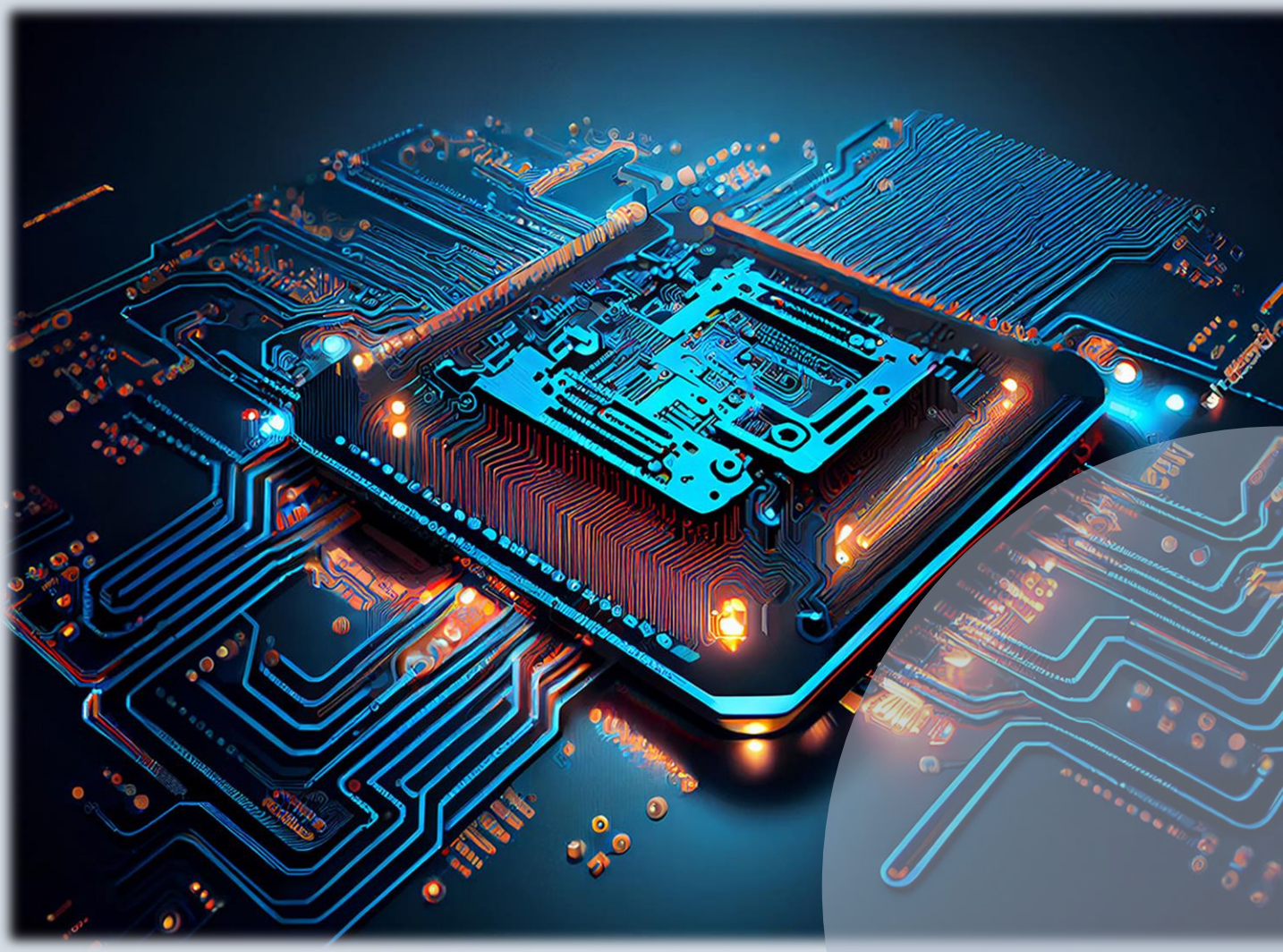


حل اللغز الكمومي: فهم المفاهيم الكمومية في الأمن السيبراني

تأليف

أسماء فالح، لمى عبد الله، نوف إبراهيم، نوف سعيد، نور أشرف.

إشراف د. نايا ناجي

مايو، ٢٠٢٤

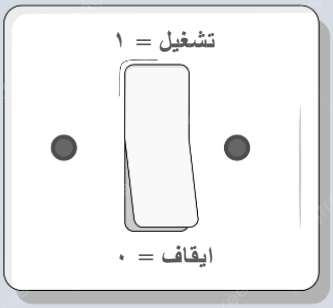
الفصل الأول: مقدمة في الحوسبة الكمومية

الحوسبة الكمومية هي مجال مثير مخصص للعلماء والفيزيائيين والمهندسين وأي شخص يرغب في استكشاف المستقبل! ولكن ما هي الحوسبة الكمومية بالضبط؟ كيف تعمل؟ وما هي العلاقة بين الحوسبة الكمومية والأمن السيبراني؟ كل هذه الأسئلة وأكثر سيتم الرد عليها في هذا الكتيب. نتمنى لك قراءة ممتعة!

في القرن السابع عشر، استخدم الناس كلمة "الكم" للحديث عن مقدار شيء ما. وهي كلمة تأتي من اللاتينية وتعني أساسا "كم". لذا، فكر في الأمر كما لو كان لديك بيتزا، وتقول "سأحصل على شريحة." هذه الشريحة هي كمية من البيتزا وهي كمية محددة. في الوقت الحاضر، عندما نسمع كلمة "الكم"، يمكننا التفكير فيها على أنها تتحدث عن شيء محدد، كمية قابلة للقياس من شيء ما. يشبه الأمر عندما تقوم بقياس مكونات الوصفة، قد تحتاج إلى كمية محددة من الدقيق أو السكر. هذا هو نوع من الطرق التي نستخدم بها "الكم" اليوم. الأمر كله يتعلق بالحديث عن الأشياء بكميات أو وحدات محددة.

ما هو الكم؟

تخيل أجهزة الكمبيوتر التقليدية كآلات تستخدم البتات لتخزين المعلومات ومعالجتها. يمكن أن يكون البت إما ٠ أو ١، مثل مفتاح الضوء الذي يمكن إطفاءه أو تشغيله.



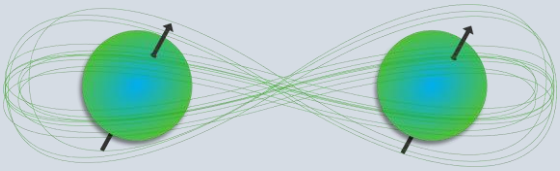
في المقابل، تستخدم أجهزة الكمبيوتر الكمومية البتات الكمومية، أو الكيوبتات الممثلة بـ |٠> أو |١>. يمكن أن توجد الكيوبتات في حالات متعددة في نفس الوقت، وذلك بفضل مفهوم يسمى التراكب. إنه مثل وجود مفتاح إضاءة يمكن تشغيله وإيقافه في وقت واحد! هذه القدرة على الوجود في حالات متعددة في وقت واحد تمنح أجهزة الحاسوب الكمومية قوة لا تصدق.

بينما يمكن للكمبيوتر التقليدي معالجة مجموعة واحدة فقط من التعليمات في كل مرة، يمكن للكمبيوتر الكمومي معالجة العديد من التعليمات في وقت واحد، مما يجعله أسرع بكثير في حل أنواع متعددة من المشاكل.

خاصية التشابك

ليس هذا فقط، بل هناك المزيد! يمكن أيضا تشابك الكيوبتات ، مما يعني أن حالة الكيوبت الواحد يمكن أن تعتمد على حالة كيوبت آخر، بغض النظر عن مدى تباعدهما. تسمح هذه الظاهرة لأجهزة الحاسوب الكمومية لإجراء حسابات معقدة بطرق لا تستطيع أجهزة الحاسوب التقليدية تقليدها ببساطة.

تخيل أن لديك اثنين من الكيوبتات المتشابكة. إذا قمت بتغيير حالة كيوبت واحد، فإن حالة الكيوبت الآخر تتغير على الفور، حتى لو كانت تفصل بينهما سنوات ضوئية. هذه الظاهرة تبدو وكأنها من الخيال، لكنها خاصية أساسية في ميكانيكا الكم.



ملخص

تستخدم الحوسبة الكمومية الخصائص المذهلة لميكانيكا الكم لتغيير كيفية حل المشكلات والتعامل مع المعلومات. إنه عالم مثير للاهتمام مع العديد من الاحتمالات، وقد بدأنا للتو في استكشاف ما يمكن أن تفعله!

في الفصل التالي، سوف نتعمق في أساسيات الأمن السيبراني ونستكشف كيف تعيد الحوسبة الكمومية تشكيل الطريقة التي نحمي بها عالمنا الرقمي. لذا، استعد للتعمق في عالم الحوسبة الكمومية واكتشاف الإمكانيات اللانهائية التي توفرها.

الفصل ٢ : المفهوم الأساسي للأمن السيبراني وتقنياته

في مجال الأمن السيبراني، يعد فهم المفاهيم الأساسية أمرا ضروريا لحماية الأنظمة والبيانات بشكل فعال من التهديدات السيبرانية. ثالوث الامن السيبراني: السرية والنزاهة والتوافر بمثابة أساس للأمن السيبراني.

يتم دعم هذه المبادئ من خلال ست مجالات رئيسية:

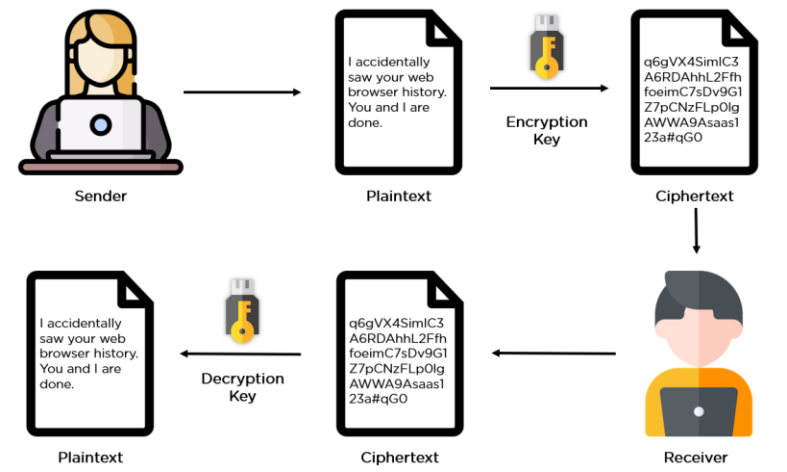
أمن الشبكات، والتشفير، وتطوير البرمجيات الآمنة، والاستجابة للحوادث، وإدارة المخاطر وتطوير السياسة الأمنية. يلعب كل مجال دورا حاسما في حماية المعلومات والتخفيف من المخاطر السيبرانية.

المفهوم الأساسي للأمن السيبراني

سيناريو أمان الشبكة: يتم تكليف الشخصيات بتأمين شبكة لحمايتها من الهجمات الإلكترونية.

يتعرفون على التدابير الأساسية مثل تعيين كلمات مرور قوية وتحديث البرامج وتوخي الحذر من رسائل البريد الإلكتروني الاحتيالية. وتشمل التحديات التي يواجهونها تحديد نقاط الضعف المحتملة في الشبكة وتنفيذ التدابير الأمنية الأساسية.

سيناريو التشفير: تقوم الأحرف بتشفير البيانات أو فك تشفير الرسائل أو استخدام بروتوكولات التشفير للاتصال الآمن. يستكشف هذا السيناريو مبادئ وممارسات التشفير.



المفهوم الأساسي للأمن السيبراني

سيناريو تطوير البرمجيات الآمنة: تتعلم الشخصيات تطوير برامج آمنة من التهديدات السيبرانية.

يكتشفون مبادئ الأمان مثل التحقق من مدخلات المستخدم بحثا عن البيانات الضارة. على سبيل المثال،

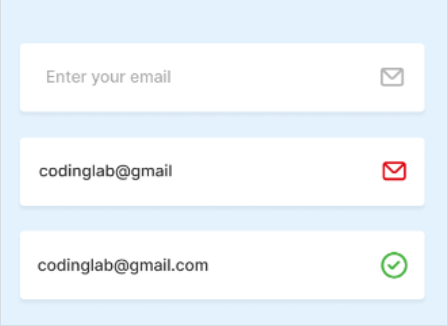
عند إدخال عنوان بريد إلكتروني عبر الإنترنت، يتحقق النظام من التنسيق (على سبيل المثال، وجود "@" واسم المجال).

تشير علامة الاختيار الخضراء إلى إدخال صالح، بينما تطالب علامة "X" الحمراء بالتصحيح.

كما أنهم يفهمون أهمية كتابة تعليمات برمجية آمنة لمنع نقاط الضعف،

مثل التحقق من صحة المدخلات واستخدام تقنيات الترميز الآمنة. بالإضافة إلى ذلك،

يتعلمون دمج الأمان في عملية تطوير البرامج بأكملها، من التخطيط إلى النشر.



سيناريو الاستجابة للحوادث: تقوم الشخصيات بإدارة الخروقات الأمنية أو الهجمات الإلكترونية والاستجابة لها.

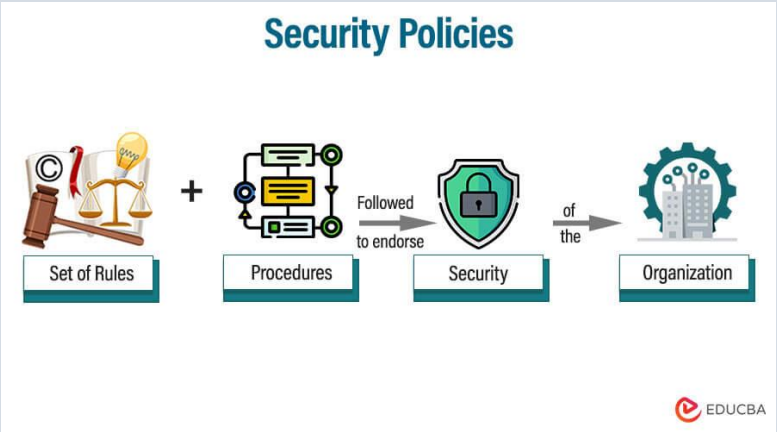
يتبعون خطة استجابة للحوادث، بما في ذلك خطوات مثل اكتشاف الحادث وتحليله، واحتواء الضرر، والقضاء على التهديد، والتعافي من الحادث.

المفهوم الأساسي للأمن السيبراني

سيناريو إدارة المخاطر: في مشروع مدرسي، تتولى مجموعة من الأصدقاء دور حماية الوصفة السرية لناديهم للحصول على أفضل ملفات تعريف الارتباط من المتسللين عبر الإنترنت. جميعهم يعملون معًا لتحديد المخاطر المحتملة، مثل قيام شخص ما بسرقة الوصفة أو العبث بقائمة المكونات.

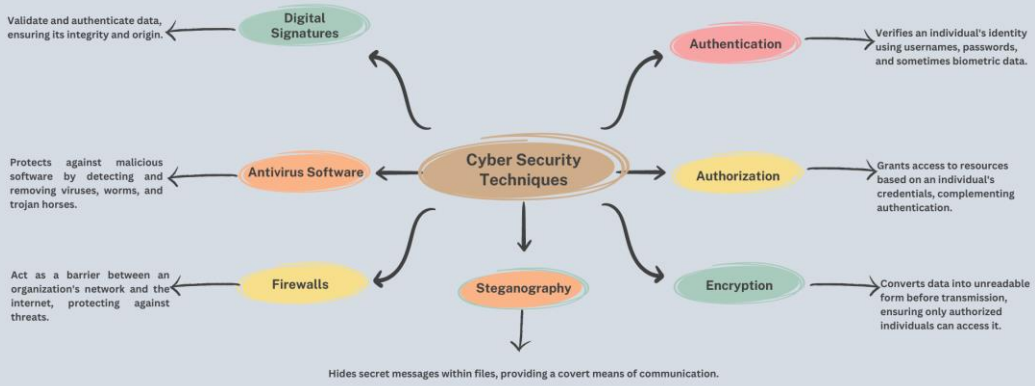
للحفاظ على وصفتهم آمنة، ينتجون استراتيجيات ذكية مثل الاحتفاظ بالوصفة في ملف مقفل ومشاركتها فقط مع الأعضاء الموثوق بهم. كما أنهم يراقبون أي نشاط مشبوه عبر الإنترنت للتأكد من بقاء وصفتهم سرية.

سيناريو تطوير سياسة الأمان: في نادي تطوير ألعاب الفيديو، ينشئ الأعضاء قواعد للحفاظ على أفكار ألعابهم آمنة من النسخ. إنهم ينتجون إرشادات حول كيفية استخدام التكنولوجيا، ومن يمكنه الوصول إلى تصميمات ألعابهم، وكيفية حماية عملهم من السرقة. باتباع هذه القواعد، يضمنون أن كل فرد في النادي يفهم كيفية الحفاظ على أفكار لعبتهم آمنة ويمكنهم التركيز على إنشاء ألعاب جديدة ومثيرة دون القلق بشأن سرقة أفكارهم.



تقنيات الامن السيبراني

يستكشف مختلف الأساليب والأدوات الأساسية للدفاع ضد التهديدات السيبرانية. في العصر الرقمي اليوم، حيث تعد المعلومات أحد الأصول، يعد تأمين البيانات والأنظمة أمرا بالغ الأهمية. يسلط هذا الملخص الضوء على الاستراتيجيات الرئيسية مثل المصادقة والترخيص والتشفير والتوقيعات الرقمية وبرامج مكافحة الفيروسات وجدران الحماية وإخفاء المعلومات، وكلها مكونات حيوية في الترسانة ضد الهجمات الإلكترونية.



كيف تعمل الحوسبة الكمومية على تحسين الأمن في الفضاء الإلكتروني؟

تشفير محسن: يمكن اختراق طرق التشفير التقليدية، مثل RSA وECC، بسهولة بواسطة أجهزة الحاسوب الكمومية. للبقاء آمنا، يتم تطوير طرق تشفير جديدة لمقاومة الهجمات من أجهزة الحاسوب الكمومية.

الاتصال الآمن: يستخدم توزيع المفاتيح الكمومية (QKD) ميكانيكا الكم لإنشاء مفاتيح سرية للاتصال الآمن. إنه مثل وجود رمز سري لا يمكن لأحد كسره، مما يضمن بقاء رسائلك خاصة (ستناقش في الفصل التالي).

اكتشاف الهجمات الإلكترونية: تساعد أجهزة الحاسوب الكمومية على تحسين اكتشاف التهديدات السيبرانية من خلال اكتشاف الأنماط غير العادية في حركة مرور البيانات بسرعة.

هذا يساعد على الحماية من الهجمات بشكل أكثر فعالية.

بروتوكولات الأمان المحسنة: يمكن أن تؤدي الحوسبة الكمومية إلى تطوير تدابير أمنية أقوى لحماية البيانات من الهجمات الكمومية. و يضمن بقاء معلوماتك آمنة، حتى مع تقدم التكنولوجيا.

ملخص

السرية والنزاهة والتوافر أمرا بالغ الأهمية في الأمن السيبراني. ست مجالات رئيسية أمن الشبكات، والتشفير، وتطوير البرمجيات الآمنة، والاستجابة للحوادث، وإدارة المخاطر، وتطوير السياسة الأمنية تشكل الأساس. تتعلم الشخصيات في السيناريوهات تأمين الشبكات وتشفير البيانات وتطوير برامج آمنة وإدارة الحوادث وتقييم المخاطر وتطوير سياسات الأمان. تشمل الاستراتيجيات الرئيسية المصادقة والتخويل والتشفير والتوقيعات الرقمية وبرامج مكافحة الفيروسات وجدران الحماية وإخفاء المعلومات. تتحدى الحوسبة الكمومية التشفير التقليدي، مما يؤدي إلى خوارزميات تشفير جديدة مقاومة للكم وبروتوكولات أمان محسنة. انضم إلينا ونحن نستكشف كيف تعيد الحوسبة الكمومية تشكيل الأمن السيبراني والاستراتيجيات التي يتم تطويرها لمواجهة هذه التهديدات الناشئة.

الفصل ٣ : الحوسبة الكمومية وتهديدات الأمن السيبراني

في الأمن السيبراني، هناك العديد من التهديدات الموجودة. على سبيل المثال، رفض الخدمة، وعمليات استغلال يوم الصفر، والتصيد الاحتيالي، وخرق البيانات، والبرامج الضارة. وتؤثر هذه التهديدات على الأصول والمعلومات على حد سواء. في الواقع، يمكن أن تكون سببا للتلاعب بالبيانات أو حذفها.
يحدث خطر أي هجوم بسبب ثلاثة جوانب مختلفة وهي التهديد والضعف والتأثير كما هو موضح في الرسم البياني التالي

من الواضح أن السبب وراء أي هجوم يعتمد على الغرض، ولكل هجوم مستوى مختلف من المخاطر والتأثير. وفي جميع الحالات، يلزم وجود آليات للتخفيف والوقاية من تلك الهجمات.

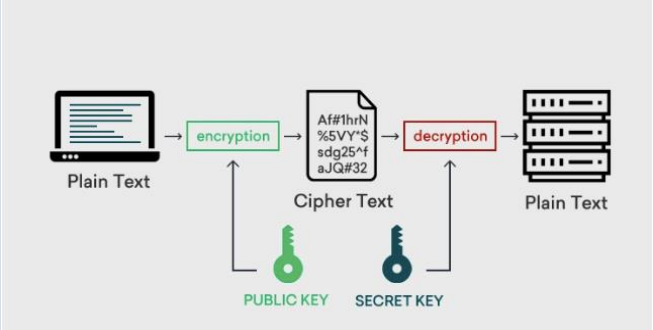
حلول الهجمات

يمكن اكتشاف الهجمات أو تخفيفها أو منعها اعتمادا على كيفية عملها والضرر الذي تسببه.

هناك العديد من التقنيات لزيادة الأمان وتقليل المخاطر. على سبيل المثال، عناصر التحكم في الوصول وجدران الحماية وبرامج مكافحة الفيروسات وتدريب الموظفين تنتج الهجمات دائما آليات وتقنيات جديدة لتنفيذ الهجوم. لذلك، يجب أن تكون جميع تقنيات الوقاية والكشف والتخفيف محدثة دائما حتى تتمكن من الحد من المخاطر والوصول إلى الهدف الأساسي وهو حماية كل من الأصول والمعلومات.

تشفير البيانات

كما ذكرنا سابقا، فإن إحدى تقنيات التخفيف الرئيسية هي تشفير البيانات. يتم تنفيذ هذه العملية عن طريق ترجمة المعلومات الأصلية إلى شكل غير قابل للقراءة، بحيث عندما يحاول المهاجمون سرقة البيانات سيكون من الصعب استرداد الكلمات الحقيقية.



هناك العديد من آليات التشفير، ولكل منها ميزات خاصة. على سبيل المثال، التشفير المتماثل والتشفير غير المتماثل والتشفير الهجين. في الختام، يعتمد فك تشفير تعقيد الرسالة المشفرة على كل من المفاتيح والخوارزميات المستخدمة.

الحوسبة الكمومية تكسر التشفير

الحوسبة الكمومية هي أحد العوامل التي تؤثر على الأمن السيبراني من خلال كسر آليات التشفير الحالية التي تركز على عملية تحليل الأعداد الكبيرة. تعتبر هذه العملية محفوفة بالمخاطر لأنها تؤثر على المعلومات الحساسة وتسبب الخسارة. أجهزة الحاسوب الكمومية قادرة على حل جميع المشاكل المعقدة مثل المهام الرياضية بسرعة عالية مقارنة بأجهزة الحاسوب الكلاسيكية التي تشكل حقا تهديدا خطيرا للأمن السيبراني والعالم الرقمي. أما بالنسبة للتشفير، فيحاول الباحثون إنشاء تشفير للمقاومة الكمومية لزيادة مستوى الأمان والحد من المخاطر.

ملخص

في الختام، تعمل الحوسبة الكمومية بسرعة فائقة لحل المشكلات والمشكلات المعقدة. في الواقع، من السريع جدا كسر تقنيات التشفير والوصول إلى البيانات في وقت قصير مما يشكل تهديدا لعالم الأمن السيبراني.

في الفصل التالي، سنناقش التشفير الآمن الكمي الذي يشرح ببساطة الأساليب ذات الصلة بلغة سهلة الفهم. استعد للتعمق أكثر في الحوسبة الكمومية وفهم تقنيات التشفير الخاصة بها.

الفصل ٤: التشفير الكمي الآمن

تدور فكرة التشفير الآمن الكمي، أو التشفير ما بعد الكمي، حول تأمين الاتصالات الرقمية من التهديدات التي تشكلها أجهزة الحاسوب الكمومية .نظرا لأن أجهزة الحاسوب الكمومية لديها القدرة على كسر العديد من خوارزميات التشفير شائعة الاستخدام .لذلك هناك حاجة ملحة لتطوير وتنفيذ خوارزميات مقاومة للكم لضمان استمرار أمن البيانات الحساسة وقنوات الاتصال.

يجب أن تكون خوارزميات التشفير الآمنة الكمومية قوية بما يكفي لتحمل هجمات أجهزة الحاسوب الكمومية، والتي لديها القدرة الحسابية على حل المشكلات المستعصية حاليا على أجهزة الحاسوب الكلاسيكية بكفاءة .لذلك، تركز الجهود البحثية على تصميم وتحليل بروتوكولات التشفير التي تظل آمنة في عصر الحوسبة الكمومية، مما يضمن بقاء بنيتنا التحتية الرقمية مرنة للتهديدات الناشئة.

التشفير الكلاسيكي مقابل التشفير الكمي

يشترك كل من التشفير الكلاسيكي والكمومي في نفس الهدف المتمثل في توفير الحماية للبيانات لمنع أي تسرب للبيانات الحساسة .ومع ذلك، فإن كل نموذج من هذه النماذج له نقاط قوته وقيوده.

تعتمد أنظمة التشفير الكلاسيكية بشكل أساسي على التعقيد الحسابي والمشكلات الرياضية الصعبة والمستهلكة للوقت لأجهزة الحاسوب الكلاسيكية .وهذا يشمل على سبيل المثال مشكلة التحليل في RSA ومشكلة اللوغاريتم المنفصل في.ECC

من ناحية أخرى، يوفر التشفير الكمي الأمان باستخدام مبادئ ميكانيكا الكم، وهو تهديد لأجهزة الحاسوب الكلاسيكية لأنه لا يتأثر بالتعقيد الحسابي.

التشفير الكمي

كما ذكرنا من قبل، يعتمد التشفير الكمي على مفاهيم ميكانيكا الكم لتوفير نقل آمن للبيانات .وتشمل هذه المفاهيم ما يلي:

١- مبدأ عدم اليقين لهايزنبرغ: يمكن تحديد خاصية واحدة فقط لزوج من الخصائص المرافقة، مثل الموضع والزخم، بدقة. يستغل التشفير الكمي هذا باستخدام استقطاب الفوتون على أسس مختلفة، والاستفادة من عدم اليقين المتأصل في القياسات الكمومية لضمان الاتصال الآمن.
٢- نظرية عدم الاستنساخ: من المستحيل إنشاء نسخ متطابقة من حالة كمومية غير معروفة. تتيح هذه الخاصية اكتشاف أي تداخل في القناة الكمومية أثناء عمليات الإرسال الحرجة.
٣- التشابك الكمومي: يسمح هذا للجسيمات بالارتباط بغض النظر عن المسافة. يؤثر قياس جسيم واحد على شريكه المتشابك. يستغل النقل الآني الكمي هذا للتواصل باستخدام القنوات الكلاسيكية.

ملخص

في هذا الفصل، قدمنا لمحة عامة عن مفهوم التشفير الآمن الكمي، والاختلافات بين خوارزميات التشفير الكلاسيكية والكمية. بشكل عام، يضمن الانتقال إلى التشفير الكمي حماية أفضل للبيانات الحساسة وحماية ضد الهجمات الإلكترونية في وقت الحوسبة الكمومية.

الفصل ٥: مقدمة في توزيع المفتاح الكمومي QKD

مفهوم التوزيع المفتاح الكمومي QKD كطريقة آمنة لتوزيع المفاتيح الرمزية

تعتمد اتصالاتنا اليومية إلى حد كبير على ما يُسمى بالتشفير بالمفتاح العام (public key cryptography). هذه التقنية تساعد بشكل كبير على حماية رسائلنا. ومع ذلك، فإن العديد من الطرق التي نستخدمها حاليا في التشفير قد تعد غير آمنة تماماً أمام أجهزة الحاسوب الكمومية ذات القوة الفائقة. يمكن للمهاجمين التقاط المعلومات المشفرة التي نتبادلها ثم حفظها حتى تتطور تلك الأجهزة الكمومية الفائقة. وعندما يحدث ذلك، قد يكون المهاجمين قادرين على فتح وقراءة جميع المعلومات التي تم التقاطها مسبقا. يُطلق على هذا الهجوم اسم "احصد الآن، فك التشفير لاحقًا" او (Harvest now, decrypt later).

إذاً، كيف لنا التعامل مع هذه المشكلة؟ بإمكاننا ان نستخدم شيئًا يُسمى توزيع المفتاح الكمومي، أو QKD بشكل مختصر QKD !هو طريقة خاصة للتواصل تستخدم الخصائص المذهلة للفيزياء الكمومية.

بهذه الطريقة بإمكاننا تبادل المفاتيح سرية مع الآخرين بطريقة آمنة للغاية.

معQKD ، يمكننا إعداد مفتاح سري محمي حتى من أقوى المهاجمين، مثل تلك الأجهزة الكمومية.

يمكننا ان نعتبر الQKD كاللغة السرية التي يمكن فهمها فقط من قبلك وأصدقائك!

كيف يحمي توزيع المفتاح الكمومي (QKD) الرسائل اثناء التواصل؟

لنأخذ أليس وبوب كمثال:

ترغب أليس في إرسال رسالة سرية إلى بوب، ولكنها ترغب في التأكد من عدم قراءة أي شخص آخر هذه الرسالة سوى بوب، كيف يمكنها تحقيق ذلك؟ باستخدام توزيع المفتاح الكمومي QKD بالطبع!

بإمكاننا ان نستخدم بروتوكولBB84 ، والذي يستند إلى مبدأ عدم التحديد لهايزنبرغ.

وفقًا لمبدأ عدم التحديد لهايزنبرغ، لا يمكن تحقيق الدقة المطلقة عند قياس أو حساب موضع وزخم الجسم.

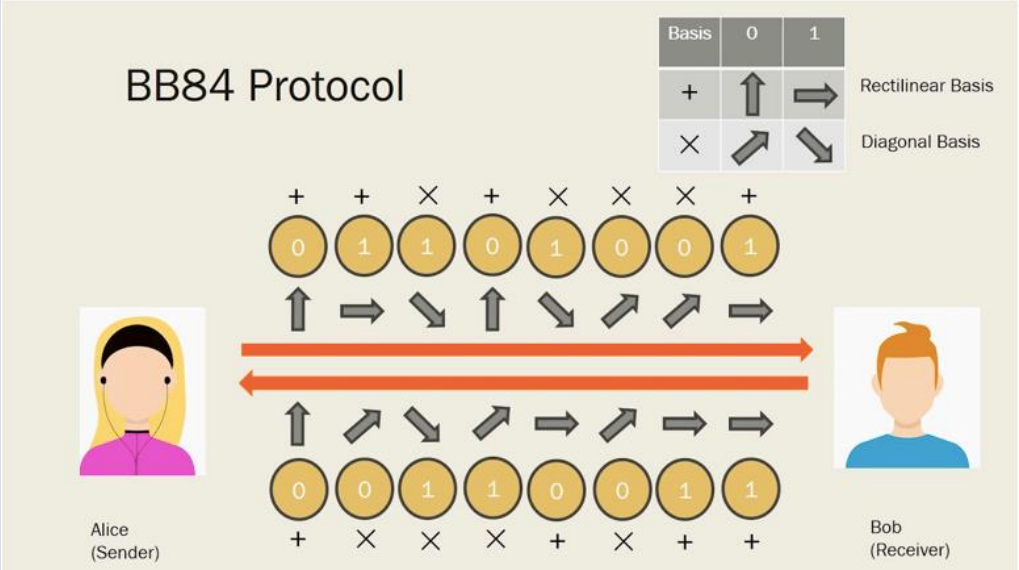
يتماشى هذا المبدأ مع أفكار بروتوكول BB84 في توزيع المفتاح الكمومي QKD. في توزيع المفتاح الكموميQKD ، يتم تشفير وفك المعلومات السرية بواسطة أليس وبوب باستخدام خصائص الجسيمات الكمومية مثل الفوتونات المستقطبة. يؤكد مبدأ عدم التحديد صعوبة قياس الجسيمات الكمومية بدقة، مما يجعل من الصعب على المتسللين التنصت على التواصل السري وفهمه. يخطط أليس وبوب لاستخدام بروتوكولBB84 ،حيث يتبادلون جسيمات الفوتون ويقيسونها بطرق مختلفة. إذا حاول أي شخص التلاعب برسائلهم، فيمكنهم اكتشاف ذلك. بهذه الطريقة يمكنهم المحافظة على سرية وأمان تواصلهم.

أولاً، ستقوم أليس بإعداد الفوتون. يمكن أن يكون الفوتون في حالات استقطاب مختلفة، مثل الصعود والهبوط أو اليسار واليمين. تمثل هذه الحالات الأرقام ١ و٠ التي تشكل رمزهم السري.

ترسل أليس الفوتون إلى بوب عبر قناة كمومية خاصة. يستلم بوب الفوتون المستقطب ويحاول معرفة كيف ضبطته أليس. يمكنه اختيار طريقتين مختلفتين لقياسه، وسنسميهما (+) و.(×)

الآن يأتي الجزء المثير! يبدأ أليس وبوب في المحادثة باستخدام قناة عادية، مثل الحديث عبر الهاتف.

ولا يقومون بالكشف عن كيف قاموا بقياس الفوتون، بحيث لا يستطيع أحد آخر معرفة رمزهم السري. خلال محادثتهما، يخمن بوب كيف قامت أليس بتقطيب الفوتون بناءً على القياس الذي اختاره. تؤكد أليس أو تصحح تخمين بوب دون الكشف عن الفعلية للفوتون. تتكرر هذه العملية لكل فوتون يستلمونه. إذا كان هناك متسلل يحاول الاستماع، فقد يقوم بتغيير استقطاب الفوتونات. الآن، يمكن لأليس وبوب اكتشاف هجوم كهذا أثناء بدء محادثة عامة. من خلال مقارنة قياساتهم ومناقشة استقطاب الفوتونات، يمكنهم معرفة ما إذا كان شخص ما قد تلاعب برسالتهم السرية.



لضمان أمان رمزهم السري، يقوم أليس وبوب بحساب ما يسمى بمعدل أخطاء البت الكمومي (QBER). إذا كان معدل أخطاء البت الكمومي مرتفعًا جدًا، فهذا يعني أنه قد يكون هناك متسلل، لذا يتوقفون عن التواصل ويبدأون من جديد. باتباع هذه الخطوات واستخدام توزيع المفتاح الكمومي (QKD)، يمكن لأليس وبوب إنشاء رمز سري يحافظ على سرية وسلامة رسائلهم ويحميها من أي شخص يحاول الاستماع إلى محادثاتهم.

مزايا وعيوب توزيع المفتاح الكمومي(QKD)

المزايا:

اتصالات مضمونة للمستقبل: يضمن QKD أنه لا يمكن التلاعب في الاتصالات بعد حدوثها. على عكس أنظمة التشفير الأخرى، لا يمكن نسخ أو تخزين مفاتيحQKD ، مما يوفر مستوى أعلى من الأمان.

حماية ضد فك التشفير التراجعي: يقضي QKD على فرصة المتسللين لتخزين الرسائل المشفرة والمفاتيح العامة لفك التشفير في المستقبل. إنها الطريقة الوحيدة المعروفة لمنع فك التشفير التراجعي، مما يجعلها مناسبة لحماية البيانات السرية طويلة الأمد.

تخزين آمن للبيانات الحساسة QKD : مثالي لحماية المعلومات المالية ومعلومات المستهلك، والسجلات الصحية الخاصة (مثل بيانات الجينوم البشري)، واتصالات الحكومة والجيش.

أمان مثالي نظرياً: تمت تجربة بروتوكولاتQKD بشكل نظري وثبت أنها آمنة تمامًا، مما يوفر مستوى أعلى من الثقة مقارنة بالخوارزميات الأخرى.

أمان غير مشروط: يمكن اعتبار" QKD آمنًا بشكل غير مشروط" لأنه لا يستند إلى افتراضات.

على الرغم من أنه لا يمكن أن يكون أي نظام آمن تمامًا في الواقع، إلا أن المبدأ الأساسي لـ QKD يوفر أساسًا متينًا للأمان.

العيوب:

تعقيد تكنولوجي: يتطلب تنفيذ QKD تكنولوجيا متخصصة وظروفًا منظمة، مما يجعل من الصعب تنظيمها للنشر الأوسع.

سرعات انتقال أقل: ينقل QKD البيانات حاليًا بمعدل أبطأ من طرق التشفير التقليدية.

تكاليف أعلى: غالبًا ما تكون أنظمة QKD أكثر تكلفة لإنشائها وصيانتها من التقنيات التشفيرية النموذجية.

تقنيات تشفير إضافية: لا يمكن لـ QKD وحده أن يوفر أمانًا شاملاً من نقطة إلى نقطة؛ ويتطلب استخدام تقنيات تشفير إضافية.

قيود عملية: يمكن أن تؤثر البيئة والضوضاء على موثوقية وكفاءة أنظمة.QKD

ملخص:

توزيع المفتاح الكمومي (QKD) هي طريقة آمنة لتوزيع المفاتيح السرية بحيث تغطي ضعف التشفير التقليدي أمام أجهزة الكمبيوتر الكمومية المستقبلية. هذه الطريقة تضمن أماناً بعد الاتصال وتوفر مزايا في تأمين البيانات السرية طويلة الأمد. يستخدم QKD بروتوكول BB84 الذي يُشفر المعلومات باستخدام خصائص الجسيمات الكمومية مثل الفوتونات المستقطبة. مما يجعل من الصعب على المتسللين التنصت على الاتصال. يوفر QKD اتصالات مضمونة للمستقبل، وحماية ضد فك التشفير التراجعي، وتخزين آمن للبيانات الحساسة.

كما انه يعتبر آمناً بشكل غير مشروط. ومع ذلك، يمكن أن تكون عملية التنفيذ العملي معقدة ومكلفة، مع سرعات انتقال أقل وحاجة لتقنيات تشفير إضافية. الوعي بهذه المزايا والقيود يساعد في اتخاذ القرارات المتعلقة بالاتصالات الآمنة.