المحاضرة الثالثة:
التشفير و الترميز

تمهيد:

نشهد العصر الرقمي بكل إنجازاته وثورة معلوماته، هذه المعلومات تكتب وتخزن وتنقل بشكل رقمي مشفر أو مرمز، وقد أذهل العلماء وجود التشفير والترميز في كل أركان الكون، بدءا من أشكال تواصل المخلوقات إلى نواة الذرة ، ومن أحماض الإنسان وصفاته، إلى مائه وسيالات أعصابه. يقول خبراء نظرية المعلومات أن المعلومات إحدى الخصائص الأساسية للكون، شأنها شأن المادة والطاقة، وكما أن الكتلة هو التعبير عن المادة، فإن التنظيم هو التعبير عن المعلومات، والتشفير والترميز هو الحافظ لها شكلا ومضمونة، وهو الأمان له.

7 .بناء المفاهيم: أولا : التشفيرEncryption

تعتبر تقنية التشفيرEncryption: من أكثر التقنيات المطلوبة في

عالم تجتاحه التكنولوجيا بشكل سريع وواسع. تمثل هذه التقنية العصب الأساسي للتواصل الالكتروني أو للشبكات العنكبوتية، لذلك هي تدخل في كل عملية اتصال وتواصل بين أي جهازين رقميين سواء من نفس النوع أو مع الأنواع الأخرى .

من المفاهيم المرتبطة بالتشفير : أنه عبارة عن عملية تغيير شكل المعلومات إلى شكل آخر باستخدام المعادلات الرياضية التي تتطلب وجود قيم معينة, و هذه القيم هي المفتاح المستخدم في عملية التشفير الناتج النهائي من عملية التشفير هو نص غير مقروء ولكن مقروء للشخص الذي يحمل المفتاح, أو الشخص الذي حاول ونجح في كسر التشفير.[1]

- **الغرض من التشفير: هو تحويل البيانات من الشكل المقروء إلى الشكل غير المقروء وذلك من أجل عدم السماح للأشخاص الغير مخولين لقراءتها أو التعامل بها، ولكن المشكلة**

أنه من السهولة إدراك أن النص الغير مقروء هو مشفر بالأصل, عملية التشفير تتطلب وجود مفتاح التشفير ليحول النص العادي (الرسالة السرية) إلى النص المشفر باستخدام خوارزميات التشفير [يكون من المهم جدا استخدام المفتاح الذي يتم الاحتفاظ به سرا جنبا إلى جنب مع النص الأصلي والخوارزمية من أجل تنفيذ عملية التشفير. على هذا النحويطلب كل من النص المشفر و الخوارزمية ومفتاح التشفير وذلك للعودة إلى النص الأصلي

•آلية عمل التشفير وفك التشفير

[1] يتقاطعمفهومالتشفيرمعمفهومإخفاءالبيانات

والتيهيعمليةمشابهةللتشفيرمنناحيهالغرضالأساسيوهوالتأكدمنعدمحصولالأشخاصالغيرمخولينمنالوصوللليانات, Steganography:
ولكنإخفاءالبياناتتمتلكالسلاحالأقوىوهوعدمإدراكالأشخاصأنهذهالبياناتهيبياناتحساسة,
لأنالناتجهوبياناتمقروءةولكنمجردبياناتمنسوخةوغيرأصليةوإخفاءالبياناتهيعمليهجعلبياناتحساسةفيبياناتغيرمهمةونقلهامنطرفإلىآخردونإشعارالآخرينبوجودبياناتحساسةتمأويتمنقلها.

بما أن التشفير هو عملية تغيير محتوى نص (بيانات إلى أرقام ورموز معقدة يصعب فهمها، تتم باستخدام خوارزميات رياضية عديدة ومتنوعة. وقوة التشفير مرتبطة بخوارزمياتها من جهة وبالمفاتيح من جهة أخرى، لذلك يسعى خبراء الأمن إلى إنتاج خوارزميات تستخدم دوال رياضة (Function)معقدة مع مفاتيح طويلة قدر الإمكان لمنع القراصنة من فك التشفير. فأثناء إرسال أي نوع من المعلومات أكانت نضا، أرقامة، صورة أو غير ذلك تتم معالجتها خوارزمية، بعدها يتم دمجها مع المفتاح، الذي ينتج عبر خوارزمية خاصة، بطريقة محددة ليظهر النص المشفر المراد إرساله. أما عملية فك التشفير أو فك الترميز (Decryption) تتلخص بإعادة النص المشفر الى وضعه السابق كنصت مفهوم ومقروء، وهذه المسألة تتم باستخدام الخوارزمية نفسها والمفاتيح بحسب نوع التشفير.

8 .أنواع التشفير

أولا : التشفير المتناظر: يعرف أيضا بتشفير المفتاح الخاص:

حيث يستخدم المفتاح نفسه للتشفير ولفك التشفير. يجب أن يتفق الطرفان على هذا المفتاح، وهنا نقطة ضعف تسجل على هذا النوع، خاصة عند إرسال المفتاح عبر الشبكة العنكبوتية، فربما يحصل أحدهم على هذا المفتاح بطريقة أو بأخرى وبالتالي يقوم بفك تشفير المعلومات المرسلة التي تكون أحيانة غاية في الأهمية. لذلك يعمل خبراء الأمن على إيجاد طريقة تضمن انتقال المفاتيح من دون العبث بها عبر اعتماد طرق تضمن سريتها] .يمكن القول أن التشفير المتماثل أو المتناظر هوتحويل الرسالة إلى لغة غير مفهومه لا يستطيع فهمها إلا المرسل و المرسل له عن طريق برنامج يفك هذا التشفير بمفتاح خاص Secret Key و نفس المفتاح الذي يستخدم في التشفير يستخدم في فك السائل المشفرة (ومن هنا تمت تسميته بالمتماثل أو التناظري).

ثانيا : التشفير غير المتناظر: يعرف أيضا بتشفير المفتاح العام:

حيث يستخدم فيه زوج من المفاتيح، أحدهما لتشفير الرسالة والآخر لفكها، يعرف الأول بالمفتاح العام وسمي بذلك لأنه يكون موعة على جميع المستخدمين الذين يتراسلون، وهنا تكمن نقطة الضعف، وهي كيفية توزيع المفتاح على جميع المستخدمين الذين قد يكون عددهم كبير في بعض الأحيان. أما المفتاح الثاني فيعرف بالمفتاح الخاص وسمي بذلك

لأنه معلوم المستخدم واحد فقط هو مالكه، ويستخدم لفك الرسائل المشفرة بالمفتاح الأول، لذلك يبقى عدد المفاتيح الخاصة يساوي عدد المستخدمين.

.1.بناء المفاهيم: ثانيا : الترميزEncoding

الترميز: هو عملية تحويل المعلومات من هيئة معينة إلى هيئة أخرى وفق نظام محدد , أو هو تمثيل المعلومات بنظام معين فكل ملف يستخدمه الكومبيوتر مثلا هو عبارة عن معلومات مرمزة

وفقا لنظام معين حسب الهيئة التي يكون عليها[2]. [لا يقتصر الترميز على ملفات الصوت والصور والفيديوكما يعتقد البعض بل إن كل هيئة رقمية هي هيئة مرمزة . فالبرامج المكتوبة بلغات البرمجة المختلفة وأطقم الحروف المختلفة للغات كاللاتينية والعربية الممثلة بشفرات، كلها ملفات قابلة للترميز] الترميز هو عملية تحويل البيانات بحيث يمكن إرسالها دون خطر عبر قناة اتصال أو تخزينها دون خطر على وسيط تخزين. على سبيل المثال ، لا تتعامل أجهزة الكمبيوتر مع النص ، بل تتعامل فقط مع البايتات ، وبالتالي فإن ترميز النص هو وصف لكيفية تحويل النص إلى شكل آخر مقروء يمكن للحاسب قراءته. (لغة الحاسوب)[3]

الهدف من الترميز : الغرض من الترميز هو

- **تحويل البيانات بحيث يمكن استهلاكها بشكل صحيح (وأمان) بواسطة نوع مختلفمن النظام**
- **يستخدم من أجل: الحفاظ على قابلية استخدام البيانات ، أي لضمان قدرتها علىالاستهلاك بشكل صحيح.**
- **آلية استرجاع البيانات: لا يوجد مفتاح ويمكن عكسه بسهولة شريطة أن نعرف الخوارزمية المستخدمة في الترميز.**
- **الخوارزميات المستخدمة: أسكي ،يونيكود ، ترميز .Base64، URLمثال: البيانات الثنائية التي يتم إرسالها عبر البريد الإلكتروني ، أو عرض الأحرف الخاصة على صفحة الويب.**

ويمكن أن يرتبط الترميز بمعنيين أساسيين :

- **المعنى الأول : في تقنية الكمبيوتر ، الترميز هو عملية تطبيق كود معين ، مثل الحروف والرموز والأرقام ، على البيانات لتحويلها إلى تشفير مكافئ.**
- **المعنى الثاني: في الإلكترونيات حيث يشير الترميز إلى التحويل التناظري الى التحويل الرقمي.**

الفرق بين الترميز والتشفير.

ويمكن مقارنة عملية الترميز(Encoding) مع عملية التشفير (Encryption). أن نعتبر التشفير احد أنواع الترميز , المرتبط بموضوع السرية , فالترميز لا يعني كثيرا" بموضوع

---

[2] يعرفالترميز بعلمالتعميةمنذالقدم،إذاستخدملإخفاءمعلوماتالرسائل،وانتهجتطرقونظمرمزيةعديدةمنأجلذلك.
وقديغيبعنالكثيرينأنأصلهعربيوأنالعربهمآباؤهوبدينلهمولادةونشأةوتطورة،وبعدكتابالكندير سالةفياستخراجالأعدادالمضمرة»،أولمرجعمعروففيعلمالتعمية واستخراجالمعمىواصطلحعلىتسميتهحديثاعلمالشفرة.

[3] يعمل الترميز على تحويل البيانات إلى تنسيق آخر باستخدام مخطط متاح للجمهور بحيث يمكن عكسه بسهولة بلا يتطلب مفتاحا لأن الشيء الوحيد المطلوب لفك تشفيره هو الخوارزمية التي تم استخدامها لتشفيرها.

السرية أو الأمان , إذ لا يخرج عن كونه خوارزميات وقواعد معلنة للتحويل من نظام الى آخر . أما التشفير فهي عملية ترميز معقدة وسرية تتبع خوارزميات معينة الطمس هوية البيانات.

•الترميز يحول البيانات إلى تنسيق آخر باستخدام مخطط متاح للجمهور بحيث يمكن

عكسه بسهولة. في حين .التشفير يحول البيانات إلى تنسيق آخر بطريقة لا يمكن إلا الفرد (أفراد) محددين عكس التحول. الترميز هو الحفاظ على قابلية استخدام البيانات ويستخدم المخططات المتاحة للجمهور. بينما التشفير هو للحفاظ على سرية البيانات وبالتالي فإن القدرة على عكس التحول (مفاتيح) تقتصر على بعض الناس..

قائمة المراجع الخاصة بالمحاضرة:

1. معايير التشفير وأمننةالمعلومات . (2018). الموسوعة الجزائرية للدراسات السياسية والاستراتيجية . متاح علىhttps://www.politics-dz.com :
2. Encoding(2011). Techopedia . URL : https://www.techopedia.com/definition/948/encoding
3. Margaret Rouse.(2011). .encoding and decoding . URL: https://searchnetworking.techtarget.com/definition/encoding-and-decoding
4. DANIEL MIESSLER(2019). Encoding vs. Encryption vs. Hashing vs. Obfuscation .URL: https://danielmiessler.com/study/encoding-encryption-hashingobfuscation/
5. Eva Sarafianou (2019) How Secure Are Encryption, Hashing, Encoding. and Obfuscation?. URL: https://autho.com/blog/how-secure-are-encryption-hashingencoding-and-obfuscation/