Evaluation of BB84 Distribution Quantum Key protocol Performance

Dr. Boushra Maala•

(Received 2 / 11 / 2024. Accepted 22 / 12 / 2024)

□ ABSTRACT □

Information and communication technology has developed to an integral part of our lives, and has deeply entered into the folds of culture, economy, defense, society, finance, and regional and international organizations. This development was accompanied by the emergence of major security risks and challenges that threaten society, so there was an urgent need to achieve a good level of security.

Quantum encryption emerged as a qualitative leap to protect data and information by taking advantage of the scientific renaissance in the world of quantum physics. Quantum encryption is a high-tech method for securing digital communications by taking advantage of quantum principles, which are the cornerstone of this encryption, as it relies on taking advantage of the unique properties of quantum particles, which ensures unbreakable encryption.

One of the most famous quantum encryption algorithms is the BB84 algorithm. Therefore, this research aims, on the one hand, to provide a detailed explanation of quantum encryption, and on the other hand, to demonstrate the effectiveness of this algorithm in generating a secure random key to be used in symmetric encryption applications, where distributing the key to users is one of the biggest problems that threaten its safe use. The research also seeks to clarify the effectiveness of this algorithm in detecting any eavesdropper trying to obtain the key.

Keywords: Quantum encryption, quantum bit, quantum key distribution, eavesdropper.

*** AAssociate Professor, Department of Communication and Electronics, Factually of Mechanical and Electrical Engineering, Tishreen University, Lattakia, Syria. boushra.maala@gmail.com**

تقييم أداء بروتوكول توزيع المفاتيح الكمومية BB84

د. بشرى معلا•

(تاريخ الإيداع 2 / 11 / 2024. قُبِل للنشر في 22/ 12 / 2024)

□ ملخّص □

لقد تطورت تكنولوجيا المعلومات والاتصالات تطوراً جعلها جزءاً لا يتجزأ من حياتنا ، ودخلت بشكل عميق في ثنايا الثقافة والاقتصاد والدفاع والمجتمع والمال وفي المنظمات الإقليمية والدولية، رافق هذا التطور ظهور أخطار وتحديات أمنية كبيرة تهدد المجتمع، فكان هناك حاجة ملحة لتحقيق مستوى جيد من الأمن، فظهر التشفير الكمومي كقفزة نوعية لحماية البيانات والمعلومات بالاستفادة من النهضة العلمية في عالم الفيزياء الكمومية، إن التشفير الكمومي هو أسلوب عالي التقنية لتأمين الاتصالات الرقمية من خلال الاستفادة من مبادئ الكم حيث تعد حجر الأساس بالنسبة لهذا التشفير، إذ يعتمد على الاستفادة من الخصائص الفريدة للجسيمات الكمومية مما يضمن تشفيراً غير قابل للكسر، يساعد هذا التشفير على اكتشاف أي اعتراض غير مصرح به فهو يجعل نقل البيانات الخاصة آمناً للغاية من خلال حمايتها من الهجمات المحتملة.

من أشهر خوارزميات التشفير الكمومي خوارزمية BB84، لذا يهدف هذا البحث من جهة أولى لتقديم شرحٍ مفصلٍ عن التشفير الكمومي، ومن جهة ثانية إظهار فعالية هذه الخوارزمية في توليد مفتاح عشوائي آمن ليستخدم في تطبيقات التشفير المتناظر، حيث يكون توزيع المفتاح على المستخدمين إحدى أكبر المشكلات التي تهدد الاستخدام الآمن له، وكما ويسعى البحث إلى إيضاح مدى فعالية هذه الخوارزمية في كشف أي متنصت يحاول الحصول على المفتاح.

الكلمات المفتاحية: التشفير الكمومي، البت الكمي، توزيع المفاتيح الكمي، المتنصت.

• **أستاذ مساعد، قسم هندسة الاتصالات والالكترونيات، كلية الهندسة الميكانيكية والكهربائية، جامعة تشرين، اللاذقية، سورية**
boushra.maala@gmail.com

مقدّمة:

في عصرنا الحالي، تعتمد جميع المؤسسات والشركات في حماية البيانات على التشفير الكلاسيكي، لكن التطور الحاصل في مجال الحوسبة الكمومية سيجعل الحواسيب الكمومية قادرة على كسر التشفير التقليدي. هكذا ستصبح تقنيات الأمن السيبراني التقليدية بلا جدوى.

من هنا انطلقت فكرة استخدام الحوسبة الكمومية لرفع مستوى أمن حماية البيانات، إن ذلك يعتمد بشكل أساسي على فيزياء الكم. ظهرت فيزياء الكم في أوائل القرن العشرين هي فرع من الفيزياء يدرس السلوك والتفاعلات والخصائص الفيزيائية للمادة والطاقة على مستوى الجسيمات الأولية مثل الالكترونات والفوتونات، حيث تُظهر أن هذه الجسيمات لا تتبع مسارات محددة ولا يمكن وصفها بدقة باستخدام مفاهيم مثل الموقع، والسرعة، كما هو الحال في الفيزياء الكلاسيكية بل من خلال دلالات موجية تعطي احتمالات تواجدها في مناطق معينة. وكان اكتشاف التشفير الكمومي وتطوره هو أحد نتائج ظهور وتطور فيزياء الكم، الذي أثبت أنه أكثر مقاومة للهجمات من التشفير الكلاسيكي.

أهمية البحث وأهدافه:

تكمن أهمية هذا الموضوع في حقيقة أن الاستراتيجيات الحالية لتوزيع المفاتيح، والتي تستخدم الحوسبة الكلاسيكية، لها جوانب سلبية خطيرة، مقارنة مع توزيع المفاتيح الكمومية. فمن أجل قناة اتصال محمية بتوزيع المفاتيح الكمومية، يمكن اكتشاف أي دخيل بين طرفين شرعيين باستخدام معايير علم المواد الكمومية التي ظهرت في بداية القرن الماضي، ومنها إرشادات هايزنبيرج، والفخ الكمومي، والتراكب، والانتقال الآني الكمومي، وفرضية عدم الاستنساخ. لذا فإن البحث في هذا الموضوع يعد قضية واعدة وسريعة النمو في مجال أمن البيانات. تعد التقنية الكمومية مقاومة للهجمات الكلاسيكية، وهذا ما يجعل التشفير الكمومي محور اهتمام العديد من الباحثين والمؤسسات في مجال أمن المعلومات، وتستخدم هذه التقنية في العديد من التطبيقات مثل تأمين الاتصالات، والتوقيع الرقمي، والحوسبة الكمومية، والحفاظ على سرية المعلومات الحساسة.

في هذا البحث نحلل فعالية تطبيق بروتوكول توزيع المفاتيح الكمومية BB84 [1,2] في كشف المتنصت على القناة.

طرائق البحث ومواده:

يعتمد هذا البحث على البرنامج CrypTool [3]، والذي يشمل مجموعة واسعة من الأدوات التي تسمح بتشفير وفك تشفير النّصوص، وتحليل الخوارزميات وحتى محاكاة الهجمات السيبرانية لتعلُّم كيفية الدفاع ضد التهديدات الأمنية. كما يستخدم على نطاق واسع في البيئات التعليمية بما في ذلك الجامعات والمدارس وكذلك من قبل الأفراد المهتمين بتعزيز معرفتهم في مجال الأمن السيبراني.

1- مفهوم التشفير الكمومي:

في عصرنا الرقمي، تعتمد جميع المؤسسات والشركات في حماية بياناتها على التشفير. لكن بفضل الحوسبة الكمومية والعمل الدؤوب للباحثين في هذا المجال، ستكون للحواسيب الكمومية القدرة على كسر التشفير التقليدي. كذلك سيصبح الأمن السيبراني بلا جدوى.

إن اكتشاف التشفير الكمومي وتطوره كان نتيجةً لتقدّم متسلسل في الفيزياء النظرية والتجريبية. فهو تقنية تعتمد على فيزياء الكم بشكل رئيس، وهنا يكمن الاختلاف، في حين أن التشفير العادي أو الكلاسيكي هو عملية تحويل النص العادي إلى نص مشفر بحيث لا يمكن قراءته إلا لمن لديه " المفتاح " الصحيح. بينما يعبر التشفير الكمومي عن استخدام خصائص الفيزياء الكمومية لحماية المعلومات وتأمينها بالاعتماد على مفهوم عدم قابلية القياس الكمومي، حيث يتعذر قياس حالة جسيم كمومي دون التأثير عليها، إذ تُستخدم الجسيمات الفردية مثل الفوتونات لنقل المعلومات بطرائق تستغل خصائصها الكمومية مثل التداخل والتشابك الكمومي، فلا يمكن لأي شخص آخر قراءة المعلومات دون أن يؤثر على حالة الجسيم، وبالنتيجة يمكن استخدام هذه الخاصية لاكتشاف أية محاولة للاختراق أو التجسس على المعلومات المشفرة[3,4] .

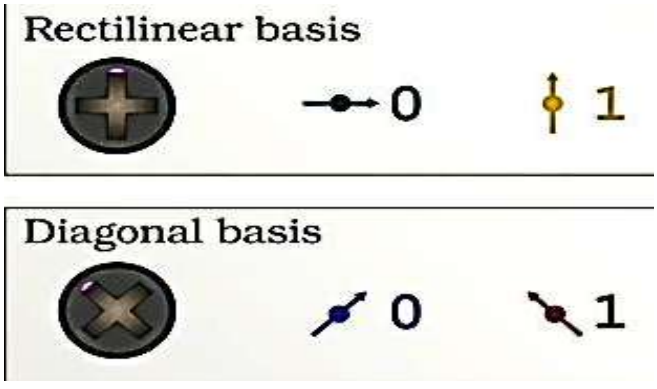
1-1 توزيع المفتاح الكمومي Quantum Key Distribution(QKD)

توزيع المفتاح الكمي هو طريقة آمنة للاتصال بين طرفين لتبادل مفاتيح التشفير السرية لبروتوكولات التشفير معتمدة على فيزياء الكم وكذلك على حسابات رياضية معقدة. مما يجعلها تتطلب قوة معالجة عالية لكسر تلك المفاتيح، ومن النظريات الهامة المعتمدة عليها هي نظرية عدم الاستنساخ والتي تنص على أنه من المستحيل إنشاء نسخ متطابقة من حالة كمية غير معروفة وذلك يمنع المهاجمين من نسخ البيانات ببساطة. فإذا حصل هجوم على نظام ما، فسيتغير النظام بطريقة يعرفها فقط المتحكمون بهذه العملية. مما يجعل من السهل أن يكتشف المستخدمون وجود أي طرف ثالث يحاول الحصول على المفتاح، إذ أنه في حال أُدخلت حالات شاذة سيكتشف ذلك لأن النظام لا يقبل بها [5].

إن توزيع المفاتيح الكمي يعتمد على إرسال ملايين من الفوتونات من الضوء عبر كابل الألياف البصرية، ولكل فوتون بالطبع حالة كمية عشوائية، تشكّل الفوتونات المرسلة سلسلة من الأصفار والواحدات والتي تسمّى الكيوبت (qubit) أو البت الكمومي هو نظير البت في الحواسيب الكلاسيكية. مثلاً البت في الحواسيب الكلاسيكية يمكن أن يكون إما 0 أو 1، بينما الكيوبت أو البت الكمومي يعتمد على خواص فيزياء الكم فيكون في حالة تراكب تمثّل 0 و1 في نفس الوقت. للتعرف أكثر سنوضح فيما يأتي مفهوم الاستقطاب [6] .

1-1-1 مفهوم الاستقطاب:

ينقل المرسل الفوتونات عبر مستقطب يمنحها بشكل عشوائي واحداً من أربعة استقطابات هي: عمودي وأفقي و45 و-45 درجة أو 135 درجة ، في الشكل (1) يمكن ملاحظة قاعدتين إما مستقيمة أو قطرية.



الشكل (1) : قاعدتي الاستقطاب

من ثم تنتقل الفوتونات إلى جهاز الاستقبال، ويُستخدم مقسمان لحزمة الفوتونات (أفقي ورأسي) لقراءة كل فوتون، لا يعرف الطرف المستقبل أي تقسيم للحزمة يمكن استخدامه لكل فوتون لذا عليه أن يخمّن أي منهما هو المستخدم. بمجرد إرسال الفوتونات والوصول إلى جزء التّخمين، يخّبر جهاز الاستقبال المرسل عن مقسم الحزمة الذي استخدمه لكل من الفوتونات في التسلسل المرسل، هنا يُقارن المرسل هذه المعلومات بتسلسل المستقطبات المستخدمة لإرسال المفتاح ويتجاهل الفوتونات التي قُرِأت بجهاز تقسيم الحزمة ويصبح تسلسل البتات هو المفتاح.

فإذا قُرِأ أو نُسخ الفوتون بواسطة المهاجم فإن حالة الفوتون ستتغير، وسيكتشف المستقبل هذا التغيير. من هنا يتضح أنه ليس من الممكن قراءة أو نسخ أو إعادة توجيه الفوتون لأن ذلك سيكشف المهاجم في كل الأحوال. يوجد العديد من برتوكولات توزيع المفاتيح الكمومية، اخترنا في هذا البحث تقييم إحدى هذه البروتوكولات وهو BB84 وذلك لأنه الأكثر شيوعاً.

2. البروتوكول (Bennett, Brassard 1984)BB84 لتوزيع المفاتيح الكمومية:

اقترح هذا البروتوكول من قبل تشارلز بننيت وجيلس براسارد كأول بروتوكول توزيع المفتاح الكمومي في عام 1984، وهو يستغل مبدأ عدم اليقين أو الشك، الذي ينص في الأساس على أن قياس خاصية واحدة لحالة كمية سيؤدي إلى إدخال عدم اليقين في خاصية أخرى. وغايته إرسال مفتاح ثنائي عبر قناة غير آمنة [1,2] .

2-1- آلية عمل البروتوكول BB84:

بفرض لدينا طرفان أليس وبوب يريدان تبادل المفتاح بينهما، يتطلب البروتوكول أن يتفق هذان الطرفان على ترميزين مختلفين للبت الكلاسيكي باستخدام البت كمومي. على سبيل المثال، يمكن ترميز 0 بواسطة فوتون مستقطب أفقياً (→) وبزاوية 45 درجة (↗)، بينما يرمز 1 بعد ذلك بواسطة فوتون مستقطب رأسياً (↑) وبزاوية 45- درجة (↖)، كما سبق وأظهر في الشكل (1)، أي لدينا قاعدتان يمكن تحضير فوتون فيهما لتمثيل جزء واحد من المعلومات. وهما قاعدتان مترافقتان حيث يُعطى الأساس المستقيم بواسطة $\{|\rightarrow\rangle,|\uparrow\rangle\}$، و يرمز له بـ + بينما الأساس القطري بواسطة $\{|\nearrow\rangle,|\nwarrow\rangle\}$ و يرمز له بـ x.

2-1-1- خطوات البروتوكول:

1. تولد أليس عشوائياً سلسلة k مكونة من m بت، والتي سيشتق منها المفتاح المشترك في النهاية.
2. تولد أليس سلسلة عشوائية a من m بت، مستخدمة بالتناوب القاعدتين المذكورتين سابقاً عشوائياً.
3. يستقبل بوب السلسلة، ويقيس الفوتونات الواصلة باستخدام الأساس الخاص به، فيحصل على السلسلة bi. وهذا ما يولد حالة من عدم اليقين بصحة السلسلة ومطابقتها للأصل.
4. تعلن أليس إلى بوب القواعد المستخدمة.
5. يبلغ بوب أليس في أية الحالات كان تخمينه مطابق للأصل. و يحتفظ بالبتات المتطابقة فقط، هكذا ستتكون سلسلة البتات الجديدة$\tilde{k}$ و التي تمثل المفتاح المشترك.

أحياناً قد يحدث أن يحصل بوب على الحالة الصحيحة حتى لو اختار الأساس الخاطئ، لكن هذا يحدث فقط بشكل احتمالي.

هذه الخطوات موضحة ضمن المثال الآتي في الشكل (2)، بفرض m=8:

المفتاح الأولي	k	0	1	1	1	0	1	0	1
ترميز أليس	a	→	↖	↖	↑	↗	↖	→	↖
قياس بوب	b	↗	↖	↖	↖	→	↖	→	↑

التطابق		N	Y	Y	N	N	Y	Y	N
المفتاح المشترك	$\tilde{k}$		1	1			1	0	

الشكل (2): مثال عن الحصول على المفتاح المشترك

2-2- آلية العمل في حال وجد مهاجم:

من الناحية المثالية، عند وجود مهاجم يحاول التنصت على القناة للحصول على المفتاح فإنه سينسخ كل بت كمومي وينتظر انتهاء الإرسال من أجل معرفة القواعد التي يستخدمها أليس وبوب، حتى يتمكن من معرفة القواعد الصحيحة. لكن نسخ البتات الكمومية محظور بموجب نظرية عدم الاستنساخ وهو أمر يميز المعلومات الكمومية عن الفكرة الأساسية لنسخ البتات.

لكن باعتبار أن البروتوكول يعتمد على التخمين وظهور حالة عدم اليقين، فإن المهاجم سيكون أمام حالتين أساسيتين هما كالآتي:

الحالة الأولى: هي حالة أن المهاجم اختار الأساس الخاطئ أي: البت الكمومي تعدل، واختار بوب أيضاً الأساس بشكل خاطئ فإن المهاجم لن يُكتشف. لكن سيكتشف في حال اختار بوب بشكل صحيح.

الحالة الثانية: هي حالة أن المهاجم اختار الأساس الصحيح، أي أن البت الكمومي لن يُعدل، بالنتيجة لن يكتشف المهاجم.

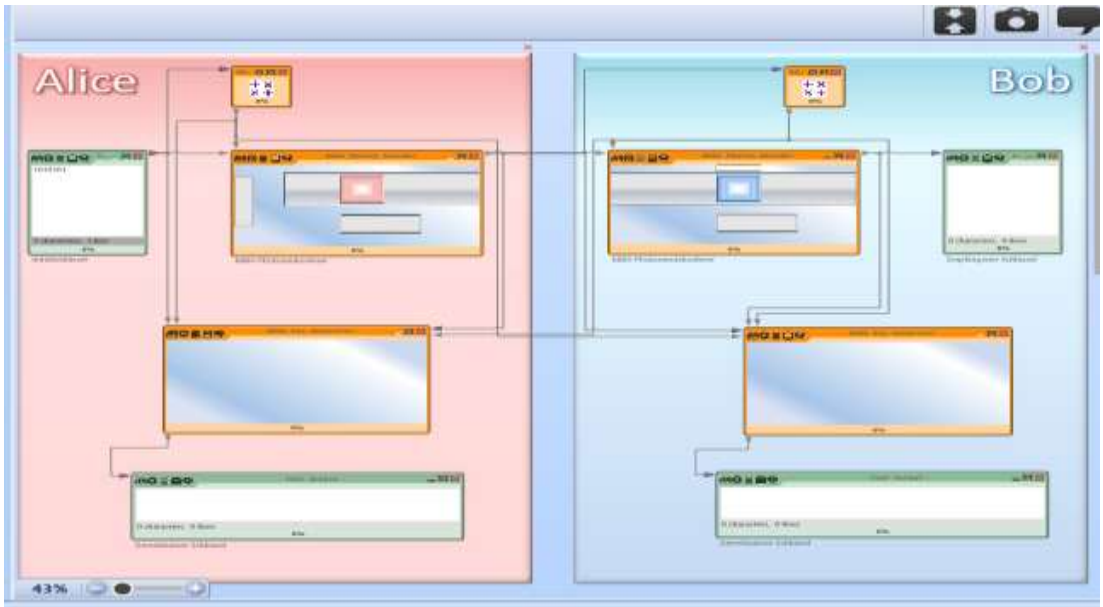
أي أنه لكل كيوبت منقول، هناك احتمال بنسبة 75% أن عمل المهاجم لا يكتشف. والاحتمال المتبقي بنسبة 25% يرجع إلى اختيار بوب الصحيح عندما يختار المهاجم بشكل غير صحيح.

3. اختبار فعالية البروتوكول BB84 :

باستخدام البرنامج CRYPTOOL حاكينا البروتوكول BB84. فرضنا لدينا المرسل أليس والمستقبل بوب، بداية سنجري عملية تبادل المفاتيح بينهما من خلال البروتوكول BB84 ومن ثم سنستخدم هذا المفتاح لتشفير نص باستخدام الخوارزمية DES والتي هي إحدى خوارزميات التشفير المتناظر[6] .

3-1. تبادل المفاتيح باستخدام البروتوكول BB84 :

باختيار واجهة البروتوكول BB84 ستظهر لدينا النافذة الآتية في الشكل (3):



الشكل (3) : واجهة البروتوكول Bb84

سيكون في جهة الإرسال أي لدى أليس المكونات الآتية:

1. مولد قاعدة الفوتون (Photon Basis Generator): وظيفته إنشاء سلسلة عشوائية من قواعد القياس الكمومي (0 و1) وإرسالها إلى الجهاز الآخر، تُستخدم هذه القواعد الأساسية لتحديد كيفية قياس الجسيمات الكمومية المرسلة، والتي ستؤدي إلى إنشاء المفتاح الكمومي المشترك بطريقة آمنة وسرية.

2 . مولد المفتاح (Key Generator): وظيفته توليد مفتاح كمومي عشوائي يُستخدم في التشفير وفك التشفير ويكون ذا مستوى عالٍ من الأمن والحماية.

3. جهاز ترميز الفوتون (Photon Encoding Device): يُستخدم لترميز الفوتونات المرسلة وفقاً لقواعد القياس التي أنشئت من قبل مولد قاعدة الفوتون، على سبيل المثال إذا كانت القاعدة المطلوبة هي الأساس المستقيم يجب على الجهاز ترميز الفوتونات لتكون في هذا الأساس.

بهذا الترتيب يمكن لأليس تجهيز الفوتونات وإرسالها إلى بوب لمواصلة عملية تبادل المفتاح الكمومي بشكل آمن.

عند طرف الاستقبال بوب، ستكون لديه نفس المكونات التي لدى أليس مع اختلاف أنه يستبدل جهاز ترميز الفوتون بجهاز فك ترميز الفوتون (Photon Decoding Device) حيث يستخدم هذا المكون لفك ترميز الفوتونات المرسلة من قبل أليس واستخراج البتات الكمومية.

3-1-1 خطوات التنفيذ:

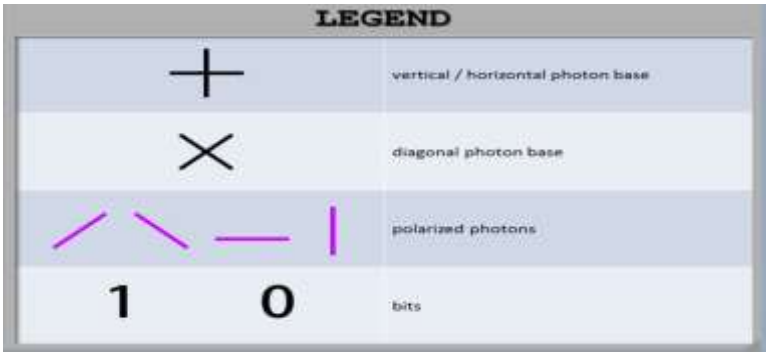
عند طرف المرسل (أليس):

1. تُدخل سلسلة من البتات وهي تمثل المفتاح الأولي بطول بت128=n مثلاً، كما يظهر في الشكل (4).

k=1000001010101010100011001110101010001110001010101010101010000000111101010100001111000101010101010100001110001110001010101010

الشكل (4): سلسلة المفتاح الأولي المستخدمة

2. لبدء تحويل هذه السلسلة إلى مجموعة من الفوتونات المستقطبة حسب قاعدتي الاستقطاب وبالتناوب العشوائي بينهما نضغط على Photon Encoding Device، فيظهر على اليمين البارامترات الخاصة بهذا المكون، حيث تغير قواعد الأساس وفقاً لما اعتمد سابقاً (_ و / : "0" ، | و \ : "1") كما تظهر في الشكل (5):



الشكل (5): قواعد الترميز المستخدمة

3. يضغط على الزر PLAY ليبدأ توليد المفتاح.

نلاحظ أن البت 0 وفق قاعدة الاستقطاب X مثله بفوتون وفق الاستقطاب /. و هكذا يرمز كل بت كلاسيكي كبت كمومي ، كما في الشكل (6).

(a): البت المراد ترميز 0 قاعدة الاستقطاب هي X

(b): ترميز البت 0 بالاستقطاب /

الشكل (6): ترميز البت الكلاسيكي 0 كبت كمومي

في جهة الاستقبال (لدى بوب):

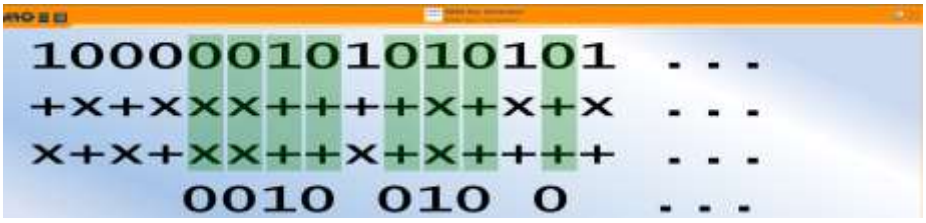
1. سيخمن البتات الواصلة باستخدام قاعدتي الاستقطاب بشكل عشوائي، باستخدام مفكك الترميز، لذا قد يصيب كما في الشكل (7–a) وقد يخطئ كما في الشكل (7–b)

(a): تخمين صحيح

(b): تخمين خاطىء

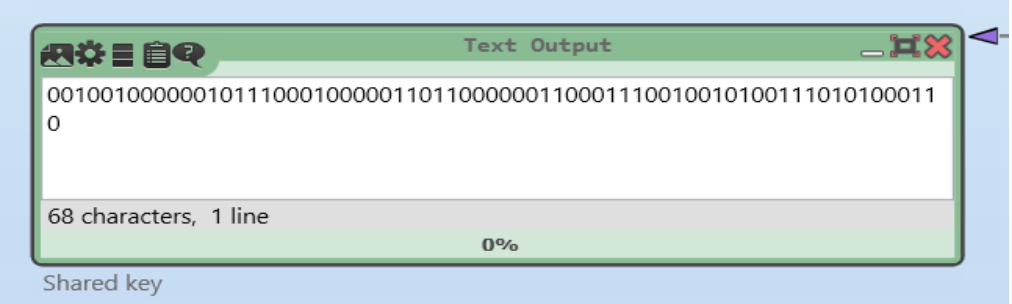
الشكل (7): مثال عن عملية التخمين

2. ضمن مولد المفتاح يُقارن الاستقطاب الذي اعتمدته أليس مع استقطاب بوب (التي تقابل بالبروتوكول مرحلة إعلان القواعد المستخدمة في الاستقطاب)، حيث يحتفظ بالبت (الملون باللون الأخضر) في حالة التطابق أما في حالة عدم التطابق فإنه يُهمل. ويكون الناتج النهائي هو المفتاح المشترك بين أليس وبوب. كما يظهر في الشكل (8).



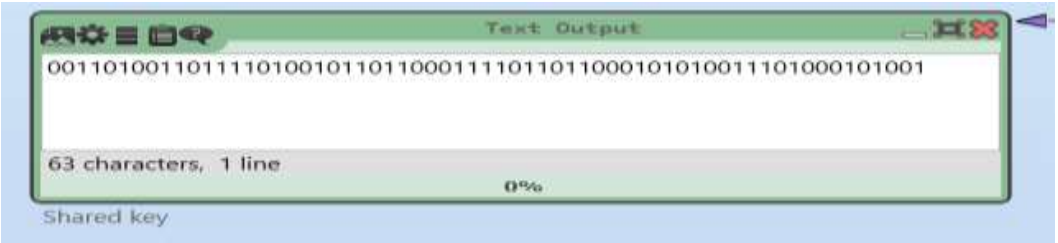
الشكل (8): مقارنة البتات المخمنة مع القواعد المعلنة من أليس

فيكون المفتاح المشترك كما يظهر في الشكل (9)، نلاحظ أن المفتاح المشترك مكون من 68 بت مشتقة من المفتاح الأولي الذي كان بطول 128بت أي أن طول المفتاح المشترك يساوي 52% من المفتاح الأولي.



الشكل (9): سلسلة المفتاح المشترك المشتق من المفتاح الأولي المولد

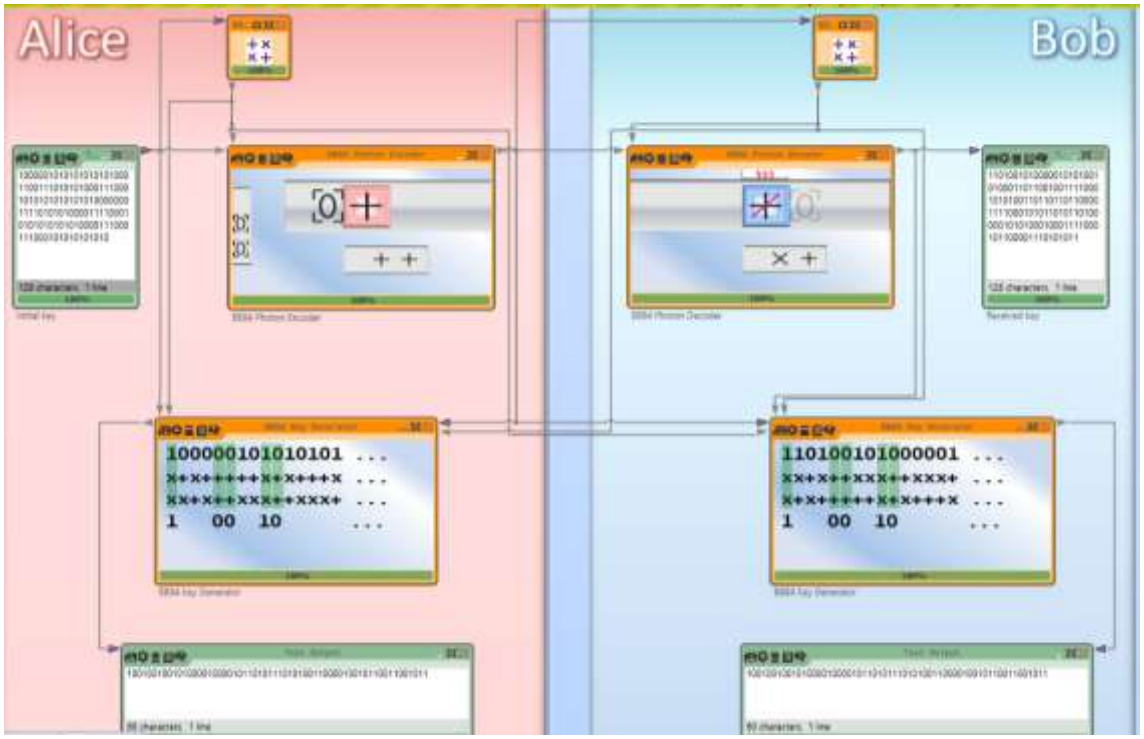
مع ملاحظة أنه في مع كل عملية توليد جديدة سينتج مفتاح جديد من مشتق من نفس المفتاح الأولي بطول وتسلسل بتات مختلف، مثلاً في الشكل (10) نلاحظ المفتاح الجديد المشترك:



الشكل (10): مفتاح مشترك جديد

يعود السبب في ذلك إلى عملية التخمين للقاعدة المستخدمة التي يعتمد عليها المستقبل بوب لقراءة الفوتونات. وهذه مفيد من الناحية الأمنية إذ يزيد من مجال المفاتيح التي يمكن أن تستخدم.

يظهر الشكل (11)، أحد سيناريوهات عمل البروتوكول BB84 كاملاً.



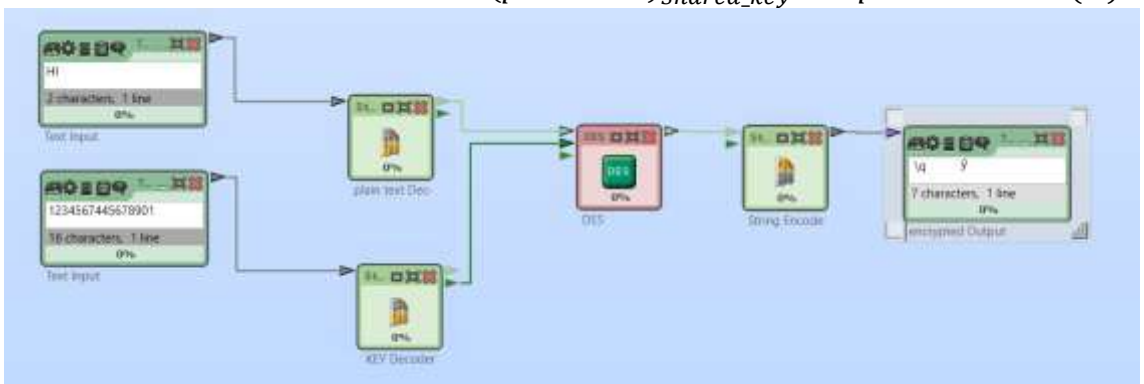
الشكل (11): مثال على عمل البروتوكول BB84 كاملاً

3-2 تنفيذ خوارزمية التشفير المتناظرة DES:

خوارزمية التشفير المتناظر الكتلية DES هي خوارزمية تعتمد على استخدام مفتاح دخل بطول 64 bits وكتلة دخل بطول 64 بت، في حال طول الدخل أقل من 64 تحشر أصفار، من الشكل (12)، نلاحظ الدخل هو نص بالأسكي لذا استخدمنا مرمز يحول الآسكي إلى الترميز الثنائي، وكذلك نفس الأمر بالنسبة للمفتاح.

عند تنفيذ الخوارزمية سينتج النص المشفر المقابل للنص الصريح نلاحظ أنه مكون من 64 بت، يمكن أن نعبر عن ذلك كالآتي:

$$E(plainttext)_{Shared\_key} = ciphertext \qquad (1)$$



الشكل (12): مثال على تطبيق الخوارزمية DES

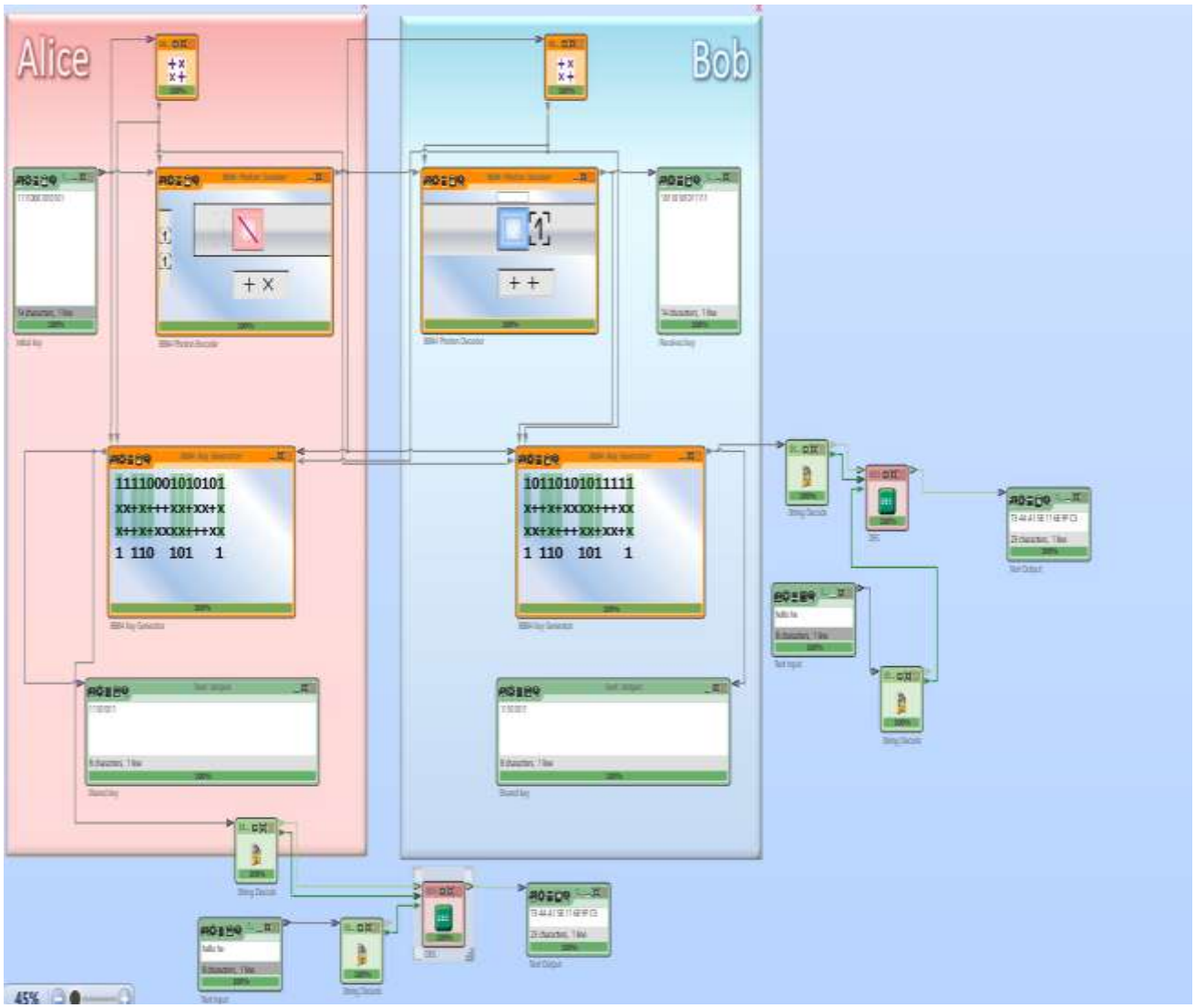
وفي حال فك التشفير سيكون الدخل هو النص المشفر الذي أرسل إلى المستقبل، إضافة إلى المفتاح الذي يوجد لديه، ويمكن التعبير عن عملية فك التشفير كالآتي:

$$E(ciphertext)_{Shared\_key} = plainttext \quad (2)$$

سنطبق في هذا البحث المفتاح المشترك الناتج عن البروتوكول BB64 كمفتاح تشفير لدى المرسل أليس ومفتاح فك تشفير لدى المستقبل بوب، كما يظهر في الشكل (13).

إن استخدام المفتاح المتبادل باستخدام البروتوكول BB84 يعطي قوة لاستخدام خوارزمية DES لأنه يرفع من قوتها تجاه حساسيتها لتبادل المفاتيح، وهي إحدى أهم المشكلات الحرجة التي تعترض استخدام خوارزميات التشفير المتناظر.

كما نلاحظ من الشكل أن أليس وبوب حصلا عل المفتاح 11101011من البروتوكول BB84، هنا الأصفار والواحدات يمثل كل منها محرف وليس بت أي كل منها مكون من 8 بتات وبالنتيجة طول المفتاح 64 بت وهو المناسب بالنسبة للخوارزمية DES. بفرض أن النص المراد تشفيره هو hello he. نلاحظ من الشكل ناتج عملية التشفير لدى أليس وناتج عملية فك التشفير لدى بوب.



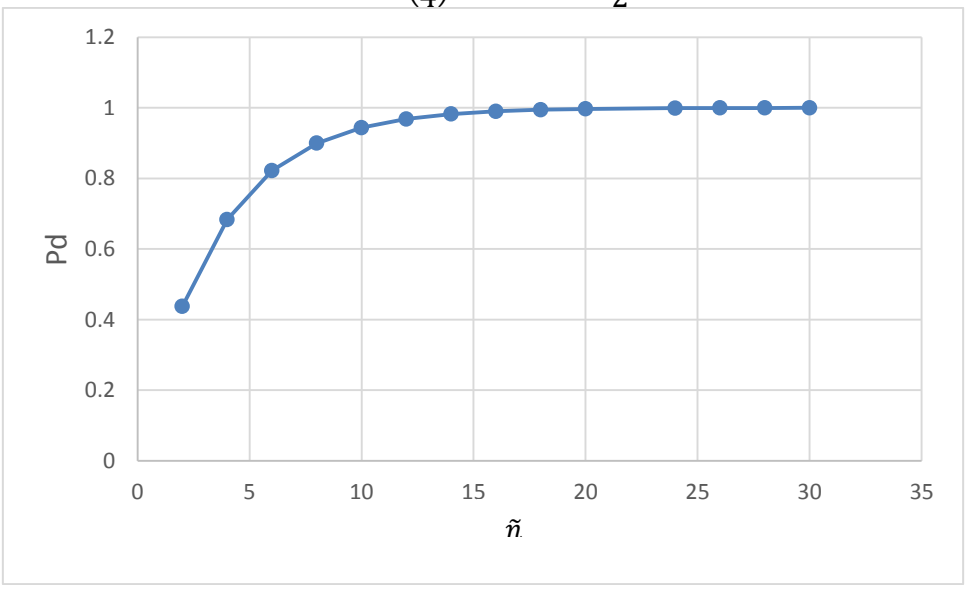
لشكل (13): تنفيذ الخوارزمية DES باستخدام مفتاح موزع اعتماداً على BB84

3-3 تنفيذ الهجوم في حال وجود متنصت على القناة:

ذكرنا سابقاً احتمال عدم كشف المهاجم تصل نظرياً إلى 0.75 إذا طبقت عملية ترميز الفوتونات وإرسالها دون أي إجراءات إضافية، لذا ونظراً لأن تسلسلات البتات الخاصة بالمرسل والمستقبل لا تتطابق تماماً، فإنهما يتخذان خطوة إضافية لاختبار التنصت. يقرران تحديد مجموعة فرعية من البتات المتبقية ومقارنتها. إذا لم تتطابق، فإنهما يعرفان بالتأكيد أن المهاجم قد تدخل. بالطبع، هناك حل وسط بين عدد البتات التي يريدون "التضحية بها" لاكتشاف وجود المهاجم باحتمالية عالية وطول المفتاح المشترك، والذي يتناقص مع تجاهل البتات التي قورنت فيما بينها.

وسطياً يستخدم عدد بتات فحص مساوٍ لنصف عدد بتات المفتاح فمن أجل مفتاح بطول n يكون عدد هذه البتات حوالي $\tilde{n} < \frac{n}{2}$ ، في حال تطابق هذه البتات فإن المهاجم لن يُكتشف، أي احتمال تطابقها يمثل احتمال عدم كشف المهاجم، أي أن هذه الاحتمالية تتناقص مع زيادة $\tilde{n}$ [7] و تعطى بالعلاقة:

$$P_d = 1 - P_e = 1 - \left(\frac{3}{4}\right)^{\tilde{n}} \quad ,\tilde{n} < \frac{n}{2} \qquad (1)$$

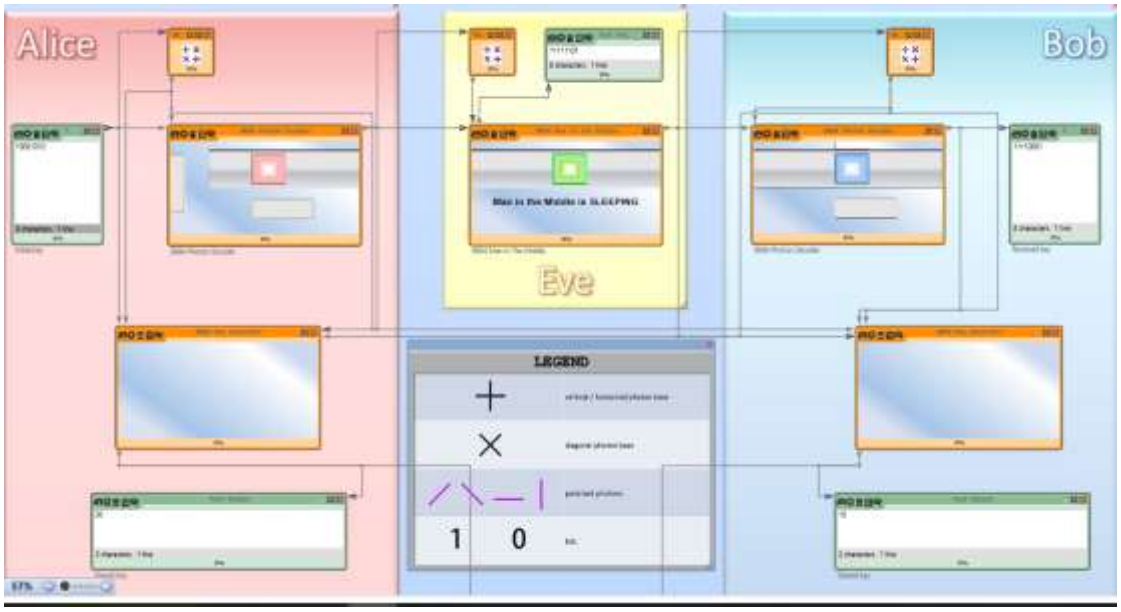


الشكل (14): العلاقة بين احتمالية كشف المهاجم وعدد بتات المطابقة

نلاحظ من الشكل (14)، من أجل مفاتيح ذات أطوال صغيرة تكون احتمالية الكشف منخفضة فمثلاً من أجل مفتاح بطول يصل إلى 20 بت لن تتجاوز احتمالية الكشف 0.89، لكن كلما كان المفتاح أطول أي بتات المطابقة الممكن استخدامها أكبر كلما زادت احتمالية كشف المهاجم، وهذا يتناسب مع خوارزميات التشفير المستخدمة عملياً، مثل خوارزمية DES التي تستخدم مفتاحاً مكوناً من 64 بت بالنتيجة يمكن أخذ قيمة $\tilde{n} = 30$ ، نلاحظ أن احتمالية الكشف تصل تقريباً إلى الواحد.

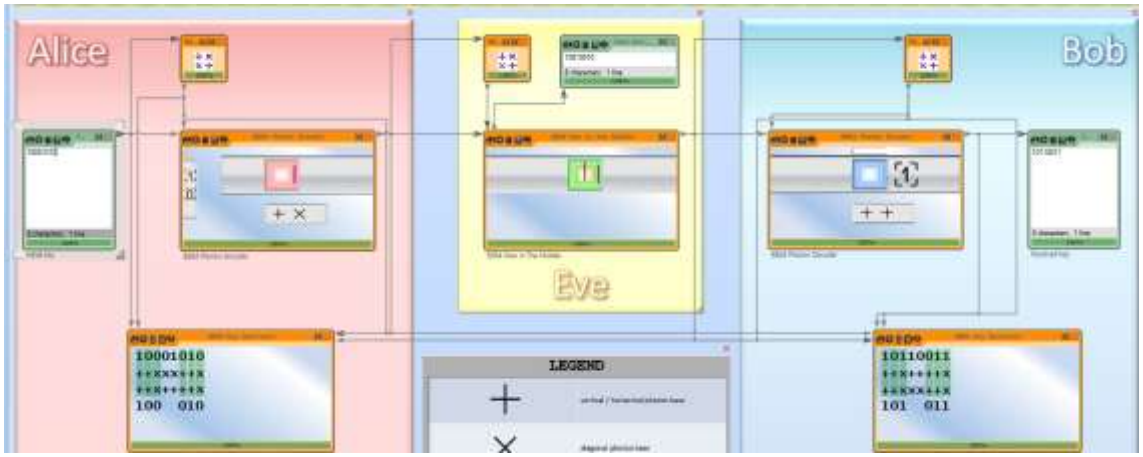
طبقنا في هذه الخطوة هجوم رجل في المنتصف (MIM) والذي سيتنصت على الفوتونات المنتقلة عبر القناة، سيخزن نسخة من هذه الفوتونات ليفك ترميزها بعد ذلك بناء على القواعد التي ستعلن عنها أليس. لكن كما ذكرنا سابقاً نسخ الفوتون سيغير من استقطابه وبالنتيجة سيؤثر ذلك على فك ترميز الفوتونات عند المستقبل بوب. أي سيظهر خلل في الوصول إلى مفتاح مشترك بين المرسل والمستقبل وبالنتيجة سيكتشف وجود المهاجم. وهكذا لن يكون قادراً رغم تنصته استخدام المفتاح الذي حصل عليه لأنه غير صحيح.

كما يظهر في الشكل (15):



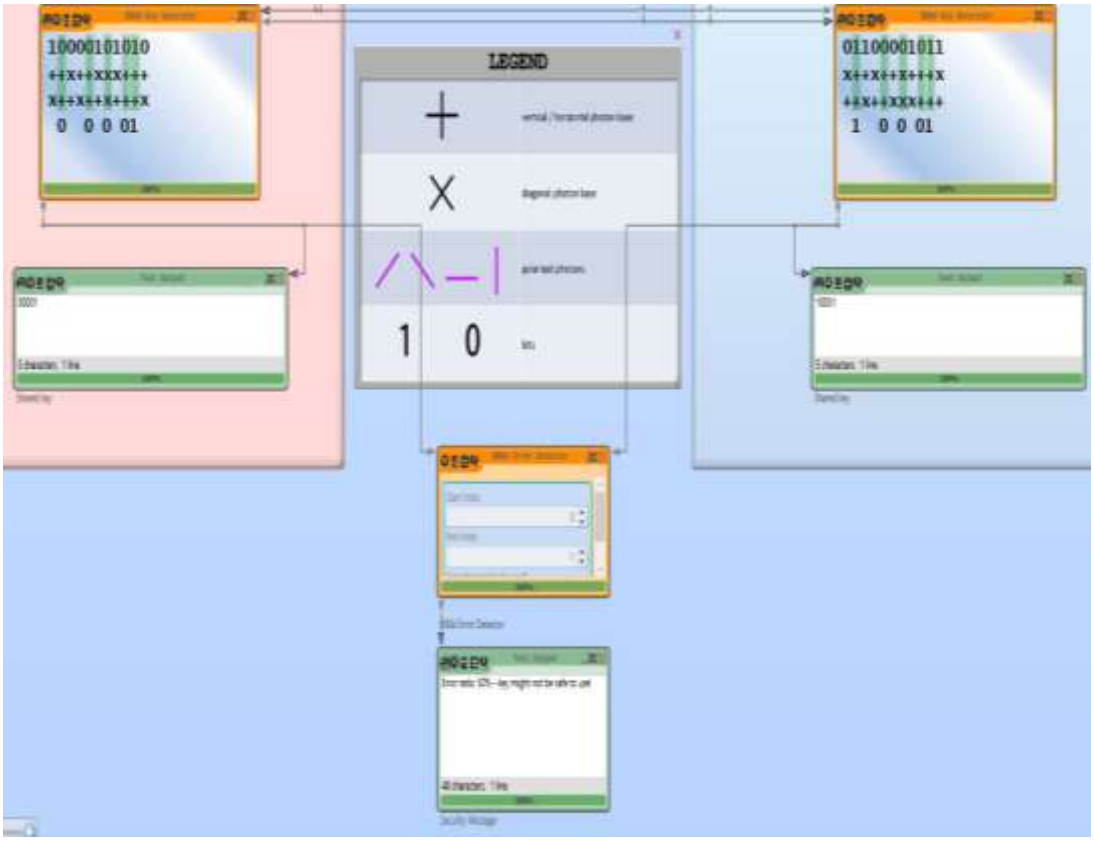
الشكل (15): تطبيق هجوم رجل في المنتصف (MIM)

في المثال الذي يظهر في الشكل (16)، نلاحظ أنه أثناء عملية تبادل المفاتيح بين أليس وبوب وبوجود المهاجم إيف، نتج لدى كل منهما مفتاح مختلف عن الآخير، فلدى أليس المفتاح 100010ولدى بوب المفتاح هو 101011.



الشكل (16): مثال على تطبيق هجوم رجل في المنتصف أثناء عمل البروتوكول BB84

كما شرحنا سابقاً، يستخدم كل من المرسل و المستقبل بتات مقارنة للتحقق من المفتاح الذي حصل عليه، يظهر ذلك في الشكل (17)، فعملية المقارنة أعطت أن هناك خطأ بالمفتاح المشترك المولد بنسبة 50% ، وهذا يدل وجود متنصت يحاول الحصول على المفتاح أي بالنتيجة عدم صلاحية المفتاح للاستخدام . طبعاً هذه النسبة غير ثابتة إنما تختلف حسب كل عملية توليد وذلك بسبب استخدام قاعدة التخمين ضمن البروتوكول BB84 التي ذكرناها سابقاً.



الشكل (17): مثال على استخدام بتات المقارنة لكشف هجوم رجل في المنتصف

الاستنتاجات والتوصيات:

مما سبق نستنتج أن البروتوكول BB84 هو برتوكول فعال في تبادل المفاتيح، ويعود ذلك إلى اعتماده على فيزياء الكم أي استخدام استقطاب الفوتونات لتوليد المفتاح لدى المستخدمين، وقدرته على كشف أي متنصت يحاول الحصول على هذا المفتاح، وذلك كون محاولة المتنصت نسخ أي فوتون أو قراءته سيؤثر على استقطابه، وهكذا سيعطي قراءة خاطئة وهذا سينبه المستخدمين إلى وجوده وعدم استخدام المفتاح. لذا نوصي باستخدام هذا البروتوكول في التطبيقات التي تستخدم خوارزميات تشفير متناظر وتعمل في بيئات غير آمنة. وهذا سيضع حداً لكثير من الهجمات التي تستهدف كسر المفتاح وكسر تشفير البيانات المتبادلة المهمة المشفرة.

References:

[1] Gilles, B, and Charles H, B. , "Quantum cryptography public key distribution and coin tossing ", Theoretical Computer Science , V.560, part1, pp7-11,2014

[2] Cyril B., Nicolas G., Barbara K, and Valerio S.," Security of two quantum cryptography protocols using the same four qubit stats", Physical Review A, V.72,Issue 3, 2005

[3] www.cryptool.org/en/ Homepage - CrypTool, last visit 14/10/2024

[4] Rashmi R, and Thakur K.K., "Quantum Cryptography: Fundamentals and Advanced Techniques", International Journal for Research in Applied Science & Engineering Technology (IJRASET) ISSN: 2321-9653; Volume 12 , 2024

[5] James L.Park." The concept of transition in quantum mechanics", Foundation of physics ,springer,V.1,pp23-33, 1970

[6] Scarani V., Bechmann-Pasquinucci H., Cerf N.J, Dusek M., Lutkenhaus N.,and Peev M." The security of practical quantum key distribution ", Reviews of Modern Physical , V,81, issue 3, pp1301-1350, 2009

[7] Mihai-Zicu M. and Emil S., "A Scalable Simulation of the BB84 Protocol Involving Eavesdropping", Innovative Security Solution for information Technology and Communications, v.12596, springer, 2021

[8] J. Orlin G , "The DES Algorithm Illustrated" , laissez faire city times, V 2, No. 28. 2024