Encryption and Data Security: Protecting Information in the Digital Age

التشفيير وامن البيانات:حماية المعلومات في العصر الرقمي

(اختبار صلاحية تدريس(

الفئة المستهدفة: طلبة المرحلة الأولى والثانية

كلية القانون

اسم متدرب: رؤى خالد سكران

ماجستير هندسة تكنلوجيا المعلومات

البريد الإلكتروني

ruaa.khalid.sakran@uomus.edu.iq

تشفير البيانات والمعلومات

مقدمة

في ظل التزايد المستمر للجرائم الإلكترونية خلال السنوات الأخيرة باتت حماية أمن الشبكة ضرورة لا غنى عنها للمنظمات التي ترغب في الحفاظ على معلوماتها من الاختراق وتتعدد التقنيات التي ت ستخدم في هذا الغرض ومن أبرز تلك التقنيات تشفير البيانات والتي ت عد من أكثر التقنيات أمان ا وفعالية في حماية البيانات

يلعب التشفير دورا حاسما في ضمان أمن البيانات والخصوصية في عالم اليوم الرقمي. مع تزايد الجرائم الإلكترونية وانتهاكات البيانات أصبح التشفير ضرورة للأفراد والشركات والحكومات لحماية معلوماتهم الحساسة من الوصول غير المصرح به.

يساعد التشفير على منع اختراق البيانات من خلال جعل من الصعب على المخترقين الوصول إلى المعلومات الحساسة وقراءتها. حتى لو تمكن أحد المخترقين من اعتراض البيانات المشفرة فلن يتمكن من فك تشفيرها دون مفتاح فك التشفير الصحيح. وهذا يجعل من الصعب على مجرمي الإنترنت سرقة البيانات واستخدامها لأغراض خبيثة.

يساعد التشفير أيض ا على حماية خصوصية المستخدم من خلال ضمان وصول الأفراد المصرح لهم فقط إلى المعلومات الحساسة. وهذا الأمر مهم بشكل خاص في صناعات مثل الرعاية الصحية والمالية والحكومة حيث تكون خصوصية وأمن البيانات الشخصية ذات أهمية قصوى.

تعريف التشفير

التشفير هو عملية تحويل نص عادي أو بيانات إلى لغة مشفرة لا يمكن قراءتها إلا من قبل الأفراد أو الأنظمة المصرح لهم. وهي تقنية مهمة تستخدم لحماية المعلومات الحساسة من الوصول غير المصرح به وضمان أمن البيانات. ينطوي التشفير على استخدام خوارزميات معقدة ومفاتيح تشفير لتحويل البيانات إلى صيغة غير قابلة للقراءة مما يجعل من المستحيل عمليا على أي شخص فك تشفير الرسالة الأصلية دون مفتاح فك التشفير الصحيح.)(

يستخدم التشفير عدد ا من خوارزميات التشفير منخفضة المستوى لتحقيق واحد أو أكثر من أهداف أمان المعلومات هذه. تتضمن هذه الأدوات خوارزميات التشفير وخوارزميات التوقيع الرقمي وخوارزميات التجزئة ووظائف أخرى. ستصف هذه الصفحة عدد ا قليلا من خوارزميات التشفير منخفضة المستوى الأكثر استخدام ا. تتمثل فكرة أي نظام تشفير في إخفاء المعلومات السرية بطريقة يصبح من خلالها معناها غير مفهوم بالنسبة إلى أي شخص غير مصر ح له بالاطلاع عليها. يتمثل الاستخدامان الأكثر شيوع ا للتشفير في تخزين البيانات بأمان في ملف كمبيوتر أو نق لها عبر قناة غير آمنة مثل الإنترنت. في كلتا الحالتين حقيقة كون المستند مشفر ا لا تمنع الأشخاص غير المصر ح لهم بالوصول إليه ولكنها تضمن عدم تمك نهم من فهم ما يرونه.

غالب ا ما يطل ق على المعلومات الم راد إخفاؤها اسم »النص الأصلي« فيما يطلق على عملية إخفائها اسم »التشفير«. ويطلق على النص الأصلي المشف ر اسم »النص المشف ر« أو »بيان التشفير« كما يطلق على مجموعة القواعد المستخدمة في تشفير معلومات النص الأصلي »خوارزمية التشفير«. عادة تعتمد هذه الخوارزمية على »مفتاح التشفير« وهو يمثل مدخل ا لها بالإضافة إلى الرسالة. وحتى يتمكن المتلقي من استرجاع الرسالة من خلال النص المشف ر يجب أن تتوافر »خوارزمية فك التشفير« التي عند استخدامها مع »مفتاح فك التشفير« المناسب تسترجع النص الأصلي من النص المشف ر.

أنواع التشفير في أمن المعلومات

تتعدد أنواع التشفير في الأمن السيبراني يمكن ذكرها على النحو التالي:

1. التشفير المتناظر .

التشفير المتناظر:Symmetric Encryption والذي ي عرف أيض ا باسم تشفير المفتاح الخاص هو طريقة تعتمد على استخدام بعض الخوارزميات مفتاح ا خاص ا في عمليات التشفير وفك التشفير أي أن المفتاح الم ستخدم للترميز هو نفسه الم ستخدم لفك الشفرة وتتطلب هذه الطريقة وصول المرسل والمستقبل إلى نفس المفتاح لذلك يحتاج المستلم إلى المفتاح قبل فك تشفير الرسالة.

وت عد طريقة التشفير المتماثل هي الطريقة الم فضلة للمستخدمين الأفراد والأنظمة المغلقة كما أنها أقل أمان ا.

2. التشفير غير المتناظر.

التشفير غير المتناظر Asymmetric Encryption والذي ي عرف أيض ا باسم التشفير

بالمفتاح العام وي ستخدم في غالبية بروتوكولات أمن الإنترنت وفي هذه الطريقة يتم استخدام مفتاحين في عملية التشفير وهما مفتاح عام وخاص توجد بينهما علاقة رياضية والاثنين عبارة عن أرقام كبيرة ليست متطابقة ولكنها مقترنة ببعضها البعض إذ يستخدم المستخدم أحدهما للتشفير والآخر لفك التشفير. والمفتاح العام في التشفير غير المتناظر متاح ا لأي شخص مجان ا بينما المفتاح الخاص يمتلكه المستلمين المقصودين فقط الذين يحتاجون إليه لفك شفرة الرسائل.)(

مراحل عملية تشفير البيانات:

تمر عملية تشفير البيانات بعدة مراحل نوضحها فيما يلي:

1- تحديد المتطلبات الأمنية

أولى مراحل عملية تشفير البيانات هي تحديد المتطلبات الأمنية للمؤسسة إذ أن اختلاف أنظمة التشفير في القوة وقدرات المعالجة يفرض على المنظمة تقييم احتياجاتها الأمنية أول ا.

وعند تحديد المتطلبات الأمنية يتم الكشف عن نقاط الضعف في النظام من أجل تقييم التهديدات ومعرفة القرارات التجارية ولوائح الامتثال التي يمكن أن تؤثر على الاستراتيجية مع مراجعة أطر الأمن السيبراني.

2- تصنيف البيانات

بعد ذلك يتم تصنيف البيانات التي تخزنها وترسلها المنظمة والتي تشمل البيانات المالية ومعلومات العملاء وتفاصيل حساب المؤسسة وكافة البيانات التي يعتمد عليها العمل. وت صنف بيانات المؤسسة وفق ا لدرجة حساسيتها ومدى تنظيمها وآلية التنظيم وعدد مرات استخدامها.

3- تحديد أدوات التشفير المناسبة

في هذه الخطوة يتم تحديد أدوات تشفير البيانات التي تناسب احتياجات المنظمة ولذلك لا بد من تثبيت مجموعة من خوارزميات وتقنيات التشفير لحماية جميع أشكال البيانات عبر قواعد البيانات والملفات والتطبيقات الخاصة بالمنظمة ومن ثم يتم الاختيار ما بين التشفير المتماثل وغير المتماثل وذلك بعد موازنة المفاضلات بين السرعة والأمان والتعقيد.

ومن خلال تقنيات التشفير يمكن تشفير البيانات على مستويات متعددة في أماكن العمل وفي السحابة وتلك المستويات هي التطبيق وقاعدة البيانات والملفات كما تقدم تلك التقنيات لوحة معلومات إدارية مركزية لتشفير البيانات وتشفير السياسات والتكوينات الرئيسية وضوابط تسجيل السجلات والمشاركة بين المجموعات والوصول القائم على الأدوار. ويساعد استخدام تقنيات التشفير الصحيحة في جميع مستويات تخزين البيانات ونقلها على الحفاظ على بيانات المنظمة آمنة قدر الإمكان.

4- الاستعداد لنشر خطة التشفير

في هذه الخطوة يجب أن تضع المنظمة خطة لتنفيذ استراتيجية التشفير الخاصة بها

والتخطيط لحل أي مشكلة يمكن أن تنشأ وعلى سبيل المثال فقد يؤدي التخطيط الجيد والمبكر إلى تقليل الاضطرابات الناتجة عن دمج طريقة التشفير الجديدة الخاصة بالمنظمة مع الأنظمة القديمة.

ولتنفيذ هذه الخطوة على النحو الأمثل ي فضل دعم فريق تكنولوجيا المعلومات الخاص بالمنظمة من خلال التعاون مع مزود تكنولوجيا المعلومات التابع لجهة خارجية.

5- إنشاء المفاتيح وتخزينها وتطبيق التشفير

بعد ذلك يتم إنشاء المفاتيح الخاصة بالتشفير ومفاتيح فك التشفير مع حفظ تلك المفاتيح بشكل آمن في ملفات مشفرة من أجل حمايتها من الوصول غير المصرح به. ثم تستخدم المنظمة نظام التشفير الذي اختارته مع استخدام مفتاح تشفير البيانات ومن ثم تطبيق الخوارزمية التي تحول البيانات إلى نصوص مشفرة لا يمكن قراءتها.

6- التحقيق والمراقبة وفحص الأمان

بعد تطبيق التشفير لا بد من التحقق من أن المفاتيح والبيانات المشفرة لا يمكن أن يصل إليها سوى الأشخاص المصرح لهم مع وضع نظام مراقبة يكشف عن أي محاولة للوصول إلى تلك البيانات.

وللتأكد من خلو نظام التشفير من أي ثغرة أمنية تسمح بكسر التشفير لا بد من إخضاع نظام التشفير للفحص الدوري واختبار الاختراق.

أهداف التشفير:

ت ستخدم عملية تشفير البيانات من أجل تحقيق مجموعة من الأهداف وهي:)(

1. الحفاظ على أمن البيانات

توفر عملية التشفير الحماية للبيانات من أجل منع انتهاكها خلال النقل والتخزين ففي حال فقدان الجهاز مثل الكمبيوتر أو الهاتف تظل البيانات المشفرة آمنة ومن خلال خطوط الاتصال المشفرة يمكن نقل البيانات الحساسة دون خوف من اختراقها.

وي عد طلب بروتوكول نقل النص الفائق الآمن)HTTPS(هو نوع التشفير الم ستخدم في هذا الغرض إذ ي ستخدم في التحقق من أصل الخادم أو موقع الويب.

2. المزيد من الخصوصية

ت ستخدم عملية تشفير البيانات من أجل التأكد من أن الذي يقرأ الرسالة هو صاحب البيانات أو المستلم المقصود وبالتالي لا يمكن أن ت قرأ البيانات الحساسة من ق بل شبكات الإعلانات ومهاجمي البيانات ومقدمي خدمات الإنترنت.

3. حماية البيانات من التلاعب

ي عد تشفير البيانات من أهم التقنيات التي تساعد على حماية البيانات من التلاعب خلال نقلها

إذ تمنع المخترقين من تغيير محتويات الملف وحجمه ونوعه كما تمنعهم من حذف أو نسخ الملفات خلال نقلها ولذلك تستخدمه شركات مواقع التواصل الاجتماعي للحفاظ على المعيار مستوى الأمان لديها.

4. التحقق من بيانات الويب

من أبرز أهداف استخدام التشفير التحقق من بيانات موقع الويب فعند زيارة موقع ويب تنتقل المعلومات المشفرة بين متصفح الإنترنت وخادم الموقع ومن خلال هذا الانتقال يمكن التحقق من اتصال المتصفح بموقع الويب الحقيقي وليس المنشور.

كما يساعد التشفير على تثبيت اتصال الإنترنت ومن ثم ضمان إرسال واستلام الوحدات الصغيرة من الحزم وهو ما يؤدي إلى منع فقدان الحزمة.

التقنيات المستخدمة في التشفير:

إليكم فيما يلي التقنيات الأكثر استخدام ا في عملية تشفير البيانات:)(

1. كلمات مرور الكمبيوتر

تساعد هذه التقنية على الحفاظ على أمن الكمبيوتر إذ يتم تشفير كلمات المرور لمنع المتسلل من قراءتها حتى وإن نجح في الوصول إلى قاعدة بياناتها. وتعتمد هذه التقنية على تجزئة كلمة المرور وتشفيرها قبل تخزينها فعندما يقوم المستخدم بتسجيل الدخول يتم تجزئة كلمة المرور الخاصة به ومقارنتها بالتجزئة التي تم تخزينها سابق ا.

2. المصادقة

تعتمد تقنية التشفير للمصادقة على البروتوكولات التي تتحقق من هوية المستخدم ومن أن لديه حقوق الوصول المطلوبة إلى المورد. وت ستخدم هذه التقنية عند الوصول إلى حساب مصرفي أو تسجيل الدخول إلى جهاز كمبيوتر أو استخدام شبكة آمنة.

3. التوقيعات الإلكترونية

ي ستخدم التشفير في إنشاء التوقيعات الإلكترونية ويتم التحقق من صحتها عن طريق تشفير المفتاح العام وت ستخدم تلك التوقيعات كمعادل رقمي للتوقيع المكتوب بخط اليد من أجل التوقيع على الوثائق.

4. العملات الرقمية

وهي العملات التي تستخدم التشفير بغرض حماية المعاملات ومنع الاحتيال وذلك عن طريق استخدام الخوارزميات المعقدة ومفاتيح التشفير فيصعب تشكيل المعاملات أو العبث بها.

5. التصفح الآمن للويب

ي ستخدم التشفير في حماية المستخدمين من الاختراقات والتجسسات خلال التصفح عبر الإنترنت وفي هذه التقنية يتم تشفير البيانات المرسلة بين خادم الويب والعميل باستخدام

التشفير بالمفتاح العام بواسطة طبقة المقابس الآمنة)SSL(وبروتوكولات أمن طبقة النقل (TLS).

ست فوائد أساسية للتشفير

1. يساعد التشفير في الحفاظ على تكامل البيانات

المتسللون لا يسرقون المعلومات فحسب بل يمكنهم أيض ا تغيير البيانات لارتكاب عملية احتيال. وفي حين أنه من الممكن للمتسللين المهرة تغيير البيانات المشفرة فإن مستلمي البيانات سيكونون قادرين على اكتشاف التلف مما يسمح باتخاذ استجابة سريعة.)(

2. التشفير يساعد المؤسسات على الالتزام باللوائح التنظيمية

تضع العديد من الصناعات مثل الخدمات المالية أو الرعاية الصحية لوائح صارمة حول كيفية استخدام بيانات المستهلك وتخزينها. ويساعد التشفير المؤسسات على تلبية هذه المعايير وضمان الامتثال لها.

3. يحمي التشفير البيانات عند انتقالها عبر الأجهزة

يستخدم معظمنا أجهزة متعددة في حياتنا اليومية ويمكن أن ينطوي نقل البيانات من جهاز إلى آخر على بعض المخاطر. تساعد تقنية التشفير في حماية البيانات عبر الأجهزة حتى أثناء النقل. كما تساعد إجراءات الأمان الإضافية مثل المصادقة المتقدمة في ردع المستخدمين غير المصرح لهم بالوصول.

4. يساعد التشفير عند نقل البيانات إلى التخزين السحابي

يقوم المزيد والمزيد من المستخدمين والمؤسسات بتخزين بياناتهم في السحابة مما يعني أن أمان السحابة بات ضروري ا. يساعد التخزين المشفر في الحفاظ على خصوصية تلك البيانات. ويجب على المستخدمين التأكد من أن البيانات مشفرة أثناء نقلها وأثناء استخدامها وأثناء التخزين.

5. التشفير يساعد المؤسسات على تأمين المكاتب

يشمل العديد من المؤسسات مكاتب تعمل عن ب عد وخاصة في مرحلة ما بعد الجائحة. يمكن أن يشكل ذلك مخاطر على الأمن الإلكتروني حيث يتم الوصول إلى البيانات من عدة مواقع مختلفة. وهنا يساعد التشفير في الحماية من السرقة أو الفقد العرضي للبيانات.

6. يحمي تشفير البيانات الملكية الفكرية.

تقوم أنظمة إدارة الحقوق الرقمية بتشفير البيانات في حالة السكون وي قصد بها في هذه الحالة الملكيات الفكرية مثل الأغاني أو البرامج لمنع الهندسة العكسية والاستخدام غير المصرح به أو إعادة إنتاج المواد المحمية بحقوق النشر.

1. التحكم في الوصول | Access Control

يمكن استخدام التشفير للتحكم في الوصول للتأكد من أن الأطراف التي لديها الأذونات المناسبة فقط هي التي يمكنها الوصول إلى مورد. فقط أولئك الذين لديهم مفتاح فك التشفير الصحيح يمكنهم الوصول إلى المورد بفضل التشفير.

2. الاتصال الآمن | Secure communication

للاتصال الآمن عبر الإنترنت يعد التشفير أمرا بالغ الأهمية. يوفر آليات آمنة لنقل المعلومات الخاصة مثل كلمات المرور وأرقام الحسابات المصرفية والبيانات الحساسة الأخرى عبر الإنترنت.

3. الحماية من الهجمات | Protection against attacks

يساعد التشفير في الدفاع ضد أنواع مختلفة من الاعتداءات بما في ذلك هجمات الإعادة وهجمات الرجل في الوسط. يقدم استراتيجيات لاكتشاف هذه الاعتداءات ووقفها.

4. الامتثال للمتطلبات القانونية | Compliance with legal requirements

يمكن أن يساعد التشفير الشركات في تلبية مجموعة متنوعة من المتطلبات القانونية بما في ذلك تشريعات حماية البيانات والخصوصية.

الاستخدامات للتشفير

للتشفير تطبيقات واسعة في المجالات الدبلوماسية والعسكرية والأمنية والتجارية والإعلامية والمصرفية والمعلوماتية. ويستخدم على نطاق واسع منها :)(

1. في كل مرة تستخدم فيها ماكينة صراف آلي أو تشتري شيئ ا عبر الإنترنت باستخدام هاتف ذكي يتم استخدام التشفير لحماية المعلومات التي يتم نقلها.
2. تأمين الأجهزة مثل التشفير لأجهزة الكمبيوتر المحمولة.
3. تستخدم معظم مواقع الويب السليمة "طبقة المقابس الآمنة")SSL(وهي شكل من أشكال تشفير البيانات عند إرسالها من موقع ويب وإليه. وهذا يمنع المهاجمين من الوصول إلى تلك البيانات أثناء نقلها. ابحث عن رمز القفل في شريط URL وحرف في "https://" للتأكد من أنك تجري معاملات آمنة ومشفرة عبر الإنترنت. "s"
4. يمكن أيض ا أن يتم تشفير بريدك الإلكتروني باستخدام بروتوكولات مثل OpenPGP.
5. تستخدم الشبكات الافتراضية الخاصة)VPN(التشفير ويجب تشفير كل ما تخزنه في السحابة. يمكنك تشفير محرك الأقراص الثابتة بالكامل بل إجراء مكالمات صوتية مشفرة.
6. يستخدم التشفير لإثبات سلامة وصحة المعلومات وهذا باستخدام ما يعرف بالتوقيعات الرقمية. التشفير جزء لا يتجزأ من إدارة الحقوق الرقمية وحماية المؤلفات.

7. يمكن استخدام التشفير لمحو البيانات. نظر ا لأنه يمكن أحيان ا إعادة المعلومات المحذوفة باستخدام أدوات استعادة البيانات فإنك إذا قمت بتشفير البيانات أولا وتخلصت من المفتاح فلن يمكن لأي شخص أن يسترد إلا النص المشفر وليس البيانات الأصلية.

8. في المراسلات النصية المكتوبة بين الأفراد والشركات والبعثات الدبلوماسية والجهات الحكومية والدول عامة لحماية المعلومات ولمنع الاطلاع عليها في أثناء عملية نقلها.

9. في منظومات الاتصالات الشخصية للحفاظ على الخصوصية كما هي الحال في أجهزة الهاتف الجوال mobile لمنع المتنصتين على الاتصالات)مسترقي السمع(من فهم المحادثات الهاتفية.

10. في منظومات الاتصالات العسكرية والأمنية الخاصة وللحفاظ على سرية المعلومات المنقولة سواء أكانت محادثات كلامية أم نصوصا مكتوبة أم صورا ومخططات مختلفة.

11. في منظومات الاتصالات التجارية للحفاظ على سرية التبادلات التجارية وفي المصارف حفاظا على سرية العمليات المالية والمصرفية. ويستخدم على نطاق واسع في إشارات البث التلفزيوني الرقمي عن طريق السواتل بهدف الحماية التجارية ومنع غير المشتركين من فك تعمية الصورة التلفازي ة ورؤية البرامج.

12. في شبكات المعلوماتية التي تنقل المعلومات بين الحواسيب للحفاظ على خصوصية البيانات والمعلومات المنقولة أو سري تها.