغرات أمنية يمكن من خلالها تنفيذ العديد من الهجمات، ومن ثَمَّ يمكن من خلالها اختراق الشبكة المحمية بهذا البروتوكول.

7) تُستخدم قيمة IV في البروتوكول WEP لتجنب إعادة استخدام مفتاح التشفير وهي بحجم 24 بتاً ومن ثَمَّ يوجد $2^{24}$ مفتاح تشفير مختلفاً، ولكن هذه المفاتيح تعتبر قليلة، إذْ يمكن استخدامها خلال دقائق في الشبكات المزدحمة، ومن ثَمَّ إعادة استخدام مفتاح التشفير.

## 4- الهجمات التي تستهدف البروتوكول ويب :

يوجد عدد كبير من الهجمات التي تستهدف البروتوكول ويب تحدّثنا في هذه المقالة عن هجمات استعادة المفتاح، إذْ تستغل معظم هذه الهجمات نقاط ضعف خوارزمية التشفير RC4 أو طريقة استخدام هذه الخوارزمية لتشفير الرزم في البروتوكول WEP، على سبيل المثال هجمة FMS وهجمات كورك السبع عشرة وهجمة PTW وهجمة كيلين وغيرها، سنخصص هذه المقالة للحديث عن هجمة FMS وهجمات korek كما سَتُدَرَسُ وتُقَيَّمُ وتُقَارَنُ هذه الهجمات.

**4-1-مصطلحات:** لتسهيل عملية شرح الهجمات نبيَّن فيما يأتي بعض المصطلحات المستخدمة:

1) $S_p$: هي قيمة المصفوفة S في الخطوة P من الخوارزمية KSA.
2) $j_p$: هي قيمة المؤشر j بعد pخطوة من الخوارزمية KSA.
3) K: هي مفتاح التشفير الأساسي (الذي يدخل إلى الخوارزمية لتوليد سلسلة المفتاح).
4) X: هي سلسلة المفتاح (خرج الخوارزمية PRGA).
5) X[0]: البايت الأول من سلسلة المفتاح أي البايت الأول من خرج الخوارزمية PRGA ويكون X [1]X هو البايت الثاني وهكذا.
6) $S^{-1}$[X[0]] : يقصد بها موقع أول بايت من سلسلة المفتاح في المصفوفة S.
7) $S_p^{-1}$[X[0]] : يقصد بها موقع أول بايت من سلسلة المفتاح في المصفوفة S عند الخطوة p من الخوارزمية KSA .
8) k[0]، k[1]،.....k[2] : يقصد بها أول بايت، ثاني بايت، ثالث بايت ... من مفتاح التشفير.
9) عمليات الجمع جميعها تجرىn mod إذْ n=256 على سبيل المثال: $6 + n = 6$ .

**4-2-هجمة FMS :**

هي أول هجمة استعادة مفتاح تستهدف البروتوكول WEPإذْ نُشِرَتْ من قبل Fluhrer، Mantin، Shamir عام 2001، وطُبِّقَتْ هذه الهجمة أول مرة ضمن بيئة شبكة حقيقية من قبل Stubblefield، إذْ لم يُقدم مُصممو هذه الهجمة تطبيقاً عملياً لها.

يعتمد مبدأ عمل هذه الهجمة على افتراض أن المخترق يعرف أول p كلمة من مفتاح التشفير ويريد تطبيق الهجمة من أجل الحصول على قيمةK[p] إذْ أنَّ2=< p، كما تعتمد على افتراض معرفة المخترق قيمة أول كلمة من خرج الخوارزمية RC4-PRGA أي أول كلمة من سلسلة المفتاح، ومن ثَمَّ بإمكانه محاكاة أول p خطوة من الخوارزمية RC4-KSA ومعرفة $S_p$ و $J_p$ فضلاً عن قيمة i.

اعتمد مصممو هذه الهجمة على قيم محددة لشعاع التهيئة أسموها القيم الضعيفة لشعاع التهيئة Weak IV؛ وذلك لإيجاد علاقة تمكنهم من إطلاق الهجمة، فتم الاعتماد على قيم شعاع تهيئة من النمط :

A+3 255 X

واكتشفوا بأنه باستخدام قيم شعاع تهيئة من هذا النمط يمكن اكتشاف قيمة المفتاح k[A+3]، إذْ يعود سبب استخدام الرقم 3هو معرفة المخترق بأول ثلاثة بايتات من مفتاح التشفير، وهي قيمة شعاع التهيئة التي لا يتم تشفيرها كما أسلفنا سابقاً.

مثال: إذا كنا نريد معرفة قيمة K[3] فإنَّنا ننتظر حتى نتلقى قيمة شعاع تهيئة من الشكل255,X،IV=3، ويمكننا الحصول على قيمة K[3] بالاعتماد على معرفتنا بأول بايت خرج من الخوارزمية PRGA، وذلك بالإفادة من خاصية أنَّ أول جزء في جميع رزم شبكات المعيار 802.11 متشابه، إذْ يبدأ بترويسة متحكم الوصلة المنطقية logical Link Control (LLC) متبوعة بترويسة بروتوكول النفاذ للشبكة الفرعية Subnetwork Access Protocol (SNAP) ويكون حجمها ككل 8 بايت، إذْ تكون هاتان الترويستان ثابتتين غالباً في جميع الرزم، الحقل الوحيد المختلف هو آخر بايت في ترويسة SNAP، ويسمى Ether Type؛ وهو يشير إلى البروتوكول الذي غُلِفَتْ الرزمة بواسطته، وتكون قيمة هذا الحقل إمَّا IP أو ARP حصراً في معظم الشبكات، تحجز هاتان الترويستان أول 8 بايت من الرزمة ،ومن ثَمَّ يمكن معرفة أول بايت من سلسلة المفتاح بمجرد عمل XORقيمة هاتين الترويستين مع بداية الرزمة.

نقوم في البداية بمحاكاة أول ثلاث خطوات من الخوارزمية KSAإذْ تكون S كما يأتي:

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | |
|---|---|---|---|---|---|---|---|---|
| $S_0$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | ……. |

$i= 0$، $j_1=k[0]=3$

بإجراء عملية التبديل بين S[i] وS[j]:

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | |
|---|---|---|---|---|---|---|---|---|
| $S_1$ | 3 | 1 | 2 | 0 | 4 | 5 | 6 | ……. |

$i = 1$ , $j_2=j_1+S[1]+k[1]=3+1+255=3$

بإجراء عملية التبديل بين S[i] وS[j] :

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | |
|---|---|---|---|---|---|---|---|---|
| $S_2$ | 3 | 0 | 2 | 1 | 4 | 5 | 6 | ……. |

$i = 2$ , $j_3=j_2+S[2]+k[2]=3+2+X=5+X$

بإجراء عملية التبديل بين S[i] وS[j] :

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | |
|---|---|---|---|---|---|---|---|---|
| $S_3$ | 3 | 0 | $S_3[5+X]$ | 1 | 4 | 5 | 6 | ……. |

$i= 3$, $j_4=j_3+S[3]+k[3]=5+X+1+K[3]=6+X+K[3]$

| | 0 | 1 | 2 | 3 | 4 | … |
|---|---|---|---|---|---|---|
| $S_4$ | 3 | 0 | $S_3[5+X]$ | $S_3[6+X+K[3]]$ | 4 | … |

نفترض بأنَّ ثلاث قيم لا تتعرض لأي تغيير في بقية خطوات الخوارزمية KSA، وهي S[3],S[1],S[0] وهذا هو مبدأ عمل الهجمة، وهذا يتم باحتمال:

$$P_{fms} = (\frac{256-q}{256})^{(256-p)} = (\frac{253}{256})^{253} = 0.05$$

إذْ إنَّ q: عدد العناصر التي يجب ألَّا تتغير في بقية خطوات KSA.

P: عدد الخطوات من خوارزمية KSA التي يجب أن لا تتغير هذه القيم من بعدها.

أي أنَّ احتمال نجاح هذه الهجمة من أجلK[3] هو5%.

نقوم بعد ذلك بمحاكاة أول خطوة في الخوارزمية PRGA والحصول على أول كلمة خرج:

| | 0 | 1 | 2 | 3 | 4 | … |
|---|---|---|---|---|---|---|
| $S$ | 3 | 0 | ? | $S_3[6+X+K[3]]$ | ? | … |

$i=1$ , $j=S[1]=0$

يتم التبديل بين[i]S و[j]S:

| | 0 | 1 | 2 | | 3 | 4 | … |
|---|---|---|---|---|---|---|---|
| S | 0 | 3 | ? | $S_3[6+X+K[3]]$ | | ? | … |

$$X[0]=S[S[i]+S[j]]= S[S[1]+S[0]]=S[3] = S_3[6+X+K[3]]$$

بحل المعادلة من أجل [3]K:

$$K[3]=S_3^{-1}[X[0]]-6-X$$

بتعويض قيمة [3]K في $j_4$ نحصل على:

$$j_4=6+X+K[3]=S_3^{-1}[X[0]]-X-6+X+6 =S_3^{-1}[X[0]]$$

ولدينا:

$$j_4=j_{p+1}=S_3[3]+j_3+k[3]$$
$$K[3]=j_4-S_3[3]-j_3$$

هذا ينتج:

$$K[3]=S_3^{-1}[X[0]]-S_3[3]-j_3$$

ويمكن تعميم هذه النتيجة كما يأتي:

$$F_{\text{fms}}(K[0]\dots K[p-1]) = S_p^{-1}[X[0]]-S_p[p]-j_p$$

إذْ:

$k[0]\dots k[p-1]$:هي قيم بايتات المفتاح المعروفة قبل الهجمة.

P: هي رقم بايت المفتاح الذي نبحث عنه مثلاً في حالة كنا نبحث عن [3]K فإنَّ P=3، واعتمدنا هذا حتى نهاية البحث.

اِقْتُرِحَ حل لهجمة FMS بفلترة القيم الضعيفة لشعاع التهيئة التي تعتمد عليها هذه الهجمة وعدم استخدامها في تشفير الرزم المرسلة على الشبكة.

**4-3-هجمات كورك korek attacks:**

قام كورك بنشر كود يحتوي على 17 هجمة تستهدف البروتوكول WEP على منتدى NetStumbler، إذْ قام بوضع هذه الهجمات ككود مصدري ولم يقم بشرح هذه الهجمات وشروط تنفيذها، وقد كانت هذه الهجمات نقطة انطلاق للعديد من الهجمات الأخرى إذْ تم الاعتماد عليها في عدد كبير من البحوث اللاحقة لإطلاق هجمات جديدة تستهدف بروتوكول الحماية WEP وقد قللت هذه الهجمات عدد الرزم اللازمة للحصول على مفتاح التشفير بشكل كبير كما سنرى في الجزء العملي، لذلك شرحنا في هذه المقالة آلية عمل هذه الهجمات واستنتجنا المعادلات والعلاقات الخاصة بها ومن ثم نُفِّذَ عدد من هذه الهجمات وقُيِّمَ مدى فاعليتها وقُورِنَتْ بهجمة FMS، ويمكننا تقسيم هذه الهجمات إلى ثلاثة مجموعات:

- المجموعة الأولى: تعتمد على معرفة أول بايت من سلسلة المفتاح (خرج الخوارزمية PRGA).
- المجموعة الثانية: تعتمد على معرفة البايتين الأول والثاني من سلسلة المفتاح (خرج الخوارزميةPRGA).
- المجموعة الثالثة تعتمد على استخدام طرائق عكسية لتقليل فضاء البحث، وتدعى الهجمات العكسية Inverted attacks.

هذه الهجمات لا تعتمد على قيم محددة لشعاع التهيئة، وإنَّما تعتمد على سلوك الخوارزميتين KSA وPRGA، ولذلك لا يمكن تطبيق فلاتر معينة في نقطة النفاذ لمنع الهجمات كما في هجمة FMS.

نقوم في هذه الهجمات بمحاكاة أول p خطوة من الخوارزمية KSA وحفظ كل قيمة يأخذها البارامتر j وبناء جدول يحتوي على موقع كل عنصر في S في أثناء عمل KSA، أي في كل خطوة من الخوارزمية KSA تُحْفَظُ قيم عناصر S في هذا الجدول نسميها $S_p$ إذْ p رقم الخطوة. ويمكن حساب احتمال نجاح كل هجمة من هذه الهجمات بالطريقة نفسها التي اتبعناه لحساب احتمال نجاح هجمة FMS .

**4-3-1 هجمة كورك الأولى KorekA_s5_1:**

احتمال نجاح هذه الهجمة في حالة كان الهدف من الهجمة الحصول على البايت الرابع من مفتاح التشفير أي أن p=3 هو: $(\frac{253}{256})^{256-p} \approx 5.07\%$

**4-3-2 هجمة كورك الثانية Korek A_s13:**

احتمال نجاح هذه الهجمة في حالة كان الهدف من الهجمة الحصول على البايت الرابع من مفتاح التشفير أي أن p=3 هو: $(\frac{254}{256})^{256-p} \approx 13.75\%$

**4-3-3 هجمة كورك الثالثة Korek A_u13_1:**

احتمال نجاح هذه الهجمة في حالة كان الهدف من الهجمة الحصول على البايت الرابع من مفتاح التشفير أي أن p=3هو: $(\frac{254}{256})^{256-p} \approx 13.75\%$

**4-3-4 هجمة كورك الرابعة Korek A_u5_1:**

احتمال نجاح هذه الهجمة في حالة كان الهدف من الهجمة الحصول على البايت الرابع من مفتاح التشفير أي إنَّ p=3هو: $(\frac{253}{256})^{256-p} \approx 5.07\%$

**4-3-5 هجمة كورك الخامسة KorekA_u5_2:**

احتمال نجاح هذه الهجمة في حالة كان الهدف من الهجمة الحصول على البايت الرابع من مفتاح التشفير؛ أي إنَّ p=3هو: $(\frac{253}{256})^{256-p} \approx 5.07\%$

**4-3-6 هجمة كورك السادسة Korek A_u13_2:**

احتمال نجاح هذه الهجمة في حالة كان الهدف من الهجمة الحصول على البايت الرابع من مفتاح التشفير؛ أي إنَّ p=3هو: $(\frac{254}{256})^{256-p} \approx 13.75\%$

**4-3-7 هجمة كورك السابعة Korek A_U13_3:**

احتمال نجاح هذه الهجمة في حالة كان الهدف من الهجمة الحصول على البايت الرابع من مفتاح التشفير؛ أي إنَّ p=3 هو: $(\frac{254}{256})^{256-p} \approx 13.75\%$

**4-3-8 هجمة كورك الثامنة KorekA_u5_3 :**

احتمال نجاح هذه الهجمة في حالة كان الهدف من الهجمة الحصول على البايت الرابع من مفتاح التشفير؛ أي إنَّ p=3هو :$(\frac{253}{256})^{256-p} \approx 5.07\%$

**4-3-9 هجمة كورك التاسعة KorekA_s3 :**

احتمال نجاح هذه الهجمة في حالة كان الهدف من الهجمة الحصول على البايت الخامس من مفتاح التشفير p=4 هو: $(\frac{253}{256})^{256-p} \approx 5.13\%$

هذه المجموعة من الهجمات تعتمد على المعرفة المسبقة بثاني بايت من الخرج X[2]، وكما نلاحظ أنَّ في هذه الهجمة يشترط معرفة أول أربعة بايتات من الخرج.

**4-3-10 هجمة كورك العاشرة KorekA_u15 :**

احتمال نجاح هذه الهجمة في حالة كان الهدف من الهجمة الحصول على البايت الرابع من مفتاح التشفير أي إنَّ p=3 هو: $(\frac{254}{256})^{256-p} \approx 13.75\%$

**4-3-11 هجمة كورك الحادية عشرة KorekA_s5_2 :**

احتمال نجاح هذه الهجمة في حالة كان الهدف من الهجمة الحصول على البايت الرابع من مفتاح التشفير أي إنَّ p=3 هو: $(\frac{253}{256})^{256-p} \approx 5.07\%$

**4-3-12 هجمة كورك الثانية عشرة KorekA_s5_3 :**

احتمال نجاح هذه الهجمة في حالة كان الهدف من الهجمة الحصول على البايت الرابع من مفتاح التشفير أي إنَّ p=3 هو:$(\frac{253}{256})^{256-p} \approx 5.07\%$

**4-3-13 هجمة كورك الثالثة عشرة KorekA_4_s13 :**

احتمال نجاح هذه الهجمة في حالة كان الهدف من الهجمة الحصول على البايت الخامس من مفتاح التشفير؛ أي إنَّ p=4 هو:$(\frac{254}{256})^{256-p} \approx 13.85\%$

في هذه الهجمة نفترض أننا نعرف كلّاً من قيم k[0],k[1],k[2],k[3] ونبحث عن قيمة k[4] ومن ثَمَّ p=4، بمعنى آخر يُشترط في هذه الهجمة معرفة أول أربعة بايتات من المفتاح، كما نفترض أنَّ $j_{p+1} = S_p^{-1}[0]$؛ وذلك لوضع الصفر في S[4]، ومن ثم وضع هذه القيمة أي الصفر في X[1].

**4-3-14هجمة كورك الرابعة عشرة Korek A_4_u5_1**

احتمال نجاح هذه الهجمة في حالة كان الهدف من الهجمة الحصول على البايت الخامس من مفتاح التشفير؛ أي إنَّ p=4هو :$(\frac{253}{256})^{256-p} \approx 5.13\%$

نفترض في هذه الهجمة أنَّ $J_{p+1} = S^{-1}[254]$ وذلك لوضع هذه القيمة في S[4] وأن يأخذX[1] القيمة الموجودة في الدليل صفر أي $X[1]=S^{-1}[0]$ .

**4-3-15هجمةكورك الخامسة عشر KorekA_4_u5_2**

احتمال نجاح هذه الهجمة في حالة كان الهدف من الهجمة الحصول على البايت الخامس من مفتاح التشفير أي إنَّ p=4 هو: $(\frac{253}{256})^{256-p} \approx 5.13\%$

نفترض في هذه الهجمة أن $J_{p+1} = S^{-1}[255]$ وذلك لوضع هذه القيمة في S[4] وأن نعطي X[1] القيمة الموجودة في الدليل واحد أي $X[1]=S^{-1}[1]$.

**4-3-16 هجمة كورك السادسة عشر Korek A_u5_:**

احتمال نجاح هذه الهجمة في حالة كان الهدف من الهجمة الحصول على البايت السابع من مفتاح التشفير أي أنَّ p=6هو: $(\frac{253}{256})^{256-p} \approx 5.25\%$

نفترض في هذه الهجمة معرفة قيم كل من k[0],k[1],k[2],k[3],k[4],k[5] ونبحث عن قيمة k[6] ومن ثَمَّ p=6

**4-3-17- هجمة كورك السابعة عشرة KorekA_neg:**

هذه الهجمة عبارة عن مجموعة من الهجمات التي قدمها كورك والهدف منها هو تقليص مجال البحث عن المفتاح المطلوب، وقام كورك، بتحديد أربعة أنماط غير مقبولة لقيم المفتاح؛ وذلك بالنسبة إلى أربع حالات خاصة بقيم المصفوفةS في الخطوة P من الخوارزميةKSA، وَعَدَّ هذه القيم كفلاتر لتحديد القيم المفيدة من المفاتيح، دَرَسْنا الحالات الأربع لقيم المصفوفة S في الخوارزمية KSA وقيم المفتاح غير المقبولة بالنسبة إلى كل حالة:

**1)** الحالة الأولى: عندما تكون قيمة المصفوفة S في الخطوة P من الخوارزمية KSA كما يأتي :

| | 0 | 1 | 2 | 3 | 4 | ..... |
|---|---|---|---|---|---|---|
| S | ? | 2 | 0 | ? | ? | ..... |

إذا كانت كل من S[1] و S[2] لا تشتركان بأي تبديل في بقية خطوات الخوارزمية KSA، وعندما نصل إلى الخوارزمية PRGA فإنَّ X[0]=2 كما يأتي:

| | 0 | 1 | 2 | 3 | 4 | ..... |
|---|---|---|---|---|---|---|
| S | ? | 2 | 0 | ? | ? | ..... |

i=1 , j=S[1]=2

بالتبديل بين S[i] و S[j]:

| | 0 | 1 | 2 | 3 | 4 | ..... |
|---|---|---|---|---|---|---|
| S | ? | 0 | 2 | ? | ? | ..... |

X[0]=S[S[1]+S[2]]=S[2]=2

ومن ثَمَّ إنَّ هذه المجموعة تتلخص بتجاهل القيم التي تؤثر في قيمة كل من S[1] و S[2] وعليه يمكن أن نرفض بعض قيم المفتاح وفقاً للقاعدتين الآتيتين:

$K[p] \neq 1-S[p]-j_p$

$K[p] \neq 2-S[p]-j_p$

وذلك لأنَّ $j_{p+1} = j_p + S_p[p] + k[p]$ ومن ثَمَّ باستثناء القيمتين السابقتين نتجنب تبديل قيمتي S[2],S[1].

**2) الحالة الثانية:** في هذه المجموعة يجب تجاهل قيم المفتاح التي تؤدي إلى عدم تحقق الشروط الآتية:

- S[2]=0 .
- X[1]=0 .
- S[1]≠2 و X[0]≠2: وذلك لاستثناء المجموعة السابقة.

نظراً إلى S[1]≠2 فإنَّ قيمة S في الخوارزمية KSA تكون من النمط:

| | 0 | 1 | 2 | 3 | 4 | ..... |
|---|---|---|---|---|---|---|
| S | ? | α | 0 | ? | ? | ..... |

إذْ إنَّ α≠ 2.

عند الوصول إلى الخوارزمية PRGA تكون S على الشكل الآتي:

| | 0 | 1 | 2 | 3 | ... | α | ..... |
|---|---|---|---|---|---|---|---|
| S | ? | α | 0 | ? | ... | ? | ..... |

i=1 ,j= α

بالتبديل بين S[i] و S[j]:

| | 0 | 1 | 2 | 3 | ... | α | ..... |
|---|---|---|---|---|---|---|---|
| S | ? | ? | 0 | ? | ... | α | ..... |

i=2 , j= α

بالتبديل بين S[i] و S[j] :

| | 0 | 1 | 2 | 3 | … | α | …… |
|---|---|---|---|---|---|---|---|
| S | ? | ? | α | ? | … | 0 | …… |

$X[1]=S[S[2]+S[\alpha]]=S[\alpha]=0$

في هذه الحالة يجب على S[2] إنَّ لا تتغير ومن ثَمَّ نتجاهل القيم التي تؤدي إلى تغييرها عن طريق العلاقة الآتية:

$K[p] \neq 2\text{-}S[p]\text{-}j_p$

3) **الحالة الثالثة** : في هذه المجموعة عندما تكون S[1]=1 إذا لم تتعرض هذه القيمة لأي تغيير ينتج عنه X[0]=S[2] وذلك لأنَّ:

$X[0]=S[S[1]+S[S[1]]]=S[1+S[1]]=S[1+1]=S[2]$

للحفاظ على هذا السلوك للخوارزميتينKSA و PRGA يجب تجاهل قيم المفتاح التي تؤدي إلى تغيير S[1]، أو S[2] وفق العلاقتين الآتيتين :

$K[p] \neq 1\text{-}S[p]\text{-}j_p$

$K[p] \neq 2\text{-}S[p]\text{-}j_p$

4) **الحالة الرابعة:** المجموعة الأخيرة من المفاتيح التي اقترح كورك تجاهلها هي المجموعة التي ينتج عنها تغيير قيمة S[1] أو S[0]؛ وذلك في حالة أردنا أن تكون S[1]=0 و S[0]=1 حتى نهاية الخوارزمية KSA وينتج عنها X[0]=1، ويكون سلوك الخوارزمية PRGA كما يأتي:

| | 0 | 1 | 2 | 3 | 4 | …… |
|---|---|---|---|---|---|---|
| S | 1 | 0 | ? | ? | ? | …… |

i=1 , j=0

بالتبديل بين S[i] و S[j]:

| | 0 | 1 | 2 | 3 | 4 | …… |
|---|---|---|---|---|---|---|
| S | 0 | 1 | ? | ? | ? | …… |

$X[0]=S[1+0]=S[1]=1$

ولتحقيق ذلك نقوم بتجاهل قيم المفتاح التي تؤثر في قيمة S[1]؛ وهي تمثل بالعلاقة:

$K[p] \neq 1\text{-}S[p]\text{-}j_p$

## 5- التطبيق العملي و النتائج:

طبَّقْنا في هذا البحث عدداً من هجمات كورك لاستعادة مفتاح التشفير في الشبكة اللاسلكية، إذْ جرى العمل ضمن بيئة نظام التشغيل Backtrack live CD، وهو نسخة من نظام التشغيل لينوكس أبونتو Linux Ubuntu خاصة بالمخترقون Attackers، إذْ تحتوي على الأدوات جميعها التي يستخدمها المخترقين في مهاجمة واختراق الشبكات سواء كانت السلكية منها أو اللاسلكية والتطبيقات البرمجية وقواعد البيانات وتطبيقات الويب وغيرها.

يحتوي نظام التشغيل Backtrack على أدوات خاصة باختراق الشبكات اللاسلكية ،مع إمكانية إجراء مسح أمني لها، واكتشاف الثغرات الموجودة ضمن هذه الشبكات. وقد قمنا في هذا البحث بالاعتماد على مجموعة الأدوات suite Aircrack-ng وهي عبارة عن مجموعة أدوات مفتوحة المصدر Open source، يمكن من خلالها إطلاق عدد كبير من الهجمات التي تستهدف الشبكات اللاسلكية، وتكمن قوة هذه الأدوات في كونها مفتوحة المصدر، بحيث يمكن للباحثين التعديل على الكود الخاص بالهجمات، وعمل هجمات جديدة خاصة ببحوثهم وتقييمها ونشرها.

وقدتم تضمين الكود الخاص بهجمات كورك السبع عشرة ضمن أداة في هذه المجموعة تدعى Aircrack-ng.

وتتلخص خطوات البحث بما يأتي:

1) تطبيق هجمة FMS وتقييم عملها.
2) استخلاص الكود المصدري الخاص بهجمات كورك من الأداة Aircrack-ng، ودراسة الكود الخاص بكل هجمة واستخلاص شروطها ومحاكاة عملها.
3) تطبيق عدد من هذه الهجمات وتقييم عملها ودراسة احتمال نجاح هذه الهجمات.
4) تطبيق هجمة كورك العامة، وهي هجمة تتضمن تطبيق هجمات كورك السبع عشرة دفعة واحدة وتقييم عملها.

5) إجراء مقارنة بين هجمات كورك وهجمة FMS، إذْ إنَّ هجمات كورك جاءت كتحسين لهجمة FMS التي تعتمد على قيم محددة لشعاع التهيئة كما ذكرنا سابقاً.

**5-1- بيئة العمل:**

أُجْرِيَ التطبيق في بيئة شبكة لاسلكية تتكون من:

1) نقطة نفاذ AP من نوع Dlink: تم تفعيل البروتوكول WEP كوسيلة حماية ضمنها.
2) مستخدمون متصلون بالشبكة: عبارة عن حاسوبين محمولين بالمواصفات الآتية:
- حاسوب محمول Compaq Presario 2100 يعمل كمخدم server ضمن الشبكة يحتوي على بيانات تُسْتَخْدَمُ من قبل المستخدمين على الشبكة.
- حاسوب محمول DELL Vostro يعمل كزبون Client يقوم بنسخ بيانات عن طريق الشبكة ومن ثَمَّ توليد دفق بيانات على الشبكة.
3) حاسوب محمول DELL Inspiron 1525 يعمل كمخترق تم تنصيب نظام التشغيل Backtrack5R2 عليه، إذْ يقوم بالتنصت Sniffing على دفق البيانات على الشبكة، وتخزين الرزم Packets ضمن ملف.

ومن المهم أن يدعم محول الشبكة اللاسلكية Wi-Fi Adapter في حاسوب المخترق العمل ضمن نمط المراقبة Monitoring mode، وذلك من أجل التقاط البيانات من الشبكة لاستخدامها في عملية الحصول على مفتاح التشفير من خلال تطبيق الهجمات عليها.

**5-2-خطوات تنفيذ الهجمات:**

1) تفعيل نمط المراقبة ضمن محول الشبكة اللاسلكية في حاسوب المخترق.
2) التنصت والتقاط الرزم من الشبكة Packets sniffing من أجل تنفيذ الهجمات، وهنا يجب التقاط عدد مناسب من رزم البيانات Data Packetsيختلف بحسب الهجمة.
3) لتسريع عملية الاختراق والتقاط أكبر عدد من الرزم يُنَفِّذُ المخترق تنفيذ هجمات مصادقة وهمية Fake Authentication، فضلاً عن توليد رزمARP وحقنها للشبكة ، وذلك بهدف توليد دفق بيانات على الشبكة.
4) بعد التقاط عدد مناسب من الرزم يتم تُنَفَذُ الهجمات ، إذْ يختلف عدد الرزم المطلوب حسب الهجمة، كما ذكرنا سابقاً.

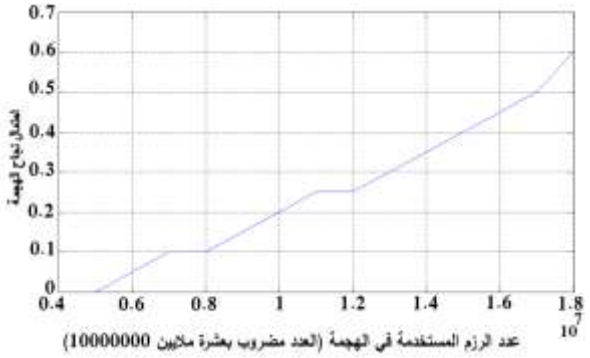
## 5-3-النتائج:

دَرَسْنَا في هذا البحث عينات إحصائية لنسبة نجاح كل هجمة، وذلك بتنفيذ الهجمة 20 مرة عند كل قيمة محددة لعدد الرزم، ومن ثم حُسِبَ احتمال النجاح عند هذه القيمة وذلك بالاعتماد على عدد المرات التي تم الحصول فيها على مفتاح التشفير الخاص بنقطة النفاذ.

**5-3-1- تقييم احتمال نجاح هجمة FMS :**

عند تطبيق هجمة FMS على نقطة النفاذ ضمن بيئة الشبكة التي تم ذِكرَتْ، وجدنا أنَّ هذه الهجمة تحتاج إلى عدد كبير من الرزم حتى يتم الحصول على مفتاح التشفير، إذْ بدأ نجاح الهجمة عند ستة ملايين رزمة باحتمال 0.05، وهو ما يعادل نجاحها مرة واحدة خلال تنفيذ الهجمة عشرين مرة عند هذا العدد من الرزم، ثم بدأ احتمال النجاح بالزيادة بزيادة عدد الرزم حتى وصلنا إلى احتمال نجاح 0.6 عندما وصل عدد الرزم التي جمعت 18 مليون رزمة من الشبكة ، وهو ما يعادل نجاح الهجمة 12 مرة من أصل عشرين تجربة.

الشكل(3) الآتي يبيّن تقييم احتمال نجاح هذه الهجمة:

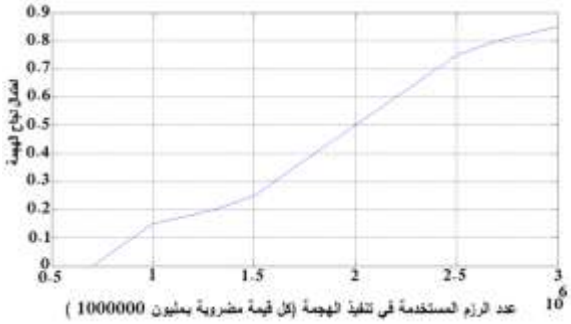



**الشكل(3) احتمال نجاح هجمة FMS**

أما بالنسبة إلى هجمات كورك فقد طَبَّقنا ثلاث هجمات منفردة ودُرِسَتْ وقُيِّمت نسبة النجاح في كل منها كمثال على تطبيق هجمات كورك منفردة، ومن ثم طُبِقَتْ هجمة كورك العامة.

**5-3-2 تقييم احتمال نجاح هجمة كورك الأولى:**

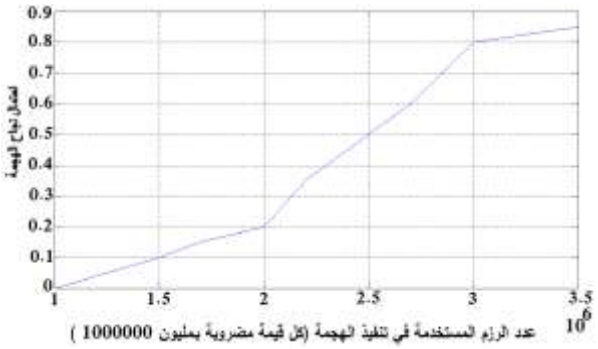
نلاحظ عند تنفيذ هذه الهجمة التحسن الكبير باحتمال نجاحها مقارنة بهجمة FMS، إذْ وصل احتمال نجاحها إلى 0.15 عندما كان عدد الرزم المستخدمة مليون رزمة، وهو ما يعادل نجاحها ثلاثة مرات خلال تنفيذ الهجمة عشرين مرة عند هذا العدد من الرزم، ثم بدأ هذا الاحتمال يزداد بزيادة عدد الرزم حتى وصل إلى أكثر من 0.8 بوصول عدد الرزم إلى ثلاث ملايين رزمة، والشكل (4) يبيّن احتمال نجاح هذه الهجمة:




**الشكل(4) احتمال نجاح هجمة كورك الأولى**

**5-3-3- تقييم احتمال نجاح هجمة كورك الثانية :**

تبدأ هذه الهجمة بالنجاح عندما يصل عدد الرزم إلى مليون ونصف؛ وذلك باحتمال 0.1، ويبدأ هذا الاحتمال بالتحسن حتى يصل إلى0.85 عندما وصل عدد الرزم إلى أكثر ثلاثة ملايين رزمة، والشكل5 يبيّن ذلك:

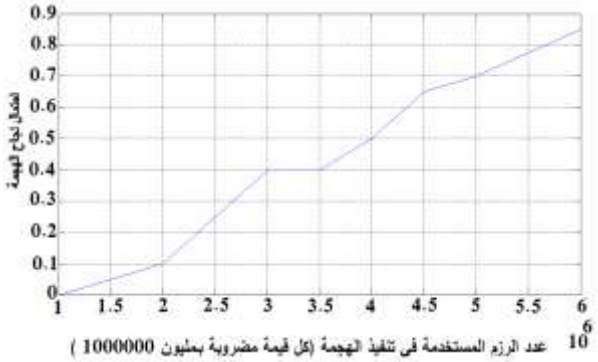



**الشكل (5) احتمال نجاح هجمة كورك الثانية**

**5-3-4- تقييم احتمال نجاح هجمة كورك السادسة:**

نلاحظ بدء نجاح هذه الهجمة عندما وصل عدد الرزم إلى مليون ونصف باحتمال نجاح 0.05، وبدأ احتمال النجاح يزداد حتى وصل إلى 0.85 عندما وصل عدد الرزم إلى ستة ملايين رزمة.

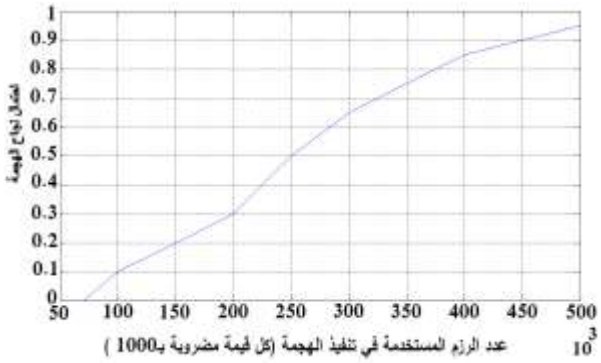
الشكل (6) يبيّن تقييم احتمال نجاح هذه الهجمة:




**الشكل (6) احتمال نجاح هجمة كورك السادسة**

**5-3-5- تقييم احتمال نجاح هجمة كورك العامة:**

نلاحظ في هذه الهجمة التحسن الكبير من إذْ زيادة احتمال النجاح وتقليل عدد الرزم المطلوبة بشكل كبير، إذْ بدأت هذه الهجمة بالنجاح بعدد رزم نحو تسعين ألف رزمة وباحتمال نجاح 0.05 وبدأ هذا الاحتمال بالتحسن حتى وصلنا إلى احتمال نجاح 100% تقريباً عندما وصل عدد الرزم إلى خمسمائة ألف رزمة فما فوق، والشكل (7) يبيّن ذلك:




**الشكل(7)احتمال نجاح هجمة كورك العامة**
**Korek default attack**

**5-4-الاستنتاجات:**

نلاحظ من خلال اختبار نسبة نجاح الهجمات أنَّ نسبة نجاح هجمة FMS هي الأسوأ بين الهجمات إذْ تحتاج هذه الهجمة إلى عدد كبير جداً من الرزم حتى نحصل على مفتاح التشفير، وباحتمال منخفض جداً، بينما نلاحظ التحسن في احتمال النجاح بالانتقال إلى هجمات كورك إذْ انخفض عدد الرزم اللازمة للحصول على مفتاح التشفير انخفاضاً كبيراً، وازداد احتمال نجاح الهجمة، أمَّا عندما نفذنا هجمة كورك العامة فلاحظنا أنَّ هجمات كورك تصبح ذات تأثير كبير، إذْ نحتاج إلى عدد قليل من الرزم للحصول على مفتاح التشفير ،ويمكن الحصول على عدد الرزم المطلوب للهجمة خلال وقت قصير جداً في الشبكات متوسطة الازدحام وحتى العادية.

ومن ثَمَّ فإنَّ هجمات كورك ذات تأثير كبير للحصول على مفتاح التشفير الخاص بالبروتوكول WEP، وهي لا تعتمد على قيم محددة لشعاع التهيئة، ويمكن من خلالها الحصول على مفتاح التشفير خلال وقت قصير.

ومن الجدير بالذكر أنَّه تم الاعتماد على هذه الهجمات كقاعدة لبحوث جديدة تم من خلالها إطلاق هجمات جديدة تستهدف هذا البروتوكول، تم فيها تقليل عدد الرزم اللازمة للهجمة بشكل كبير، لدرجة الحصول على مفتاح التشفير خلال أقل من دقيقة وبنسبة نجاح كبيرة، إذْ يمكن في بعض الحالات الحصول على مفتاح التشفير بنسخ عشرة آلاف رزمة كما في هجمة PTW على سبيل المثال، وسيتم التطرق إلى شرح آلية عمل هذه الهجمات ومحاكاتها وتنفيذها وتقييم عملها في بحوث لاحقة.

## مسرد المصطلحات:

| | |
|---|---|
| Wired Equivalent Privacy | بروتوكول الحماية المكافئة لحماية الشبكات السلكية |
| Pseudo Random Generator Algorithm PRGA | خوارزمية توليد المفتاح |
| RC4 Key Scheduling Algorithm KSA | خوارزمية جدولة المفتاح |
| key stream | سلسلة المفتاح |
| Initialization Vector | شعاع التهيئة أو قيمة التهيئة |
| Integrity Check Value (ICV) | قيمة التأكد من الصحة |
| WEP MPDU MAC Protocol Data Unit | بنية وحدة معطيات في البروتوكول ويب |
| Authentication ، Confidentiality ، Integrity | المصادقة أو الاستيقان، السرية أو الوثوقية، سلامة المحتوى |
| Key recovery attacks | هجمات استعادة المفتاح |
| Shared key authentication | المصادقة باستخدام المفتاح المشترك |
| Packet Sniffing | التنصت أو اشتمام الرزم |
| Clear text | نص واضح |
| Brute force attack | هجمة المسح الشامل |
| Inverted attacks | الهجمات العكسية |
| Attacker | مخترق |
| Packets | رزم |
| Monitoring mode | نمط المراقبة |
| Fake Authentication | استيقان وهمي أو مصادقة وهمية |
| Packet injection | حقن الرزم |
| Weak IV | القيم الضعيفة لشعاع التهيئة |
| server | مخدم |

| | | |
|---|---|---|
| Received | 18/9/2018 | إيداع البحث |
| Accepted for Publ. | 19/11/2018 | قبول البحث للنشر |


# References


1. **Information Technology- telecommunications And Information exchange Between Systems-Local And Metropolitan Area Networks-specific Requirements-part 11: Wireless LANMedium Access Control (MAC) And Physical Layer (PHY) Specifications. ANSI/IEEE Std 802.11، 1999 Edition.**
2. **Stubblefield, A. Ioannidis, J. and Rubin, A. "A Key Recovery Attack on the 802.11b Wired Equivalent Privacy Protocol (WEP)"**
3. **Beck, M. TU-Dresden, Germany "Practical attacks against WEP and WPA" , November 8, 2014**
4. **Tews, E. Buchmann , J. "Attacks on the WEP protocol "December 15, 2014**
5. **Fluhrer,S. Mantin, I. A.Shamir," Weaknesses in the key scheduling algorithm of RC4",Springer , 2011.**
6. **Tews, E. Attacks on the WEP protocol, Diploma thesis,2015**
7. **Chaabouni. R. Break WEP Faster with Statistical Analysis. June 2016**
8. **Hulton .D. "Practical Exploitation of RC4 Weaknesses in WEP Environments", February 22, 2012**
9. **Tews,E. R.Weinmann, A.Pyshkin," Breaking 104 bit WEP in less than 60 seconds", 2014**
10. **Vaudenay,S. Vuagnoux,M." Passive-only key recovery attacks on RC4", 2017**
11. **Halvorsen F.M. "Cryptanalysis of IEEE 802.11i TKIP" Master of Science in Communication Technology ,June 2017**
12. **Beck M. and Tews.E. Practical attacks against WEP and WPA.**
13. **Stubblefield,A. Ioannidis, J. Rubin: A."Using the Fluhrer, Mantin, and Shamir Attack to Break WEP", NDSS 2017**